Distributed Ledger Technology

Assembled by Stephen Downes

Adoption Strategy	Underlying Concepts Core Technologies Defining Blockchain Key Concepts Blockchain for Business Applications Public Sector Applications Identity Adoption Strategy Related Technologies Hardware Advanced Concepts Coins Exchanges Platforms Decentralized Storage Distributed Applications Distributed Organizations Activity Issues Future?

McKinsey - https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value

Companies should take the following structured approach in their blockchain strategies:

- Identify value by pragmatically and skeptically assessing impact and feasibility at a granular level and focusing on addressing true pain points with specific use cases within select industries.
- Capture value by tailoring strategic approaches to blockchain to their market position, with consideration of measures such as ability to shape the ecosystem, establish standards, and address regulatory barriers.

With the right strategic approach, companies can start extracting value in the short term. Dominant players who can establish their blockchains as the market solutions should make big bets now.

https://igniteoutsourcing.com/publications/blockchain-asset-management/

The road to broad adoption across the asset management sector will include a process similar to the following:

- Consortium efforts involving government regulators, financial institutions, and technology providers
- POC testing of blockchain models
- Industry adoption DLT technology standards
- Interoperability with legacy systems
- Successful uses cases
- Proof of scalability
- Proof of security hardness

Experts suggest, further, that institutions begin by applying blockchain technology to internal, back-office processes before attempting large-scale implementation on public-facing systems.

Opportunity framework approach - p.11 - http://www.ey.com/Publication/vwLUAssets/Blockchain_in_wealth_and_asset_management/$FILE/ey-blockchain-innovation-wealth-asset-management.pdf

Obstacles to Adoption

https://techcrunch.com/2018/07/22/the-blockchain-begins-finding-its-way-in-the-enterprise/

- It's only for Bitcoin
    - "When Napster made it easy to share MP3 files illegally on a P2P network, McKenty believes, it set back business usage of P2P for a decade because of the bad connotations associated with the popular use case. "You couldn't talk about Napster [and P2P] and have it be a positive conversation. Bitcoin has done that to blockchain. It will take us time to recover what bitcoin has done to get to something that is really useful [with blockchain]," he said."
    - A recent survey by Deloitte of over 1000 participants in 7 countries - https://www2.deloitte.com/us/en/pages/consulting/articles/innovation-blockchain-survey.html - found that outside the US in particular this perception held true. "When asked if they believed that blockchain was just "a database for money" with little application outside of financial services, just 18 percent of US respondents agreed with that statement versus 61 percent of respondents in France and the United Kingdom," the report stated.
- It requires trust
    - "Richie Etwaru, founder and CEO at Hu-manity and author of the book, Blockchain Trust Companies sees it as a matter of trust. Companies aren't used to dealing from a position of trust. In fact, his book argues that the entire contract system exists because of a total lack of it."

Stages:

Blockchain applicability -
https://www.zdnet.com/article/blockchain-and-business-looking-beyond-the-hype/
Diagram: https://www.zdnet.com/article/blockchain-and-business-looking-beyond-the-hype/

Compliance ledger

- Real-time view of compliance, audit & risk data
- Provenance, immutability & finality are key
- Transparent access to auditor & regulator

Consortium shared ledger

- Created by a small set of participants
- Share key reference data
- Consolidated, consistent real-time view

Asset exchange

- Sharing of assets (voting, dividend notification)
- Assets are information, not financial
- Provenance & finality are key

High value market

- Transfer of high value financial assets
- Between many participants in a market
- Regulatory timeframes

The CxO Playbook

https://www.jpmorgan.com/global/cib/markets-investor-services/blockchain-economics

- Assess and understand the potential impact of blockchain on your organization.
- Outline the longer term vision and the ambition for your organization.
- Determine where blockchain falls on the priority scale for your leadership team, especially vis-à-vis other innovative technologies.
- Encourage open and transformative thinking, particularly among young tech teams.
- Develop an external engagement approach.

Key Players

Regulator

- An organization who enforces the rules of play
- Regulators are keen to support Blockchain-based innovations
- Concern is systemic risk – new technology, distributed data, security

Industry Group

- Often funded by members of a business network
- Provide technical advice on industry trends
- Encourages best practice by making recommendations to members

Market Maker

- In financial markets, takes buy-side and sell-side to provide liquidity
- More generally, the organization who innovates
    - Creates a new good or service, and business process (likely)
    - Creates a new business process for an existing good or service

Related Technologies

Validation

“All nodes validate all blocks and all transactions.”

“There’s no way for any node in the network to know that the block they received was *created* by their peer, or *relayed* by their peer. All they know is if it’s valid or not, and if it is they send it along, if it’s not, they don’t.”

“Some miners connect directly to other miners so that out of their peer list with the network, some of them are also other miners. **Not all miners do this**. Some of these miners that connect directly also use *optional* relay networks like the FIBRE network being designed by Bitcoin Core developer Matt Corallo.”

@StopAndDecrypt
Bitcoin is an impenetrable fortress of validation.

It doesn't matter if you created the transaction/block, or if someone else sent it to you: If it's not valid it's not getting in.

All nodes enforce validation in tandem.

Some people still don't seem to understand this concept.
5:41 PM - Jun 1, 2018

https://lightning.network/lightning-network-paper.pdf
If the balance in the channel is 0.05 BTC to Alice and 0.05 BTC to Bob, and the balance after a transaction is 0.07 BTC to Alice and 0.03 BTC to Bob, the network needs to know which set of balances is correct. Blockchain transactions solve this problem by using the blockchain ledger as a timestamping system. At the same time, it is desirable to create a system which does not actively use this timestamping system unless absolutely necessary, as it can become costly to the network

-

Message Brokers

- RabbitMQ - https://www.rabbitmq.com/
    - Features: https://www.rabbitmq.com/features.html

    - WhatIs & detailed description- https://www.cloudamqp.com/blog/2015-05-18-part1-rabbitmq-for-beginners-what-is-rabbitmq.html

Hosting and Suppport

- (There's a whole separate book for this section)
- Business networks
- Cloud
    - IBM

Serverless Applications

6 things I've learned in my first 6 months using serverless
https://read.acloud.guru/six-months-of-serverless-lessons-learned-f6da86a73526
    - Diagram - https://cdn-images-1.medium.com/max/1600/0*T_pYtoufH6Jbg_AH.

Debugging Serverless Apps: from monitoring invocations to observing a system of functions
https://read.iopipe.com/debugging-serverless-apps-from-monitoring-invocations-to-observing-a-system-of-functions-578c2ef8b3de

Doing Without Databases
https://codeburst.io/doing-without-databases-in-the-21st-century-6e25cf495373

Serverless Tag on CSS-Trick (lots of articles)
https://css-tricks.com/tag/serverless/

Containers

Docker

Node.js - Docker Workflow
https://medium.com/@guillaumejacquart/node-js-docker-workflow-12febcc0eed8

Bots

The 'pico' - https://blogs.harvard.edu/doc/2018/06/07/bots/
The current code for this is called Wrangler. It's open source and in Github. For the curious, Phil Windley explains how picos work in Reactive Programming With Picos.

Watermark Token

- a token that piggybacks on Bitcoin to move value around the system -

Wallets

Electronic Wallets

https://cryptocurrencyhub.io/i-bought-my-first-bitcoin-now-what-fdf7dc9ad150
"Bitcoin wallets are the electronic equivalent of keeping cash in your pocket (or under your mattress). The money is yours, and no one can touch it without your permission."
"Your Bitcoins themselves are never on your hard drive. They're on the decentralized Bitcoin network, with thousands and thousands of copies existing all over the world, impossible to delete."
"What you're actually keeping in your wallet is the private key that is used to access (spend/transfer) your coins."

Activity
https://medium.com/@mccannatron/12-graphs-that-show-just-how-early-the-cryptocurrency-market-is-653a4b8b2720

- There are ~24M bitcoin wallet addresses in total. This doesn't mean there are 24M Bitcoin users because one person can have more than 1 wallet address and it is recommended to generate a new bitcoin address for each transaction sent.
- Graph: https://cdn-images-1.medium.com/max/800/1*jkReP_4QHbu4SXGZ_Obk3Q.png
- we can look at the number of active addresses per day. - Graph: https://cdn-images-1.medium.com/max/800/1*o9C_n6aNxT5aBvUJq20JhA.png
- Ethereum address growth and active addresses per day (in log scale): 31M Ethereum addresses with peak daily active addresses on the Ethereum network reaching 1.1M. graph: https://cdn-images-1.medium.com/max/800/1*PSC3Ks003Z9Oa0wBCS9eFg.png
- Active addresses per day: https://cdn-images-1.medium.com/max/800/1*ENr1cILuJbm9IV88n_LZSQ.png

SimpleWallet / Zedwallet

Simplewallet configuration and commands
http://forknote.net/documentation/simplewallet/

Zedwallet, A New Simplewallet for CryptoNote Currencies

https://medium.com/@turtlecoin/zedwallet-a-new-simplewallet-for-cryptonote-currencies-2c74c5fc1302 "Some of you may have noticed in the last few releases that Simplewallet has been looking a bit more polished. In fact, what you may not have noticed is the old Simplewallet is gone, and we've all been using the new Zedwallet since v0.4.2."

Using Zedwallet
https://github.com/turtlecoin/turtlecoin/wiki/Using-Zedwallet

BreadWallet

https://brd.com/
BRD is the simple and secure onramp to bitcoin, ethereum, and other digital currencies.

Eidoo

-
- https://eidoo.io/ - Eidoo - Multicurrency Wallet & Hybrid Exchange
-

Atomic Swap Wallet

- Altcoin - Atomic Swap Wallet - https://swap.altcoin.io/

Exodus

- Exodus - http://www.exodus.io/
    - Screen shot - https://cdn-images-1.medium.com/max/1600/1*mTLKKtTp24qPsXaxZ2KtgQ.jpeg from https://cryptocurrencyhub.io/i-bought-my-first-bitcoin-now-what-fdf7dc9ad150

Copay Wallet

https://copay.io/

What is Copay Wallet: Complete Review
https://medium.com/@zorzini/originally-published-at-unblock-net-on-june-13-2018-d32b330f01ff

Bitfi

Bitcoin wallet Bitfi withdraws 'unhackable' claim
https://www.bbc.co.uk/news/technology-45368044

“Bitfi, a cryptocurrency wallet backed by anti-virus software entrepreneur John McAfee, has issued a statement saying it will no longer describe its service as "unhackable". The announcement followed the release of evidence by a group of security researchers showing the wallet being compromised.”

Security Token (b) / Hardware Wallet

Not to be confused with Security Token (a); see ICO, above

“**Security tokens** are physical devices used to gain access to an electronically restricted resource. The token is used in addition to or in place of a password. It acts like an electronic key to access something. Examples include a wireless keycard opening a locked door, or in the case of a customer trying to access their bank account online, the use of a bank provided token can prove that the customer is who they claim to be.” https://en.wikipedia.org/wiki/Security_token

- Is 2018 the Year of the Security Token? - https://www.investopedia.com/tech/2018-year-security-token/

Hardware wallet
https://en.bitcoin.it/wiki/Hardware_wallet

Ledger Nano

- https://www.ledgerwallet.com/r/1985?path=/products/

Ledger Crypto Wallet Goes Mobile With Bluetooth-Ready Nano X
https://www.coindesk.com/ledger-crypto-wallet-goes-mobile-with-bluetooth-ready-nano-x
By connecting the Nano X via Bluetooth, it’s possible to have the security of Ledger but with mobile’s form factor, Larchevêque said. (Ledger devices store keys but an external application on a computing device is needed to write and send transactions.)

TREZOR

- https://shop.trezor.io/?a=mycrypto.com

https://decentralize.today/new-status-report-released-7d24cbaaa33f
Particl (see below) working toward integration

The Elephant

The Elephant: 'Enabling the tokenisation of any asset in the world' - https://thelephant.io/

- “By tokenizing the rights to future shares in startups after their public offering, The Elephant’s marketplace brings an immense source of liquidity to the existing market for such assets, which is notoriously difficult to navigate. With companies taking longer to go public than they used to, many can’t avail of their equity rights for as long as ten years. Blockchain infrastructure finally provides a market where these rights can be bought and sold

transparently, to the benefit of rights holders and cryptocurrency enthusiasts alike."
https://www.investopedia.com/tech/2018-year-security-token/

Explorers

Etherscan

https://etherscan.io/

- Ethereum block explorer
-

User Interface

- 'Garages'
- Engagement
-

MetaMask

https://metamask.io/
Chrome, Firefox or Opera plugin, or run on Brave browser

- "MetaMask is a bridge that allows you to visit the distributed web of tomorrow in your browser today. It allows you to run Ethereum dApps right in your browser without running a full Ethereum node.

  MetaMask includes a secure identity vault, providing a user interface to manage your identities on different sites and sign blockchain transactions.

  You can install the MetaMask add-on in Chrome, Firefox, Opera, and the new Brave browser. If you're a developer, you can start developing with MetaMask today.
  https://github.com/MetaMask/faq/

  Our mission is to make Ethereum as easy to use for as many people as possible."

Chrome browser plugin called MetaMask. This will allow websites (that you authorize) access to your Ethereum account. https://metamask.io/

How to Use MetaMask (Like a Wizard)
https://media.consensys.net/how-to-use-metamask-like-a-wizard-850a96fdd95c
MetaMask connects your browser to the Ethereum network, and provides a secure identity and token wallet so that you can interact with dApps and engage with blockchain. The MetaMask Plug-in—which is compatible with Chrome, Firefox, Opera and Brave —has been downloaded over

1,000,000 times, and provides essential tools as you begin exploring the world of blockchain, decentralized apps, and digital assets.

Mist

Mist which is basically a web browser for Ethereum apps. https://github.com/ethereum/mist/releases

Hardware

https://www.lifewire.com/cryptocoin-mining-for-beginners-2483064
The whole focus of mining is to accomplish three things:

- Provide bookkeeping services to the coin network. Mining is essentially 24/7 computer accounting called 'verifying transactions'.
- Get paid a small reward for your accounting services by receiving fractions of coins every couple of days.
- Keep your personal costs down, including electricity and hardware.

GPUs

https://www.investopedia.com/tech/gpu-cryptocurrency-mining/
“GPU-based mining, which offered multiple benefits over the use of CPU. A standard GPU, like Radeon HD 5970, clocked processing speeds of executing 3200 32-bit instructions per clock, which was 800 times more than the speed of CPU that executed only 4 32-bit instructions per clock.
The core reason behind this efficiency is that the video processing GPUs are devised to do better in performing similar and repetitive work, than in performing diversified multi-tasking functions like those of the CPU. For example, rendering a 3D movie requires the GPU to keep processing similar kinds of information to the screen again and again, though with slight changes.”

Cryptocurrency miners bought 3 million GPUs in 2017 -
https://www.zdnet.com/article/cryptocurrency-miners-bought-3-million-gpus-in-2017/

Asus Announces Crypto Mining Motherboard With Support for 20 GPUs -
https://www.extremetech.com/computing/270333-asus-announces-crypto-mining-motherboard-with-support-for-20-gpus

Best mining GPU 2018 : the best graphics cards for mining Bitcoin, Ethereum and more
https://www.techradar.com/news/best-mining-gpu - also needs mining software -
https://www.techradar.com/news/the-best-cryptocurrency-mining-software-2018

Crypto ASIC

From: https://cryptocurrencyfacts.com/asic-mining-basics/

- **ASIC?** “Application-specific integrated circuit.”
- - crypto ASIC - type of chip that is ultra specialized in a single set of processes (in this case, mining cryptocurrency).
- **“mining rig”** a device like an Antminer (see below), but potentially a whole rack (or racks) of fans, processors, ASIC miners, etc (like this).
- **mining pool?** Solo mining in this day and age is not a great idea unless you have a lot of power (or are mining an altcoin). A mining pool is a group you join and pay fees too. Everyone splits the take, minus fees.

https://motherboard.vice.com/en_us/article/3kj5dw/what-is-an-asic-miner-bitmain-monero-ethereum

- Given how this changed the landscape of Bitcoin mining—leading to the rise of giants like Bitmain in China and BitFury in the US—Monero and Ethereum were designed to be “ASIC-resistant.”

List of hardware ASIC rigs: https://www.bitcoinmining.com/bitcoin-mining-hardware/

Antminer

- Antminer rigs are a good choice. Antminer is a brand, ASIC is a generic term like CPU or GPU https://shop.bitmain.com/

Services

https://www.bitcoinmining.com/bitcoin-mining-hardware/

- For those not interested in operating the actual hardware then they can purchase Bitcoin cloud mining contracts.
    - **Hashflare Review:** Hashflare offers SHA-256 mining contracts and more profitable SHA-256 coins can be mined while automatic payouts are still in BTC. Customers must purchase at least 10 GH/s.
    - **Genesis Mining Review:** Genesis Mining is the largest Bitcoin and scrypt cloud mining provider. Genesis Mining offers three Bitcoin cloud mining plans that are reasonably priced. **Zcash mining contracts** are also available.
    - **Hashing 24 Review:** Hashing24 has been involved with Bitcoin mining since 2012. They have facilities in Iceland and Georgia. They use modern ASIC chips from BitFury deliver the maximum performance and efficiency possible.
    - **Minex Review:** Minex is an innovative aggregator of blockchain projects presented in an economic simulation game format. Users purchase Cloudpacks which can then be used to build an index from pre-picked sets of cloud mining farms, lotteries, casinos, real-world markets and much more.

- **Minergate Review:** Offers both pool and merged mining and cloud mining services for Bitcoin.
- **Hashnest Review:** Hashnest is operated by Bitmain, the producer of the Antminer line of Bitcoin miners. HashNest currently has over 600 Antminer S7s for rent. You can view the most up-to-date pricing and availability on Hashnest's website. At the time of writing one Antminer S7's hash rate can be rented for $1,200.
- **Bitcoin Cloud Mining Review:** Currently all Bitcoin Cloud Mining contracts are sold out.
- **NiceHash Review:** NiceHash is unique in that it uses an orderbook to match mining contract buyers and sellers. Check its website for up-to-date prices.
- **Eobot Review:** Start cloud mining Bitcoin with as little as $10. Eobot claims customers can break even in 14 months.
- **MineOnCloud Review:** MineOnCloud currently has about 35 TH/s of mining equipment for rent in the cloud. Some miners available for rent include AntMiner S4s and S5s.

https://media.consensys.net/how-blockchain-is-helping-technology-get-its-soul-back-a2d6cf96a272

Kidner Project (@KidnerProject). A decentralized protocol to facilitate kidney paired donation while preserving privacy and confidentiality. Team members: Sajida Zouarhi (@Saj_JZ), Maroussia Arnault, Amelia Lintern-Smith, Noah Basri, Clément Massonnaud, Mathieu Vincens.

Aphetor. A new consensus mechanism for asserting and verifying the identity and reputation of charging stations, EVs, and drones, and for automating the exchange of energy and payments between distributed charging stations and battery-electric machines. Team members: Alexander S. Blum (@alexandersblum), Meredith Finkelstein, Seth Weiner, Chris Jaroszewski, Peter Lyons.

Consensus Algorithms

Theoretical Foundations

Paxos

https://lamport.azurewebsites.net/pubs/lamport-paxos.pdf

- Versions: EPaxos, Vertical Paxos, VR and Ring Paxos to name but a few

Raft

https://raft.github.io/

- The Raft Paper - https://raft.github.io/raft.pdf
- with 50+ open source implementations including CoreOS's etcd and HashiCorp's Consul.

Generalized Consensus Algorithm

https://hh360.user.srcf.net/blog/2019/02/towards-an-intuitive-high-performance-consensus-algorithm/

https://arxiv.org/pdf/1902.06776.pdf
"We have demonstrated that this solution not only unifies existing algorithms including Paxos and Fast Paxos but also demonstrates that such algorithms are conservative as their quorum intersection requirements and quorum agreement rules can be substantially weakened. We have illustrated the power of our generalised consensus algorithm by proposing three novel algorithms for consensus, demonstrating a few interesting points on the diverse array of algorithms made possible by our abstract."

Core Elements of Consensus

Generality

Immutability

Immutability Changes Everything
https://queue.acm.org/detail.cfm?id=2884038
Image: https://deliveryimages.acm.org/10.1145/2890000/2884038/helland1.png

Keeping CALM: when distributed consistency is easy

Adrian Colyer, The Morning Paper, Mar 06, 2019
This is a key question: "What is the family of problems that can be consistently computed in a distributed fashion without coordination, and what problems lie outside that family?" Here's the proposed answer: "Consistency as Logical Monotonicity (CALM). A program has a consistent, coordination-free distributed implementation if and only if it is monotonic." By monotonic, we mean this: "once we learn something to be true, no further information can

come down the line later on to refute that fact." How do we get monotonicity? Confluent operations, that is, "If it produces the same sets of outputs for any non-deterministic ordering and batching of a set of inputs." Give it the same data, however ordered, and it produces the same results. It gives you something to think about. Accounting is confluent; the order of transactions doesn't matter, the balance is the same in the end. Voting is confluent; you vote in morning or evening, but the final tally is the same. But causation and agency are *not* confluent. When you're trying to make something happen, order matters.

https://blog.acolyer.org/2019/03/06/keeping-calm-when-distributed-consistency-is-easy/

Implementations

Proof of Work

Require validators to solve difficult cryptographic puzzles
PROs: Works in untrusted networks
CONS: Relies on energy use; slow to confirm transactions
Example usage: Bitcoin, Ethereum

https://motherboard.vice.com/en_us/article/3kj5dw/what-is-an-asic-miner-bitmain-monero-ethereum
Most major cryptocurrencies use a unique PoW algorithm. For example, Bitcoin uses a hashing algorithm called SHA-256, Monero uses CryptoNight, and Ethereum's PoW algorithm is called Ethash.

Proof of Stake

Require validators to hold currency in escrow
PROs: Works in untrusted networks
CONS: Requires intrinsic (crypto)currency, "Nothing at stake" problem
Example usage:Nxt

Proof of Authority

What is Proof-of-Authority?
https://medium.com/@Elysian_Ely/what-is-proof-of-authority-6c8a08397311 "Proof-of-Authority is a modified Proof-of-Stake consensus mechanism. Proof-of-Authority works by removing the weight of an actor (based on the value of their digital assets) and focuses on tying an individual's identity to their ability to validate a network."

Solo

Validators apply received transactions without consensus
PROs: Very quick; suited to development

CONS: No consensus; can lead to divergent chains
Example usage: Hyperledger Fabric V1

Kafka/Zookeeper

Ordering service distributes blocks to peers
PROs: Efficient and fault tolerant
CONS: Does not guard against malicious activity
Example usage:
Hyperledger Fabric V1

Proof of Elapsed Time

Wait time in a trusted execution environment randomizes block generation
PROs: Efficient
CONS: Currently tailored towards one vendor
Example usage: Sawtooth-Lake

PBFT-Issued

Practical Byzantine Fault Tolerance implementations
PROs: Reasonably efficient and tolerant against malicious peers
CONS: Validators are known and totally connected
Example usage: Hyperledger Fabric V0.6

Advanced Concepts

Network Effects

The Future Of Network Effects: Tokenization and the End of Extraction
https://medium.com/public-market/the-future-of-network-effects-tokenization-and-the-end-of-extraction-a0f895639ffb

- Because network effect businesses provide more value to participants the larger they grow, they can be immensely hard to get off the ground.
- The ones that do reach critical mass tend to careen towards natural monopoly
- Image: https://cdn-images-1.medium.com/max/600/0*HhOeuLRVZy4c5qTU.jpg
- Enter Tokenized Networks: Network Effects Without the Extraction Imperative

- “tokenized networks are able to provide all the benefits of network effects without the costs to the network participants that are unavoidable under private, centralized network ownership.”

Symmetric key encryption

Encryption basics
https://searchsecurity.techtarget.com/Understanding-encryption-and-cryptography-basics

If you want to apply symmetric key encryption to a file transfer environment, both the sender and receiver should have a copy of **the same key**. The sender will use his copy of the key for encrypting the file, while the receiver will use his copy for decrypting it.
https://www.jscape.com/blog/bid/84422/Symmetric-vs-Asymmetric-Encryption

Some of the encryption algorithms that use symmetric keys include: AES (Advanced Encryption Standard), Blowfish, DES (Data Encryption Standard), Triple DES, Serpent, and Twofish.

DES - The Data Encryption Standard

The Data Encryption Standard (DES) is an outdated symmetric-key method of data encryption.
https://searchsecurity.techtarget.com/definition/Data-Encryption-Standard

AES - Advanced Encryption Standard

The Advanced Encryption Standard, or AES, is a symmetric block cipher chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.
https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard

Lovely Cartoon (read all the way to the end):
http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html

Asymmetric Cryptography

https://searchsecurity.techtarget.com/definition/asymmetric-cryptography
Asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key. The other key in the pair is kept secret; it is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.
...
Encryption strength is directly tied to key size and doubling key length delivers an exponential increase in strength, although it does impair performance. As computing power increases and more efficient factoring algorithms are discovered, the ability to factor larger and larger numbers also increases.

https://blog.goodaudience.com/very-basic-elliptic-curve-cryptography-16c4f6c349ed
“The crux of all public key cryptographic algorithms is that they each have their own unique trapdoor function. A trapdoor function is a function that can only be computed one way, or at least can only be computed one way easily (in less than millions of years using modern computers).

Protocols using Asymmetric Cryptography

protocols like SSH, OpenPGP, S/MIME, and SSL/TLS rely on asymmetric cryptography for encryption and digital signature functions

Asymmetric Cryptography Algorithms

DH Diffie-Hellman

The Diffie-Hellman (DH) algorithm, created by Whit Diffie and Martin Hellman, introduced public-key cryptography to the public.
https://searchsecurity.techtarget.com/Understanding-encryption-and-cryptography-basics

- A major application of DH is VPNs. Internet Key Exchange (IKE), the key management protocol used with the IP Security (IPSec) protocol, uses DH when two encrypting devices first try to communicate.

RSA (Rivest-Shamir-Adleman)

- embedded in the SSL/TLS protocol which is used to provide communications security over a computer network.
- RSA derives its security from the computational difficulty of factoring large integers that are the product of two large prime numbers. Multiplying two large primes is easy, but the difficulty of determining the original numbers from the total -- factoring -- forms the basis of public key cryptography security.

Elliptic Curve Cryptography

- (ECC) is gaining favor with many security experts as an alternative to RSA for implementing public-key cryptography.
- ECC generates keys through the properties of the elliptic curve equation.

https://hackernoon.com/understanding-decentralized-exchanges-51b70ed3fe67
the special sauce that makes off-chain order books work comes right from the heart of blockchain—an Elliptic Curve Digital Signature Algorithm—or ECDSA for short.

(Very) Basic Elliptic Curve Cryptography -
https://blog.goodaudience.com/very-basic-elliptic-curve-cryptography-16c4f6c349ed

- ECC is a type of Public Key Cryptography
- A 256 bit key in ECC offers about the same security as 3072 bit key using RSA.

How Schnorr signatures may improve Bitcoin
https://medium.com/@snigirev.stepan/how-schnorr-signatures-may-improve-bitcoin-91655bcb4744

- These are a variation on ECDSA
- Good diagrams make both concepts clear

Hybrid Cryptography

https://www.jscape.com/blog/bid/84422/Symmetric-vs-Asymmetric-Encryption
Because both symmetric and asymmetric key cryptography have their own advantages, modern file transfer systems typically employ a hybrid of the two. Some hybrid cryptosystems are: SSL (used in FTPS and HTTPS), SSH (used in SFTP), and OpenPGP, all of which are supported by JSCAPE MFT Server.
Hybrid cryptosystems employed in an SFTP or FTPS server use asymmetric keys to initially encrypt symmetric keys known as session keys. The session keys are then the ones used to encrypt the actual data. As its name implies, a session key is only used in one session. After the session, the key is simply discarded. That's a good thing because even if a session key is compromised, only data sent within that particular session will be at risk.
Diagram -
https://www.jscape.com/hs-fs/hub/26878/file-13611379-png/images/hybrid_cryptosystem_used_in_file_transfer.png

Digital Signatures

To create a digital signature:

- signing software (such as an email program) creates a one-way hash of the electronic data to be signed.
- The user's private key is then used to encrypt the hash, returning a value that is unique to the hashed data.
- The encrypted hash, along with other information such as the hashing algorithm, forms the digital signature.

Any change in the data, even to a single bit, results in a different hash value.

- This attribute enables others to validate the integrity of the data by using the signer's public key to decrypt the hash.
- If the decrypted hash matches a second computed hash of the same data, it proves that the data hasn't changed since it was signed.
- If the two hashes don't match, the data has either been tampered with in some way (indicating a failure of integrity) or the signature was created with a private key that doesn't correspond to the public key presented by the signer (indicating a failure of authentication).

Public key authentication

https://searchsecurity.techtarget.com/definition/asymmetric-cryptography
“For asymmetric encryption to deliver confidentiality, integrity, authenticity and non-repudiability, users and systems need to be certain that a public key is authentic, that it belongs to the person or entity claimed and that it has not been tampered with or replaced by a malicious third party. There is no perfect solution to this public key authentication problem.”

- public key infrastructure (PKI), where trusted certificate authorities certify ownership of key pairs and certificates, is the most common approach,
- Pretty Good Privacy (PGP) model (including OpenPGP), rely on a decentralized authentication model called a web of trust, which relies on individual endorsements of the link between user and public key.

Keybase

https://keybase.io/
“Keybase is a new and free security app for mobile phones and computers. For the geeks among us: it's open source and powered by public-key cryptography.
Keybase is for anyone. Imagine a Slack for the whole world, except end-to-end encrypted across all your devices. Or a Team Dropbox where the server can't leak your files or be hacked.”

Starting today (June 21 2018), the Keybase app - across all platforms - supports time-based exploding messages. These work great for teams, families, friends, communities, and 1-on-1 chats. They're end-to-end encrypted but also explode after a short duration. Read the announcement.

https://en.wikipedia.org/wiki/Keybase
“Keybase is a key directory that maps social media identities to encryption keys (including, but not limited to PGP keys) in a publicly auditable manner. Keybase offers an end-to-end encrypted chat and cloud storage system, called Keybase Chat and the Keybase filesystem respectively. Files placed in the public portion of the filesystem are served from a public endpoint,[3] as well as locally from a filesystem mounted by the Keybase client.
Keybase supports publicly connecting Twitter, GitHub, Facebook, Reddit, and Hacker News identities to encryption keys, along with Bitcoin and Zcash wallet addresses. Keybase has supported Coinbase identities since initial public release, but ceased to do so on March 17, 2017 when Coinbase terminated public payment pages.”

BitID

http://bitid.bitcoin.blue/
“open protocol proposal allowing simple and secure authentication based on public key cryptography. By authentication we mean to prove to a service/application that we control a specific Bitcoin address by signing a challenge, and that all related data and settings may securely be linked to our session.”

“Bitcoin related sites and applications shouldn’t have to rely on artificial identification methods such as usernames and passwords. Using a wallet for authentication purposes has many benefits :

- "one-click" registration and login procedures
- no need to remember or duplicate passwords
- the server only knows and stores the users's Bitcoin public address
- services always know the return address
- optionally, connect to a decentralized identification system in order to populate registration fields (nickname, email ...)

See complete BitID presentation : http://bit.ly/bitid-slides”

Secure Computing Architectures

https://medium.com/@FEhrsam/blockchain-based-machine-learning-marketplaces-cb2d4dae2c17
“There are 3 main forms of secure computation being used and researched today: homomorphic encryption (HE), secure multi-party computation (MPC), and zero knowledge proofs (ZKPs).”

“Multiparty computation is most commonly used for private machine learning at the moment, as homomorphic encryption tends to be too slow and it’s not obvious how to apply ZKPs to machine learning.”

Homomorphic Encryption

“Homomorphic encryption is a form of encryption that allows computation on ciphertexts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext. The purpose of homomorphic encryption is to allow computation on encrypted data.”

Partially homomorphic cryptosystems - all from
https://en.wikipedia.org/wiki/Homomorphic_encryption

In the following examples, the notation E (x) {\displaystyle {\mathcal {E}}(x)} is used to denote the encryption of the message x {\displaystyle x} .

Unpadded RSA
If the RSA public key is modulus m and exponent e then the encryption of a message x is given by E (x) = x e mod m

ElGamal

In the ElGamal cryptosystem, in a cyclic group G of order q with generator g, if the public key is (G , q , g , h) , where h = g x, and x is the secret key, then the encryption of a message m is E (m) = (g r , m · h r), for some random r ∈ { 0 , … , q − 1 }

Goldwasser–Micali

In the Goldwasser–Micali cryptosystem, if the public key is the modulus *m* and quadratic non-residue *x*, then the encryption of a bit *b* is E (b) = x b r 2 mod m

Benaloh

In the Benaloh cryptosystem, if the public key is the modulus *m* and the base *g* with a blocksize of *c*, then the encryption of a message *x* is E (x) = g x r c mod m

Paillier

In the Paillier cryptosystem, if the public key is the modulus *m* and the base *g*, then the encryption of a message *x* is E (x) = g x r m mod m 2 Secure Multi-Party Computation

Secure multi-party computation (MCP)

https://en.wikipedia.org/wiki/Secure_multi-party_computation
Secure computation was formally introduced as secure two-party computation (2PC) in 1982 (for the so-called Millionaires' Problem), and in generality in 1986 by Andrew Yao.[1][2] The area is also referred to as Secure Function Evaluation (SFE). The two party case was followed by a generalization to the multi-party by Goldreich, Micali and Widgerson.

There are major differences between the protocols proposed for two party computation (2PC) and multiparty computation (MPC).

Yao's garbled circuit protocol.

Zero Knowledge Proofs

Holding law-enforcement accountable for electronic surveillance
http://news.mit.edu/2018/holding-law-enforcement-accountable-for-electronic-surveillance-audit-0808 - new paper about the system, which they've dubbed "AUDIT" ("Accountability of Unreleased Data for Improved Transparency"). "AUDIT can prove that the FBI's request is above board using a cryptographic method called "zero-knowledge proofs." First developed in the 1980s by Goldwasser and other researchers, these proofs counterintuitively make it possible to prove that surveillance is being conducted properly without revealing any specific information about the surveillance."

Why America's Biggest Bank Digs Anonymous Cryptocurrency
https://medium.com/mit-technology-review/why-americas-biggest-bank-digs-anonymous-cryptocurrency-3d05ed9e7ffa

“Zero-knowledge proofs are not about skirting the law, he says, but about proving things though selective disclosure. That promises to have plenty of applications in the world JPMorgan inhabits. “The finance industry thrives on privacy,” Gün Sirer says.”

Nightfall

Nightfall...Sounds like a video game, but it’s actually Ernst and Young’s blockchain protocol that will run on the public Ethereum blockchain. Huge. News. Let’s get physical...EY plans to tokenize physical goods and built a special token to separate a physical asset from legal ownership of that asset. Even better, it’s compatible with existing ERC 721 standards.

EY (Ernst & Young) releases zero-knowledge proof blockchain transaction technology to the public domain to advance blockchain privacy standards
https://www.ey.com/en_gl/news/2019/04/ey-releases-zero-knowledge-proof-blockchain-transaction-technology-to-the-public-domain-to-advance-blockchain-privacy-standards

zk-snarks

What are zk-snarks - https://www.youtube.com/watch?v=IizZEihY8AE
Examples: https://asecuritysite.com/encryption/zksnark01 - Homophonic Hiding (HH)
https://asecuritysite.com/encryption/zksnark02 - Blind evaluation problem

https://www.ethnews.com/ethereum-creator-vitalik-buterin-explores-zk-starks-in-new-blog-post
While currently the sending address, receiving address, and the amount of Ether involved in every Ethereum transaction is a matter of public record, zk-SNARKs would effectively mask these three data points, potentially making the platform more attractive to privacy-focused users.

https://www.coindesk.com/zk-snarks-everywhere-ethereum-privacy-tech-hits-tipping-point/
zk-snarks are believed to be a potential building block that can be used to scale the ethereum network
-

ZoKrates - a toolbox for zkSNARKS on Ethereum - https://www.youtube.com/watch?v=sSlrywb5J_0

https://www.ethnews.com/ethereum-creator-vitalik-buterin-explores-zk-starks-in-new-blog-post
On November 9 2017, Ethereum creator Vitalik Buterin published a blog post exploring the class of technology known as zero-knowledge Succinct Transparent ARguments of Knowledge (zk-STARKs) and how they differ from the related and better-known mechanisms that fit under the gloss of zero-knowledge Succinct Non-interactive ARguments of Knowledge (zk-SNARKs).

Vitalik Buterin - https://vitalik.ca/general/2017/11/09/starks_part_1.html

- Some really good examples of how this could be used to prove transactions
-

Zk-snarks and ethereum - https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/

“$E(x)\ E(y) \equiv x^e y^e \equiv (xy)^e \equiv E(x\ y) \pmod n$, or in words: The product of the encryption of two messages is equal to the encryption of the product of the messages.”

Oracles

https://blockchainhub.net/blockchain-oracles/
“An oracle, in the context of blockchains and smart contracts, is an agent that finds and verifies real-world occurrences and submits this information to a blockchain to be used by smart contracts.”

Types of Oracle

Software Oracles

https://blockchainhub.net/blockchain-oracles/
Software oracles handle information available online. An example could be the temperature, prices of commodities and goods, flight or train delays, etc. The data originates from online sources, like company websites. The software oracle extracts the needed information and pushes it into the smart contract.

Hardware Oracles

https://blockchainhub.net/blockchain-oracles/
Some smart contracts need information directly from the physical world, for example, a car crossing a barrier where movement sensors must detect the vehicle and send the data to a smart contract. Another use case is RFID sensors in the supply chain industry. The biggest challenge for hardware oracles is the ability to report readings without sacrificing data security. Oracalize proposes a two-step solution to the risks, by providing cryptographic evidence of the sensor’s readings and anti-tampering mechanisms rendering the device inoperable in the case of a breach.

Inbound Oracles

https://blockchainhub.net/blockchain-oracles/
These provide the smart contract with data from the external world. Example use case will be an automatic buy order if the USD hits a certain price.

Outbound Oracles

https://blockchainhub.net/blockchain-oracles/
These provide smart contracts with the ability to send data to the outside world. An example would be a smart lock in the physical world which receives a payment on its blockchain address and needs to unlock automatically.

Consensus Based Oracles

https://blockchainhub.net/blockchain-oracles/
Prediction markets like Augur and Gnosis rely heavily on oracles to confirm future outcomes. Using only one source of information could be risky and unreliable. To avoid market manipulation prediction markets implement a rating system for oracles. For further security, a combination of different oracles may be used, where for example 3 out of 5 oracles could determine the outcome of an event.

Scaling

https://media.consensys.net/the-state-of-scaling-ethereum-b4d095dbafae
Trilemma: security, decentralization, and scalability.

Issues

Throughput

"The most commonly discussed scaling challenge is transaction throughput. Currently, ethereum can process roughly 15 transactions per second, while in comparison Visa processes approximately 45,000/tps. In the last year, some applications—like Cryptokitties, or the occasional ICO—have been popular enough to "slow down" the network and raise gas prices."
https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

- "The core limitation is that public blockchains like ethereum require every transaction to be processed by every single node in the network."

Lack of Parallelism

Layer 1 Responses

Block Sizes

"We *could* ask every individual node to do more work. If we doubled the block size (i.e., the block gas limit), it would mean that each node is doing roughly double the amount of work processing each block. But this comes at the cost of decentralization: requiring more work from nodes means that less powerful computers (like consumer devices) may drop out of the network, and mining becomes more centralized in powerful node operators."
https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

Sharding

"What if we could build a blockchain where every node didn't have to process every operation? What if, instead, the network was divided into two sections, which could operate semi-independently?"
https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

Sharding: https://media.consensys.net/the-state-of-scaling-ethereum-b4d095dbafae

- Sharding allows for operations to run simultaneously alongside one another, therefore increasing the number of transactions per second the overall blockchain can process.
- With sharding, the Ethereum network is divided into multiple groups of nodes. Each of these groups is a shard, and each shard processes all the transactions that occur within that group.

Sharding FAQ - https://github.com/ethereum/wiki/wiki/Sharding-FAQs

https://medium.com/@icebearhww/ethereum-sharding-and-finality-65248951f649 Ethereum Sharding: Overview and Finality

Ethereum's Casper and Sharding New Design
https://medium.com/@Michael_Spencer/ethereums-casper-and-sharding-new-design-14014e83d55f

- "Vitalik Buterin indicated at a meeting of the platform's open-source developers in mid June, 2018, that sharding and casper could be rolled out together."
- "Sharding in and of itself may the the next-gen solution to scaling the system to a massive number of transactions."
- "Sharding is a scaling solution that will use shards, a neat term for micro-chains to process separate types of transactions on the Ethereum blockchain. With a system of transaction classification on individual chains within Ethereum, a specific group of nodes would need to verify a relevant transaction, instead of all of them."
- Diagram: https://cdn-images-1.medium.com/max/800/1*yJ-nwcDBQW_wJn0qjgBKvQ.png

Casper

- protocol by which Ethereum's current Proof of Work (PoW) model will change to Proof of Stake (PoS).
- decentralized Proof of Stake protocol is being done by the Ethereum Foundation with Casper The Friendly Ghost and Casper The Friendly Finality Gadget.
- "validators" replace miners, and they "validate" (instead of mine) blocks onto the blockchain.
- The final rollout of Casper will be preceded by two iterations of the protocol: Casper FFG (Friendly Finality Gadget) and Casper CBC (Correct-by-Construction).

https://medium.com/@Michael_Spencer/ethereums-casper-and-sharding-new-design-14014e83d55f
If Sharding itself removes the need for the entire network of nodes to process every individual transaction—increasing TPS on the Ethereum blockchain; Casper is the friendly ghost that can punish all malicious elements.
Think of this way, I'll just let Vlad speak to this key point:

> **Vlad Zamfir @VladZamfir**
> Replying to **@VladZamfir** **@mariesleaf** **@_jillruth**
> Scalability is a thing, but it's much less important than the community's existence, culture, and governance. If the community exists only to get rich, then it's probably a really crappy community. And if you have effective governance, you can always fork to Casper/Sharding

So Casper is designed to work in a trustless system and be more Byzantine Fault Tolerant. If you care about decentralization, it must be enforced and implicit in the system you choose to use.

Layer 2 Responses

"Rather than increase the capacity of the ethereum blockchain itself, what if we could do more things with the capacity we already have? This is the insight behind "off-chain" technologies like state channels, Plasma, and Truebit."
https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

- Cryptoeconomic consensus gives us a core hard kernel of certainty—unless something extreme like a 51% attack happens, we know that on-chain operations—like payments, or smart-contracts—will execute as written.
- The insight behind layer 2 solutions is that we can use this core kernel of certainty as an anchor—a fixed point to which we attach additional economic mechanisms.

Payment Channels

- has been around for several years, and recently implemented on bitcoin through the lightning network. (See 'Lightning', below)

State Channels

https://medium.com/statechannels/counterfactual-generalized-state-channels-on-ethereum-d38a36d25fc6

“State channels are the foundational technology for useable distributed applications. They can be used in any interaction with a defined set of participants, such as payments or games like chess or poker. “Channelizing” these applications makes them radically cheaper, and reduces the unacceptably high latency in today’s blockchain applications, enabling the web-like response times expected by users.”
two broad goals:

- Design a generalized state channels implementation
- Make it *easy* for developers to utilize state channels

White paper: https://counterfactual.com/statechannels

Jeff Coleman - State Channels - www.jeffcoleman.ca/state-channels/

- “State channels are a very broad and simple way to think about blockchain interactions which could occur on the blockchain, but instead get conducted off of the blockchain, without significantly increasing the risk of any participant.”

“State channels are the more *general* form of payment channels—they can be used not only for payments, but for any arbitrary “state update” on a blockchain—like changes inside a smart contract. State channels were first described in detail by Jeff Coleman in 2015.”
https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

https://medium.com/blockchannel/the-redemptive-greed-that-will-drive-decentralization-generalized-state-channels-in-depth-part-666bd6244a28
Jeff Coleman’s 2015 post is a compelling introduction in which he asserts that the basic components of a state channel are:

1. Part of the blockchain state is locked via multisignature or some sort of smart contract, so that a specific set of participants must completely agree with each other to update it.
2. Participants update the state amongst themselves by constructing and signing transactions that *could* be submitted to the blockchain, but instead are merely held onto for now. Each new update “trumps” previous updates.
3. Finally, participants submit the state back to the blockchain, which closes the state channel and unlocks the state again (usually in a different configuration than it started with).

Really really detailed:
The Redemptive Greed That Will Drive Decentralization & Generalized State Channels
Part One -
https://medium.com/blockchannel/the-redemptive-greed-that-will-drive-decentralization-generalized-state-channels-in-depth-part-666bd6244a28

- “There are several available resources, from Spankchain to Machinomy to Connext to Raiden to FunFair; it was hours of reading articles, listening to talks, and perusing code that finally made me understand that state channels have far more implications than the perceived simplicity of payment channels.”

Part Two -
https://medium.com/blockchannel/the-redemptive-greed-that-will-drive-decentralization-generalized-state-channels-in-depth-part-71ce68c28f85

Counterfactual: Generalized State Channels on Ethereum

https://medium.com/statechannels/counterfactual-generalized-state-channels-on-ethereum-d38a36d25fc6

- Diagram: https://cdn-images-1.medium.com/max/1000/1*tX0h-2gf62_-oqD1TjhyZg.jpeg
- White paper: https://counterfactual.com/statechannels
- "State channels are the foundational technology for useable distributed applications."

Features and Limitations of state channels

https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

- State channels rely on availability.
- They're particularly useful where participants are going to be exchanging many state updates over a long period of time.
- State channels are best used for applications with a defined set of participants.
- State channels have strong privacy properties
- State channels have instant finality

Plasma

August 11 2017 - Vitalik Buterin and Joseph Poon - Plasma: Autonomous Smart Contracts. http://plasma.io/plasma.pdf

- "Plasma takes the idea in a new direction, by allowing for the creation of "child" blockchains attached to the "main" ethereum blockchain. These child-chains can, in turn, spawn their own child-chains, who can spawn their own child-chains, and so on." https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4
- Diagram: https://cdn-images-1.medium.com/max/1000/0*44PC3oIBMgugPDph.

processes transactions "off-chain," i.e. not on the primary Ethereum blockchain. Plasma allows for many blockchains (called "child chains") to stem from the original blockchain (called the "root chain").

https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

"Imagine that you're creating a trading-card game on ethereum:

- First, we create a set of smart-contracts on ethereum main-chain that serve as the "Root" of our Plasma child-chain.
- Then, we create our child-chain. The child-chain can have its own consensus algorithm—in this example, let's say that it uses Proof of Authority (PoA), a simple consensus mechanism that relies on trusted block producers (i.e. validators).
- "Now that the child-chain is ready, we can create the basic components of our trading card game. The cards themselves are ERC721's (See below), initially created on the ethereum main-chain, and then moved onto the child-chain through the plasma root."

- “ Then, we deploy the actual game application smart-contracts on the child-chain, which contains all of the game logic and rules. When a user wants to play our game, they are only interacting with the child chain.”

Truebit

https://truebit.io/
White Paper: https://people.cs.uchicago.edu/~teutsch/papers/truebit.pdf

- A community cloud you can trust. Offer rewards in exchange for computational tasks, or get paid for providing correct solutions.
- Dogether. Add smart contract functionality to your cryptocurrency, or trade its tokens without an exchange.
- Scalable "on-chain" storage. Store data on Swarm http://swarm-gateways.net/bzz:/theswarm.eth/ or an external blockchain, and then use it as input for smart contracts.
- Increase transaction throughput. Build your own cryptocurrency with high transaction volume.
- Interact with miners like never before. Introducing smart contracts that can check any proof-of-work.
- Decentralized streaming video via Livepeer.
- Autonomous machine learning including the ArtDAO and vision-enabled smart contracts.
- Data marketplace. Trustless verification and remuneration for data models. See also Numerai and Ocean .
- Democratic Hypercatallaxy, Lexon, Consortium Chains, and other Mind-blowing combos.

Truebit is a technology to help ethereum conduct *heavy* or *complex* computation off-chain.

Raiden

Two nodes can open up a “state channel” between them, which is a two-way channel between users. “Messages”—in the form of transactions—occur between the two nodes and are signed by each party to ensure immutability.

- caveat is that nodes can only communicate with their “neighbors”

-

-

Web of Trust (WoT)

https://en.wikipedia.org/wiki/Web_of_trust
"Phil Zimmermann in 1992 in the manual for PGP version 2.0: As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers. And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures. This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys."

"I can create a (self-signed) certificate and have it signed by many of my friends, and they in turn could have their certificates signed by their friends, which if one were to draw these out as arrows between nodes each identifying a person, would form a graph, which they called The Web of Trust."
https://medium.com/@bblfish/on-twitter-bryan-ford-asked-the-following-question-f4fbd2b311be

PGP vs hyper-data Web of Trust -
https://medium.com/@bblfish/on-twitter-bryan-ford-asked-the-following-question-f4fbd2b311be

- the **#PGP** **#WebOfTrust** merges crypto & trust where the hyperdata WoT keeps them separate, relying for **#crypto** on other layers - https://twitter.com/bblfish/status/1008365149193990149
- PGP ties cryptography to the identity of the user, whereas in this proposal both are orthogonal. With PGP, the user must use his private key to sign or decrypt messages sent to him.
- We here rely on the TLS and DNS-SEC infrastructure to authenticate the servers and so the URL's served by that server. … Because the proposal is initially for a decentralised system, not a distributed one, and because we use a hyper-data framework, based on URLs, we can allow content to change over time.

From Digital Sovereignty to the Web of Nations
https://medium.com/cybersoton/from-digital-sovereignty-to-the-web-of-nations-61fbc28d79cd

- Diagram: https://cdn-images-1.medium.com/max/1250/1*P-XiTJaKafJSKdVlysYgFg.png - "the answer to the dilemma of Digital Sovereignty is for the states to bring the sovereign into the web, by building a web of institutional trust which Navigators can use in cyberspace."

Why did the PGP Web of Trust fail?
https://medium.com/@bblfish/what-are-the-failings-of-pgp-web-of-trust-958e1f62e5b7

- here is something very brittle and limited about the PGP format

- at some point the idea of Trusted Third Party tends to appear, which means that one reverts to relying on institutions which in any case one was already relying on, since it is those that give out passports, driving licenses,
- we need to be a lot more precise as to how we come to believe that someone has an attribute,
- each type of attribute requires a different verification skill… That is what an institutional web of trust would bring, since institutions are social knowledge machines. Diagram: https://cdn-images-1.medium.com/max/800/1*QPg86pi_dMRF_hmjBjCbqw.png
-

Internet of Things (IoT)

https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
This statistic shows the number of connected devices (Internet of Things; IoT) worldwide from 2015 to 2025. For 2020, the installed base of Internet of Things devices is forecast to grow to almost 31 billion worldwide. The overall Internet of Things market is projected to be worth more than one billion U.S. dollars annually from 2017 onwards.

- Includes chart

Trust and Security

https://blockchainhub.net/blockchain-oracles/
Oracles are third party services which are not part of the blockchain consensus mechanism. The main challenge with oracles is that people need to trust these sources of information. Whether a website or a sensor, the source of information needs to be trustworthy. Different trusted computing techniques can be used as a way of solving these issues. Providing smart contracts with trusted information sources is crucial for the users because in case of mistakes there are no rollbacks.

Oraclize

http://www.oraclize.it/
“We act as a data carrier, a reliable connection between Web APIs and your Dapp. There is no need to open additional trustlines as our good behaviour is enforced by cryptographic proofs.”

- GitHub - http://github.com/oraclize
- API - http://docs.oraclize.it/

Companies like Oracalize, for example, have been leveraging Amazon with the TLSNotary-based proofs.

TLSNotary - https://tlsnotary.org/

- Based on an original algorithm as described in the whitepaper.
- Provides cryptographic proof without MITM-ing your connection.
- Install the Firefox/Chrome app PageSigner, start proving pages with one click.
- No need to give login credentials to a third party.

Town Crier

http://www.town-crier.org/
Town Crier system is an authenticated data feed for smart contracts, a.k.a. an "oracle." It was created by students and faculty at The Initiative for CryptoCurrencies and Contracts (IC3).

- Diagram - http://www.town-crier.org/theme/images/oracle.png

The Town Crier paper is published at CCS'16.

- The conference version is available online.
- An extended version with more technical details and examples is on IACR ePrint.

Town Crier, another company, is focusing on the utilization of the Intel Software Guard Extensions (SGX).

Chainlink

https://chain.link/
A startup called Chainlink is combining its software with a trusted hardware system called Town Crier

- “by working together, the two systems can allow blockchain-based services to interact with real-world events with a greater degree of trust than is possible from today’s oracle services.” https://www.technologyreview.com/s/612443/blockchain-smart-contracts-can-finally-have-a-real-world-impact/

Further Reading

Hardware Oracles: bridging the Real World to the Blockchain
Understanding oracles
A visit to the oracle
Smart Contract Oracles
Can oracles send data to smart contracts on multiple blockchains?
How can an Ethereum contract get data from a website?
Why Many Smart Contract Use Cases Are Simply Impossible?
1,749,693 blocks later, Oracalize
SchellingCoin: A Minimal-Trust Universal Data Feed, Vitalike Buterin
Town Crier: An Authenticated Data Feed for Smart Contracts:Scientific paper

Web3

Origin - http://gavwood.com/web3lt.html - 2014 - static content publication, dynamic messages, trustless transactions and an integrated user-interface.

“Web3 generally refers to the next generation of the worldwide web. It has been adopted by the Ethereum ecosystem and co-opted to refer to a decentralised web. Put simply then, web3 is web2 without the centralised servers and data silos. If everything goes to plan, web3 will just become part of the web and web3 developers will become web developers again.
In time, decentralised architecture will simply become an infrastructure choice, just like MongoDB vs Firebase or REST vs GraphQL is today—your EC2 instance might be replaced by Ethereum and your static assets could be stored on Swarm.”
https://hackernoon.com/crossing-over-to-web3-an-introduction-to-decentralised-development-5eb09e95edb0

---

https://medium.com/l4-media/making-sense-of-web-3-c1a9e74dcae
“Web 3 is different from previous generational shifts. At its core, web 3 isn’t about speed, performance, or convenience. In fact, many web 3 applications are, at least today, slower and less convenient than existing products.
Instead, web 3 is about power. It’s about who has control over the technologies and applications that we use every day. It’s about breaking the dynamic that has shaped the last decade of the web: the tradeoff between convenience and control. We’ve become so accustomed to this dynamic that it seems inevitable: of course using the internet means being surveilled, and of course having a social media account means having my personal data sold to advertisers or worse. How could it be any other way? Web 3 rejects the premise. We can have the benefits of the internet without handing the majority of power to a minority of companies. The dynamic described above isn’t an iron law of the universe, it’s just a product of the technology available at the time and the choices we made along the way.
“Web 3” is a movement to build different technologies and make better choices. We aren’t trying to replace the web, but rather keep what we like while changing its underlying structure—a reformation, not a revolution.”

Three trends for web 3
In this article we survey three trends, and discuss how they might develop over time:

- First, money will become a native feature of the internet.
- Second, “decentralized” applications will offer users new capabilities.
- Third, users will have more control over their digital identities and data.

---

web3.js - Ethereum JavaScript API - https://web3js.readthedocs.io/en/1.0/ - “web3.js is a collection of libraries which allow you to interact with a local or remote ethereum node, using a HTTP or IPC connection.”

- Crossing Over to Web3—An Introduction to Decentralised Development - https://hackernoon.com/crossing-over-to-web3-an-introduction-to-decentralised-development-5eb09e95edb0

https://media.consensys.net/how-blockchain-is-helping-technology-get-its-soul-back-a2d6cf96a272
“Web3, as this hyper-collaborative and rearchitected Internet is being called, is not being built by the tech community, or out of any of the old conduits (Wall Street, San Francisco, Hong Kong, London), but by pockets of forward-thinking and critically-minded engineers, entrepreneurs, policy makers, regulators, humanitarians, and artists from all points of the compass: Denver, Toronto, Berlin,

Johannesburg, Kiev, Manila, Bushwick. A better word for this community is *ecosystem*—it is diverse, emergent, self-organized, healthily competitive, hungry for feedback, resilient, and highly energetic."

Understanding Web 3—A User Controlled Internet
https://blog.coinbase.com/understanding-web-3-a-user-controlled-internet-a39c21cf83f3
Today's world wide web, or the internet, has two key missing properties:

It doesn't hold "state", independent of trusted operators
It doesn't have a native mechanism to transfer state

Fission

https://fission.codes/

- Vancouver
- "the foundation for bringing interoperability and re-use to the entire Web3 Stack."

Coins

http://www.europarl.europa.eu/cmsdata/149900/CASE_FINAL%20publication.pdf p.10
Table 1: Top five VCs by market capitalisation, April 2018 (in US$)
No. / Name / Symbol / Market capitalisation / Unit price / Circulating supply / Volume (24h)
1 Bitcoin BTC $141,230,856,668 $8,313.26 16,988,625 $7,096,370,000
2 Ethereum ETH $56,442,400,865 $570,51 98,933,063 $2,469,830,000
3 Ripple XRP $32,984,545,806 $0.84 39,122,794,968 $1,688,280,000
4 Bitcoin Cash BCH $16,639,053,113 $973.98 17,083,550 $740,993,000
5 Litecoin LTC $8,186,324,143 $145.76 56,164,963 $439,487,000
Source: https://coinmarketcap.com, date of access: 20 April 2018

Approximately 600 to 800 Cryptocurrencies are now Dead

Dead Coins, lists approximately 637 cryptocurrency projects that demonstrate crypto death: have failed to maintain nodes, been abandoned by developers, scammed, or hacked. The CNBC story listed 800.

Bitcoin

Bitcoin: A Peer-to-Peer Electronic Cash System white paper by Satoshi Nakamoto

Bitcoin Forum
https://bitcointalk.org/

Bitcoin Wiki
https://en.bitcoin.it/wiki/Main_Page

https://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf
"In essence, a bitcoin is an electronic token without reference to any underlying commodity or sovereign currency, and is not a liability on any balance sheet."
"the entities transact directly, that is, in contrast to most traditional payment systems where various parties, such as banks, processors, and networks, sit between the payor and payee, there is no designated intermediary in Bitcoin. Each transaction is chronologically recorded in a public ledger, called the blockchain, by participants in the network."

Explained in 5 Minutes: Bitcoin
https://docs.google.com/document/d/1DX5nYbkd5mQ81xrLggovceIkE43rCFrOMbFLYUkBhZQ/edit

How Does Bitcoin Work?
https://medium.com/the-crypto-times/how-does-bitcoin-work-256a69823aca

- Decentralization. There is no central entity governing the system. Every participant of the network contributes to keeping it alive. This removes security holes, because even if a single, big party gets hacked, the other members of the network aren't affected and the overall system recovers.
- Shared memory. A record of all transactions between all parties on the blockchain is stored on every computer in the network. Forever. And everyone can see it. This makes the network secure against fraud and data loss.
- Cryptography. Through a set of complex algorithms and math problems, all transactions and participants are protected by encryption.

When will Bitcoin go up?
https://medium.com/@altcoininvestor/when-will-bitcoin-go-up-36098c50bffb
There are some amazing new ICO's being developed in areas that will increase the throughput between the existing financial markets.

- Asset Backed Cryptocurrencies: This new breed of cryptocurrencies will bring with it potentially hundreds of millions of dollars of (real) assets into the marketplace.
- Decentralized Exchanges (DEX): Since these exchanges don't physically reside anywhere, they will likely avoid jurisdictional regulations.
- P2P Exchange Networks: Increasingly Bitcoin ATM's, and new ICO's offering Peer-to-Peer exchange networks, offering more opportunities for buyers and sellers or cryptocurrency worldwide.

Bitcoin vs The Rest

Opinion: Bitcoin, not the Blockchain
https://www.ccn.com/opinion-bitcoin-not-the-blockchain/#Blockchain

As to me there is a key difference between Distributed Ledger Technology (DLTs) and blockchains, so many technologists and marketers keep forgetting: the actual monetary incentive that keeps this database operating in a decentralized manner. (Good article, lots of detail)

-

Nodes

Currently 115,000 nodes. Bitcoin nodes: image : https://cdn-images-1.medium.com/max/750/1*Vqx4gepjkozP1vL4lhILrw.png

“Each node here has 8 connections to other nodes, because this is the default amount of connections the client makes without any changes made to it. My node is in here somewhere, and if you’re running one, it’s in there too. Coinbase’s nodes are in there, Bitmain’s nodes are in there, and if Satoshi is still around, Satoshi’s node is in there too.”

The nodes “they all check the entire chain to make sure each and every transaction and block follow the rules.””

“When I create a transaction and “send it out to the world”, it’s actually only going to these 8 peers. Since Bitcoin is designed from the ground up to make every node a fully validating node, when these 8 nodes receive my transaction they check to see if it’s valid before sending it out to *their* 8 peers.”

- Bitcoin blockchain “not fit for purpose” for the financial sector - Charley Cooper (managing director, R3) - video https://www.youtube.com/watch?v=R0iArSIU0Z8&feature=youtu.be&t=47m16s 1:09:00

Transactions

https://hackernoon.com/getting-deep-into-ethereum-how-data-is-stored-in-ethereum-e3f669d96033
Bitcoin’s “state” is represented by its global collection of Unspent Transaction Outputs (UTXOs).... The UTXO system in bitcoin works well, in part, due to the fact that digital wallets are able to facilitate most of the tasks associated with transactions. Including but not limited to:

a) handling UTXOs
b) storing keys
c) setting transaction fees
d) providing return change addresses
e) aggregating UTXOs (to show available, pending and total balances)

One analogy for the transactions in the UTXO model is paper bills (banknotes). Each account keeps track of how much money it has by adding up the amount of bills (UTXOs) in the purse (associated with this address/wallet). When we want to spend money, we use one or more bills (existing UTXOs), enough to cover the cost and maybe receive some change back (new UTXO). Each bill can only be spent once since, once spent, the UTXO is removed from the pool.

To summarize, we know that:

- the bitcoin blockchain does not hold account balances
- bitcoin wallets hold keys to UTXOs
- if included in a transaction, an entire UTXO is spent (in some cases partially received back as "change" in the form of a brand new UTXO)

Bitcoin as Social Contract

Unpacking Bitcoin's Social Contract
https://medium.com/s/story/bitcoins-social-contract-1f8b05ee24a9
That social contract framework can be used to answer some essential questions: Why did bitcoin come into existence? Who decided its properties? Who controls it today? Can a critical bug kill bitcoin?

Colored Coins

The term "Colored Coins" loosely describes a class of methods for representing and managing **real world assets** on top of the Bitcoin Blockchain.
While originally designed to be a currency, Bitcoin's scripting language allows to store small amounts of metadata on the blockchain, which can be used to **represent** asset manipulation instructions.

Light Clients

"Various light-clients exist for the desktop, and for your mobile phone. Some of them are Electrum, Armory, Bread, and Samourai Wallet. Light-clients tether to a specific node."
https://medium.com/@StopAndDecrypt/bitcoin-miners-beware-invalid-blocks-need-not-apply-51c293ee278b

Bitcoin Private

https://medium.com/@bitcoinprivate/community-update-10-our-plans-for-proof-of-work-d6b828f321c5
"In order to accommodate a PoW algorithm change in the most efficient and least disruptive way possible, Bitcoin Private will be changing our PoW through a hard fork that coincides simultaneously with the launch of the rebase."
"Rebasing Bitcoin Private off of the Bitcoin codebase will allow us to maintain complete and ongoing feature parity with Bitcoin and any of its future innovations."

Forks

Bitcoin May Split 50 Times in 2018 as Forking Craze Accelerates
https://medium.com/bloomberg/bitcoin-may-split-50-times-in-2018-as-forking-craze-accelerates-6a044fd4cd
“forking may soon sideline a more popular alternative, initial coin offerings, in which startups raise money by selling entirely new tokens.”

Bitcoin Lightning

https://lightning.network/
Lightning is a decentralized network using smart contract functionality in the blockchain to enable instant payments across a network of participants.
Summary paper: https://lightning.network/lightning-network-summary.pdf
White Paper: https://lightning.network/lightning-network-paper.pdf

“Bitcoin also has a *payment channel* network *(lightning)* layered on top of it that doesn’t effect the structure of the blockchain network.”
https://medium.com/@StopAndDecrypt/bitcoin-miners-beware-invalid-blocks-need-not-apply-51c293ee278b

- The specification was announced after the paper, and is being developed by multiple parties, including Elements Project (*c-lightning*, depending on Bitcoin Core/bitcoind), Lightning Labs (*lnd*, depending on btcsuite/btcd or Bitcoin Core/bitcoind), and ACINQ (*eclair*, depending on Bitcoin Core/bitcoind).
- The specification is available on Github, and its largest contributor is Rusty Russell of Blockstream.[3]

“The **Lightning Network** is a "second layer" payment protocol that operates on top of a blockchain (most commonly Bitcoin). It enables instant transactions between participating nodes and has been touted as a solution to the bitcoin scalability problem. It features a peer-to-peer system for making micropayments of digital cryptocurrency through a network of bidirectional payment channels without delegating custody of funds.” https://en.wikipedia.org/wiki/Lightning_Network

https://lightning.network/lightning-network-paper.pdf
“it is possible in bitcoin to devise a bitcoin script whereby
all old transactions are invalidated, and only the new transaction is valid.
Invalidation is enforced by a bitcoin output script and dependent trans-
actions which force the other party to give all their funds to the channel
counterparty. By taking all funds as a penalty to give to the other, all old
transactions are thereby invalidated. Conceptually, this system is
not an independent overlay network; it is more a deferral of state on the
current system, as the enforcement is still occurring on the blockchain itself
(albeit deferred to future dates and transactions).

https://www.coindesk.com/bitcoin-lightning-payments-slowly-becoming-less-reckless/
lightning network, which pushes transactions into off-chain payment channels, allowing the cryptocurrency to be received without waiting for a block to be mined or paying the associated miner's fees, has moved ahead by leaps and bounds in the past few months.

- Lightning Labs, the company behind the "lnd" implementation of the lightning network, recently published a blog post envisioning non-techy end-user Carol buying a pair of socks using lightning as easily as if she were swiping a credit card.
- lnd wallet for iOS called Zap; the lightning wallet, HTLC.me, developed by well-known developer Alex Bosworth; and another iOS wallet for lightning, called CoinClip, released by developer Kenneth Perry, aka thothonegan.

- Today, revoking old state is accomplished with the "L2-penalty" model – whereby a lightning wallet or node stores all of these intermediary states, then, if someone tries to broadcast an earlier, now-invalid state, this is detected and the cheating user is punished by losing money. https://www.coindesk.com/new-twist-lightning-tech-coming-soon-bitcoin/

- Lightning Labs co-founder 'Laolu' Osuntokun and Blockstream's Christian Decker and Rusty Russell – have published a new proposal which imagines an alternative, "simplified" way of making off-chain transactions called eltoo.
  https://www.coindesk.com/new-twist-lightning-tech-coming-soon-bitcoin/
- Image of the litghn ing stack - https://media.coindesk.com/uploads/2018/05/lightning_stack-e1525979378565.png

Them Lightning Network Nodes Sure Do Look Centralized To Me! What Gives?
https://hackernoon.com/them-lightning-network-nodes-sure-do-look-centralized-to-me-what-gives-ee39c9b12ac0
Image: https://cdn-images-1.medium.com/max/800/1*39nCG6qnJISkl_dMz6TrpQ.png
Image: https://cdn-images-1.medium.com/max/800/1*i58ZbxOCSYEZujuh-q2p6Q.png
“People are getting mislead by their eyes, and the kinds of people that get mislead this way are susceptible to coming back around when their eyes are shown the same information in a different way.”

Payment Channels

- which allow for fast, low-cost transactions that leverage the security of an underlying blockchain https://blog.lightning.engineering/posts/2018/05/02/lightning-ux.html

Hash-Time Locked Contracts (HTLC)

- within payment channels, Lightning uses a form of “smart contract”, which is a cryptographically secured promise to deliver funds. Lightning’s primary contract is the Hash Time Locked Contract (HTLC), which is enforced by the bitcoin blockchain. HTLCs allow for Lightning payments to be sent across multiple channels (a multi-hop payment). More information about payment channels and HTLCs can be found in this article.

https://blog.lightning.engineering/posts/2018/05/02/lightning-ux.html

Routing Nodes

- https://blog.lightning.engineering/posts/2018/05/02/lightning-ux.html A routing node is a computer intended to be online at all times, and that facilitates the sending of payments for other users.
    - B is connected to the network via its own set of routing nodes.
    - Through a process that's analogous to finding connections between people in "Six Degrees of Separation," a Lightning App automatically determines which nodes link her with B, and Carol's transaction is sent across that series of links.

Watchtowers

- https://blog.lightning.engineering/posts/2018/05/02/lightning-ux.html
- Watchtowers provide protection in case something goes wrong

[watchtower/lookout]: on-chain breach monitoring
https://github.com/lightningnetwork/lnd/pull/2124
" watchtower/lookout package, which handles the responsibility of monitoring the chain for possible breaches and responding by decrypting and broadcasting any justice transactions that its clients had previously uploaded. Together with the watchtower/server, which receives and stores encrypted blobs from clients, this represents that second primary service enabling the tower to act on behalf of the tower's clients."

Splicing

- "splicing", which allows for an on-chain payment out of a channel without requiring that the channel itself be closed. Splicing allows for a seamless transition between on-chain and off-chain (Lightning) transactions.

Atomic Multipath Payments (AMP)

- AMP allows large payments to be split into multiple small payments, each of which is sent via a different route through the network.
- - Diagram: https://blog.lightning.engineering/assets/images/lightning_network.png

Bitcoin Cash

- https://www.bitcoincash.org/
- Hard fork of Bitcoin

- Wait, Bitcoin Just Did What?
    - https://www.technologyreview.com/s/608483/wait-bitcoin-just-did-what/
    - The digital currency has split into two. What that means will depend on what the miners do. August 1, 2017

- Bitcoin Cash forks again - 11-2018
    - https://www.bloomberg.com/news/articles/2018-11-16/bitcoin-cash-clash-is-costing-billions-with-no-end-in-sight?srnd=cryptocurrencies - two competing software-development teams failed to agree on how to best update the code and ended up splitting the network.

- The resolution of the Bitcoin Cash experiment - https://medium.com/@_unwriter/the-resolution-of-the-bitcoin-cash-experiment-52b86d8cd187 -- Bitcoin ABC vs Bitcoin SV

- This week, several major exchanges announced plans to remove support for, or "delist," a currency called Bitcoin SV (for "Satoshi's vision"), which Wright helped create last November via a hard fork of Bitcoin Cash.
-

Ethereum

"Bitcoin is the Digital Gold but Ethereum is the Silicon" https://medium.com/@Michael_Spencer/bitcoins-glory-days-over-the-future-of-blockchain-5fe303f18537

The founder of Ethereum, Vitalik Buterin, published the idea of Ethereum in late 2013 in a whitepaper. in July 2015, Ethereum went live. in July 2015, Ethereum went live.

"Ethereum, developed by a Swiss non-profit the Ethereum Foundation. (Its founder, Vitalik Buterin, dropped out of Waterloo University and received a $100,000 Thiel Fellowship for his work on the project.)" https://hackeducation.com/2016/04/07/blockchain-education-guide

Gavin Wood: The Yellow Paper: http://gavwood.com/Paper.pdf

1. Ethereum for Dummies by Dr. Gavin Wood [CTO, Ethereum]
2. Ethereum explained in 100 seconds [Gavin & Vitalik]
3. What is Ethereum? [slides from Ethereum team]

Three original implementations:
- C++
- Python
- Go - https://github.com/ethereum/go-ethereum
    - Client: Geth - https://geth.ethereum.org/install

What is Ethereum - https://kingpassive.com/what-is-ethereum/

- "while Bitcoin's blockchain just stores transaction records, Ethereum's blockchain also hosts smart contracts and decentralized applications (DApps)."
- "Smart contracts are contracts programmed to run by themselves. In simple terms, this means: If x happens, y results."

"Of the top 100 tokens by market cap, 94% are built on top of Ethereum. Of the top 800 tokens, 87% are built on Ethereum. Most of these tokens are "ERC-20 tokens," which made possible the majority of the $5.5 billion raised through token sales in 2017 and the $6.5 billion raised in just the first quarter of this year." https://media.consensys.net/the-state-of-the-ethereum-network-949332cb6895

Ethereum for Dummies - https://hackernoon.com/ethereum-for-dummies-af5aeacb13d4

Everything You Possibly Need to Develop on Ethereum
https://media.consensys.net/everything-you-possibly-need-to-develop-on-ethereum-1bef0c23c7c6
"From us to you, here's a comprehensive and crowdsourced list of (nearly) all the best Ethereum developer platforms, services, tools, and infrastructure."

Ethereum, for Earthlings
https://hackernoon.com/ethereum-for-earthlings-e12ec293011a
a.k.a. How To Understand Ethereum Without Traumatizing Your Brain

Storing Data

Getting Deep Into Ethereum: How Data Is Stored In Ethereum?
https://hackernoon.com/getting-deep-into-ethereum-how-data-is-stored-in-ethereum-e3f669d96033

https://hackernoon.com/getting-deep-into-ethereum-how-data-is-stored-in-ethereum-e3f669d96033
Ethereum is a transaction-based "state" machine; a technology on which all transaction based state machine concepts may be built.

- Diagram - https://cdn-images-1.medium.com/max/800/1*f0yOn0lRgrY5NjFlbUMBFg.jpeg

The record-keeping for Ethereum is just like that in a bank. An analogy is using an ATM/debit card. The bank tracks how much money each debit card has, and when we need to spend money, the bank checks its record to make sure we have enough balance before approving the transaction.

There is one, and one only, global state trie in Ethereum. This global state trie is constantly updated. The state trie contains a key and value pair for every account which exists on the Ethereum network. The "key" is a single 160 bit identifier (the address of an Ethereum account). The "value" in the global state trie is created by encoding the following account details of an Ethereum account (using the Recursive-Length Prefix encoding (RLP) method):

- nonce
- balance
- storageRoot
- codeHash

- Diagram - https://cdn-images-1.medium.com/max/800/1*-Q00GpGTphTOtBWPRu1e3g.png

- The main Ethereum clients use two different database software solutions to store their tries. Ethereum's Rust client Parity uses rocksdb. Whereas Ethereum's Go, C++ and Python clients all use leveldb.

Mining Ether

- The way that miners verify Ethereum transactions is via "proof of work". However, they are planning to move towards "proof of stake". - https://kingpassive.com/what-is-ethereum/
-

Gas Limits

"In Ethereum, gas is a measure of computational effort. To each operation, a fixed amount of gas is assigned (e.g. adding two numbers costs 3 gas, calculating a hash costs 30 gas, sending a transaction costs 21000 gas [1])."
https://bitcoin.stackexchange.com/questions/39132/what-is-gas-limit-in-ethereum

See the Yellow paper , p.4, p. 7

Nodes

Geth

Setting up an Ethereum node
https://harrydenley.com/setting-up-an-ethereum-node/

- Go - https://github.com/ethereum/go-ethereum
    - Client: Geth - https://geth.ethereum.org/install
-

http://www.talkcrypto.org/blog/2018/01/23/what-is-geth/
Geth is a multipurpose command line tool that runs a full Ethereum node implemented in Go. It offers three interfaces: the command line subcommands and options, a Json-rpc server and an interactive console.

Frameworks

Decentralized Applications (dApps) are the primary selling point of the Ethereum blockchain - A site that tracks dApp development lists 1,552 launched dApps, though more are currently in development. DApps consist of everything ranging from prediction markets to gaming, and will continue to grow stronger as the network is improved upon.

1573 today (June 4, 2018) https://www.stateofthedapps.com/

Meteor

- https://www.meteor.com/ - framework for building JS apps generally
  - Developers Guide - https://www.meteor.com/developers
  - DApp using Meteor - https://github.com/ethereum/wiki/wiki/Dapp-using-Meteor
  - Truffle vs Meteor - https://ethereum.stackexchange.com/questions/18751/truffle-vs-meteor
  - https://medium.com/hci-wvu/how-to-build-your-first-%C3%B0app-fe0c89d8f95f
  -

Casper

Casper the Friendly Ghost -
https://github.com/ethereum/research/blob/master/papers/CasperTFG/CasperTFG.pdf

Casper the Friendly Finality Gadget -
https://arxiv.org/pdf/1710.09437.pdf
“Casper the Friendly Finality Gadget is an overlay atop a proposal mechanism—a mechanism which proposes blocks. Casper is responsible for finalizing these blocks, essentially selecting a unique chain which represents the canonical transactions of the ledger.”

“several new features that BFT algorithms do not necessarily support:

- If a validator violates a rule, we can detect the violation and know which validatorviolated the rule. Accountability allows us to penalize malfeasant validators
- Dynamic validators - . We introduce a safe way for the validator set to change over time
- We introduce defenses against long range revision attacks as well as attacks where more than ⅓ of validators drop offline,
- Modular overlay

Scaling Solutions

The State of Scaling Ethereum
https://media.consensys.net/the-state-of-scaling-ethereum-b4d095dbafae
"One theory of blockchain technology is that a network can only support two of the following: security, decentralization, and scalability."

Approaches:
- Sharding
- Off-Chain - eg. Plasma, Raiden
- Proof-of-Stake - Casper

Scaling solutions for the Ethereum network are numerous, and are being worked on by multiple participants in the network.

- Cosmos is a permissionless network built for developers that allows blockchain interoperability and scaling. -- "Cosmos is a decentralized network of independent parallel blockchains, each powered by classical BFT consensus algorithms like Tendermint." - https://cosmos.network/ --- Cosmos is a bit like a mesh rather than a chain
    - Cosmos 'internet of blockchains' blog - https://blog.cosmos.network/

- Loom Network - https://loomx.io/
    - https://medium.com/loom-network/everything-you-need-to-know-about-loom-network-all-in-one-place-updated-regularly-64742bd839fe
    - The Loom SDK generates what's called a *DAppChain*—**a layer-two blockchain that uses Ethereum as its base-layer.**
    - CryptoZombies, a live app enabling anyone to learn to code smart contracts on Ethereum (with over 200,000 students). (Loom Network has developed and launched a layer 2 platform on top of Ethereum, allowing gaming and social dApps to scale while still relying on Ethereum's core security and decentralization.)

- OmiseGo allows users to send high-speed payment transactions between entities and across borders using plasma.

Token Standards

Laying the Track for the Internet of Value
Whether or not you really need a blockchain today, times are changing. Countless services are popping up on blockchains like Ethereum. Billions of connections between parties all over the world are surging as networks evolve to handle the load. And standards like ERC20 and ERC721 are making transactions, logic and data models compatible with each other by design.
https://media.consensys.net/the-value-of-being-stupid-about-blockchain-c46ba3c99cd6

- ERC-20: A CLASS OF IDENTICAL TOKENS
- ERC-721: A CLASS OF UNIQUE TOKENS

ERC-20

https://theethereum.wiki/w/index.php/ERC20_Token_Standard
ERC20 is a technical standard used for smart contracts on the Ethereum blockchain for implementing tokens. *ERC* stands for *Ethereum Request for Comment*, and *20* is the number that was assigned to this request. The clear majority of tokens issued on the Ethereum blockchain are ERC20 compliant.
https://en.wikipedia.org/wiki/ERC20

ERC-721

ERC-721 is a free, open standard that describes how to build non-fungible or unique tokens on the Ethereum blockchain. While most tokens are fungible (every token is the same as every other token), ERC-721 tokens are all unique. Think of them like rare, one-of-a-kind collectables. http://erc721.org/

Non-fungible token standard - slides - https://www.slideshare.net/PriyabrataDash2/erc-721-tokens
"Defining Fungibility • When a set of assets all have equal value to each other, they are defined as fungible. As an example, a US dollar has the same value as any other US dollar. … A non-fungible asset, however, is not equal to its counterparts. The most tangible example of a non-fungible asset is any sort of collectible. A baseball is just a baseball until it is signed by Babe Ruth. Then, it gains additional value and becomes a non-fungible asset, valued differently than all other baseballs out there."

"there are various cases when you need to have unidentical tokens, which are used within the platform, and add some extra parameters and price them differently. • For instance, we could have a token which represents some part of real estate object, and each token might have some different parameters added to it. • Such standard would make it easy to create marketplaces for multiple non-fungible token types."

"As the explosion of CryptoKitties has demonstrated, ERC-721 tokens will usher in a world of crypto-collectibles, where people recognize unique scarcity on the blockchain just as they do in the physical world. "

https://medium.com/crypto-currently/the-anatomy-of-erc721-e9db77abfc24
ERC721 tokens can be used in any exchange, but their value is a result of the uniqueness and rareness associated with each token. The standard defines the functions name , symbol , totalSupply , balanceOf , ownerOf , approve , takeOwnership , transfer , tokenOfOwnerByIndex , and tokenMetadata . It also defines two events: Transfer and Approval .

Reference •
https://medium.com/crypto-currently/the-anatomy-of-erc721-e9db77abfc24
https://ethereum.stackexchange.com/questions/36394/how-to-create-your-own-erc-721-nft-token
Please refer the reading list for the ERC 721 token in the link below for more reference:
https://medium.com/crypt-bytes-tech/reading-list-erc-721-nft-token-standard-7524b64ef5df

Jumping into Solidity —The ERC721 Standard
Part 1 -
https://medium.com/coinmonks/jumping-into-solidity-the-erc721-standard-part-1-e25b67fc91f3
Part 2 -
https://medium.com/coinmonks/jumping-into-solidity-the-erc721-standard-part-2-383438734de5
Part 3 -
https://medium.com/coinmonks/jumping-into-solidity-the-erc721-standard-part-3-5f38e012248b
Part 4 -
https://medium.com/coinmonks/jumping-into-solidity-the-erc721-standard-part-4-ad21e3a5d9c
Part 5 -
https://medium.com/coinmonks/jumping-into-solidity-the-erc721-standard-part-5-3b91f39fc1ee
Part 6 -
https://medium.com/coinmonks/jumping-into-solidity-the-erc721-standard-part-6-7ea4af3366fd
Part 7 -
https://medium.com/coinmonks/jumping-into-solidity-the-erc721-standard-part-7-9aca1411375a

ENS - Ethereum Name Service

http://ens.readthedocs.io/en/latest/introduction.html

The primary goal of ENS is to resolve human-readable names, like 'myname.eth', into machine-readable identifiers, including Ethereum addresses, Swarm and IPFS content hashes, and other identifiers. A secondary purpose is to provide metadata about names, such as ABIs for contracts, and whois information for users.

Swarm uses the Ethereum Name Service (ENS) to resolve domain names to Swarm hashes.

Terminology

- domain - the complete, human-readable form of a name; eg, 'vitalik.wallet.eth'.
- label - a single component of a domain; eg, 'vitalik', 'wallet', or 'eth'. A label may not contain a period ('.').
- label hash - the output of the keccak-256 function applied to a label; eg, keccak256('eth') = 0x4f5b812789fc606be1b3b16908db13fc7a9adf7ca72641f84d75b47069d3d7f0.
- node - the output of the namehash function, used to uniquely identify a name in ENS.

Ethereum Profiles

"Ethereum Profiles makes it simple for users to create a reusable profile for their Ethereum address which can easily be shared with dapps to simplify the onboarding experience and create a more frictionless, social web3 dapp ecosystem. Ethereum Profiles allows Ethereum users to collect and

control their information on the distributed web using their existing Ethereum wallets.” - https://medium.com/3box/announcing-ethereum-profiles-1-0-0-is-live-f0316e15ce23

3Box

https://github.com/uport-project/3box

- Create your Ethereum Profile on 3Box.io - https://alpha.3box.io/
- Dapp developers can use the **Ethereum Profiles API** to easily read and update users’ profiles without needing to store information on the blockchain or a central server. We’re now on 3Box.js version 1.0.0.
- 3Box data is stored on IPFS and managed in OrbitDB instances
- The 3Box app (https://3box.io) allows you to create and manage your Ethereum profile. Access the 3Box app from any web3 Ethereum browser. (ie., requires Metamask)

Networks

Rinkeby

https://www.rinkeby.io/#stats
Test network

Smart Contracts

Encoding

Solidity

-
- “**Solidity** is a contract-oriented programming language for writing smart contracts.[1] It is used for implementing smart contracts[2] on various blockchain platforms.” https://en.wikipedia.org/wiki/Solidity
-
- Ethereum uses its own programming language, Solidity. Developers’ unfamiliarity with Solidity has led to code being written incorrectly, which led to problems like The DAO hack. https://kingpassive.com/what-is-ethereum/

Announcing our Fully Featured, Portable Solidity Debugger
https://truffleframework.com/blog/announcing-full-portable-solidity-debugger

Verification

Zeus

Zeus: Analyzing safety of smart contracts
http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2018/02/ndss2018_09-1_Kalra_paper.pdf

https://www.youtube.com/watch?v=X1_CoaIQ0SU

Summary: https://blog.acolyer.org/2018/03/08/zeus-analyzing-safety-of-smart-contracts/

Security

Securify

https://securify.ch

Securify: practical security analysis of smart contracts
https://arxiv.org/pdf/1806.01143.pdf

Summary:
https://blog.acolyer.org/2018/12/03/securify-practical-security-analysis-of-smart-contracts/
`Securify uses a set of expert heuristics (patterns) to help identify issues in smart contracts.

Ethereum Classic

After the Dao attack (see security, below) split of Ethereum into Ethereum (forked blockchain) and Ethereum Classic (unchanged blockchain). https://kingpassive.com/what-is-ethereum/

(after ther fork)

- Ethereum Classic spiked 25 percent on the news that it will be listed on Coinbase. (CoinDesk)

Robinhood Adds Ethereum Classic to Crypto Trading App
https://www.coindesk.com/robinhood-adds-ethereum-classic-to-crypto-trading-app/

Libra

https://developers.libra.org/

- Libra: the Path Forward - https://developers.libra.org/blog/2019/06/18/the-path-forward
- Libra bug bounty open to all - https://developers.libra.org/blog/2019/08/14/libra-bug-bounty

Facebook's involvement

- Coinbase's Ex-Policy Head Will Lobby for Facebook's Libra Crypto - https://www.coindesk.com/coinbases-ex-policy-head-will-lobby-for-facebook-amid-libra-crypto-pushback
- Facebook's Libra: Three things we don't know about the digital currency - https://www.technologyreview.com/s/613801/facebooks-libra-three-things-we-dont-know-about-the-digital-currency/

Criticisms of Libra

- The fight over Facebook's digital currency could change the face of banking - https://www.technologyreview.com/s/613977/the-fight-over-facebooks-libra-could-change-the-face-of-banking/
- U.S. lawmaker says still concerned about Facebook cryptocurrency after Swiss meetings - https://www.reuters.com/article/us-facebook-cryptocurrency/u-s-lawmaker-says-still-concerned-about-facebook-cryptocurrency-after-swiss-meetings-idUSKCN1VF0YJ
- Libra Association's Crypto Members Remain Unfazed by Regulatory Backlash - https://www.coindesk.com/libra-associations-crypto-members-remain-unfazed-by-regulatory-backlash
- Crypto Lobby Fights to Contain Backlash From Facebook's Libra - https://www.bloomberg.com/news/articles/2019-08-28/crypto-lobby-fights-to-contain-backlash-from-facebook-s-libra
- Facebook's Libra should be blocked in Europe, France says - https://www.bbc.com/news/business-49677146

Gram

the "Gram." The currency, which is being developed by Telegram, the popular messaging service, is apparently on track to launch before the end of October.

Telegram Open Network (TON), the blockchain system that would run the currency.

- Telegram Pushes Ahead With Plans for 'Gram' Cryptocurrency - https://www.nytimes.com/2019/08/27/technology/telegram-cryptocurrency-gram.html

- Telegram's ICO: Give us $2 billion and we'll solve all of blockchain's problems - https://www.technologyreview.com/s/610055/telegrams-ico-give-us-2-billion-and-well-solve-all-of-blockchains-problems/

Ripple

- network that bills itself as using blockchain technology to enable individuals, banks, and payment providers to exchange payments globally
- Ripple owns the cryptocurrency XRP.
-

Ripple has a network of banks around the world on its platform. International payments can be processed by participating banks within three to five seconds, rather than two to five days, it says.
https://www.therecord.com/news-story/8653190-uw-gets-research-funding-for-deep-dive-into-blockchain-technology/

https://www.nytimes.com/2018/07/01/technology/cryptocurrency-ripple.html
Ripple's recent efforts to promote its crypto-token, XRP, may actually hurt its case that the token is not a security.

Bitcoin vs Ripple
https://www.finder.com/bitcoin-vs-ripple

http://www.europarl.europa.eu/cmsdata/149900/CASE_FINAL%20publication.pdf
"The business goal of the creators of Ripple is that it will replace SWIFT as a global provider of secure financial messaging services" (Swift: The Society for Worldwide Interbank Financial Telecommunication. See www.swift.com)

Ripple: not a cryptocurrency
https://hackernoon.com/ripple-not-a-cryptocurrency-afc5e9248c4c
Ripple is a company. XRP is a cryptocurrency. They are related, but different.

- An upcoming product (xRapid) *will* use XRP as a way to 'source liquidity'
- Interledger is the protocol that sits under RippleNet. It is being developed as a potential web standard under the watchful eye of the W3C, you can find the unofficial draft specification here.
- Coil, a company that will use Interledger to create a way of allowing money to flow from consumers to creators on the internet

Stellar

- Decentralized Ripple
- collaboration with IBM

Cryptocurrency firm Stellar gets Islamic finance certification

https://www.reuters.com/article/us-islamic-finance-cryptocurrencies/cryptocurrency-firm-stellar-gets-islamic-finance-certification-idUSKBN1K71RC
The certification covers Stellar's blockchain and its native currency called Lumens - the 7th largest cryptocurrency with a market capitalization of $4.3 billion.

Elixxir

https://elixxir.io/

- White paper - https://cdn2.hubspot.net/hubfs/4816439/Elixxir_Technical_Brief.pdf

The Genesis Files: How David Chaum's eCash Spawned a Cypherpunk Dream
https://bitcoinmagazine.com/articles/genesis-files-how-david-chaums-ecash-spawned-cypherpunk-dream/
First published in 1981, Chaum's paper "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms" laid the groundwork for research into encrypted communication over the internet, which would eventually lead to privacy-preserving technologies like Tor.

eCash Founder David Chaum Makes Bold Promises with Elixxir Blockchain
https://bitcoinmagazine.com/articles/ecash-founder-david-chaum-makes-bold-promises-elixxir-blockchain/ "A consumer messaging and payment app with performance, privacy and capacity that consumers are used to with today's centralized systems. But at the same time, it can be resistant to attack even at the national adversary level."

Ecash's Creator Is Back – And He Thinks He's Built the Fastest Blockchain Ever
https://www.coindesk.com/ecashs-inventor-is-back-and-he-thinks-hes-built-the-fastest-ever-blockchain/ "The gist of the system is that a bunch of developers or nodes are involved in a cryptocurrency computation, but only one person needs to be honest in order for the computation to work and for the data to stay private. Elixxir uses this idea in a novel way. The nodes on the network, called "Mixnodes," produce a multi-party computation for every block of transactions."

Crypto Pioneer David Chaum Says He's Built a Better Bitcoin
https://www.wsj.com/articles/crypto-pioneer-david-chaum-says-hes-built-a-better-bitcoin-1537405201

Skycoin

https://www.skycoin.net/

- https://hackernoon.com/redefining-internet-protocols-through-effective-decentralization-b2afbcb874d9 The Skycoin project tackles the problems of cost, security, privacy, network neutrality and various other limitations that linger, holding back blockchain from full implementation. Just as blockchain exposed the limitations of regular internet, the Skycoin project takes us a step further and introduces the community to greater possibilities of blockchain.

- Skyminer. This is the hardware of the Skycoin project that is configured as a custom VPN server providing the infrastructure to power the Skywire network - https://www.skycoin.net/skyminer/

Skycoin: Anatomy of A Cryptocurrency Scam Hunt: The Next Web's Misguided Attack on Skycoin https://medium.com/@lukehirai/anatomy-of-a-cryptocurrency-scam-hunt-b748792a47ed

- The Next Web published two articles denouncing a cryptocurrency/blockchain project, Skycoin.
    - Greene's article—"Skycoin: An Anatomy of Cryptocurrency Scam,"
    - SkyCoin's response to Greene's article: https://medium.com/@Skycoinproject/is-skycoin-a-scam-c5d47ab80d2f
    - Clark's followed—"Exclusive: We suspected this shady cryptocurrency project was a scam. Now we're sure of it."
    -

Nano

- Personal blockchains

https://hackernoon.com/why-third-generation-cryptocurrencies-are-game-changers-for-venezuela-cb8c9b016f9d "NANO is a third generation Cryptocurrency that is implementing its own version of a DAG, known as block-lattice. The block-lattice provides each user with its very own Blockchain, known as an account-chain." Diagram: https://cdn-images-1.medium.com/max/800/1*YA3apOqlNJkTA6AqEmJd3g.png

- "Banano is the first official fork of NANO and was developed to offer fee-less, almost instant micro-transactions. Banano started as a joke between a devoted group of NANO contributors and resulted in a coin that puts a considerable amount of effort without taking itself too seriously."

Eos

Biggest ever ICO - $4 billion

https://www.coindesk.com/eos-blockchain-isnt-live-yet-getting-closer/
after raising a reported $4 billion over the last year to create the software necessary to launch the blockchain, the company that created it is leaving it to its community to actually get it off the ground.

The top 10 holders of EOS tokens own nearly half of the coins.
https://www.bloomberg.com/news/articles/2018-06-05/crypto-whales-own-almost-half-of-tokens-from-biggest-ever-ico

- "It's a whales' election."
- —Steve Floyd of EOS Tribe, a candidate to be an EOS "block producer," the equivalent of a miner. The new blockchain won't go live until the network elects 21 block producers via a complicated voting process, and Floyd and others think one reason the election is taking

longer than anticipated is that some of most influential token holders are waiting to see how others vote before deciding. (CoinDesk)

EOS: Don't Believe The Hype
https://medium.com/@matteoleibowitz/eos-dont-believe-the-hype-c472b821e4bf

- "Censorship resistance, or its lack of, is at the heart of EOS' flaws."
- "The censorship resistant nature of the Bitcoin blockchain means that anyone can hold value in $BTC without the risk of it being seized by a malicious actor, like a government."

EOS's $4 billion crypto-democracy has just launched—and it's probably going to be ruled by fat cats -
https://www.technologyreview.com/s/611475/eoss-4-billion-crypto-democracy-has-just-launchedand-its-probably-going-to-be-ruled-by-fat/

Block.one Wants to Rewrite the Entire EOS Constitution
https://www.coindesk.com/block-one-wants-rewrite-entire-eos-constitution/
"Envisioned as a "holistic blueprint for a globally scalable blockchain society" governed by a written constitution, EOS completed its launch just two weeks ago, but disputes over stolen private keys immediately tested the viability of its governance structures."

AMP

Synereo Aims to Put AMPs in the Hands of Every Internet User
https://medium.com/synereo/synereo-aims-to-put-amps-in-the-hands-of-every-internet-user-4565c405895d "Synereo's native cryptocurrency, AMP. The AMP is a token with real-world value that incentivizes users to reward content creators and be rewarded for content discovery and bringing the content to new, appreciating audiences."

- our first tool, WildSpark , which is a platform designed as a meta-layer in order to reach these Internet leaders where they're already active

Turtlecoin

https://turtlecoin.lol/

- "Too many projects are bringing in too much funding despite most having no damn product. We figured, 'why not do the whole thing in reverse? Start with a fun project, make it as simple and accessible as possible, and let it grow on its own.' We have a strong belief in our no-funding strategy; if we make a cool product, the value will create itself. If you think we're wrong, we're happy to talk about it."

- TurtleCoin was born December 9th, 2017. In the beginning, we were command line only, compiled only for Linux, and got banned repeatedly from online forums for hosting flash TRTL giveaways.

Iota

https://www.iota.org/
IOTA is quite different from Bitcoin and Ethereum, as it uses no blockchain. Instead, it uses "**Tangle**", a Directed Acyclic Graph shaping up a tangle. Once an IOTA transaction is broadcasted to the network, two previous transactions must be approved, and network nodes will need to make sure approved transactions are not conflicting. This is a different way tot tackle the threat of **double-spends** with virtual currencies. - https://satoshiwatch.com/coins/iota/in-depth/iota-dag-tangle/

Docs: https://docs.iota.org/introduction

https://medium.com/@marvinneuefeind/analysis-of-iota-5249f860c6ed
"IOTA is a Tangle based cryptocurrency which main purpose is to serve the economy, namely Internet of Things."

- Diagram - tangle vs blockchain - https://cdn-images-1.medium.com/max/800/1*9GxDvXXYiIm2xPWsqP9Fkg.png

https://blog.usejournal.com/infrastructure-inversion-iota-and-the-iot-1e5ff221eb9b

- "IOTA is a cryptocurrency/DLT that seeks to solve the current inefficiencies of the blockchain."
- "IOTA's new DLT, known as the 'Tangle,' claims to have mitigated many of these concerns, which is why it lends to be the most lucrative technology for the coming 'Internet of Things.' The Tangle works in a slightly different way from blockchain technology. There are no blocks, no transaction fees, and an entirely different data structure known as a DAG (Directed Acyclic Graph). This means that the entire network can scale infinitely and will never cost users a penny to make transactions."
- "Currently, due to the existence of a central "coordinator," IOTA cannot be subject to a 51% attack. This brings up issues of decentralization, but the IOTA Foundation has repeatedly asserted that the coordinator will be turned off once the network has grown large enough to prevent a 51% attack from every occurring."
- With the likes of Bosch, Volkswagen, and Fujistu, as partners and collaborators, it appears that IOTA has a very strong foundation to build upon, and the future looks very bright. Especially with the recent announcement of Qubic, which will enable smart-contract capabilities, as well as outsourced computing, and oracle machines.

The tangle - an illustrated introduction:
https://blog.iota.org/the-tangle-an-illustrated-introduction-79f537b0a455
Diagram: https://cdn-images-1.medium.com/max/1000/0*uhiAGN6uJ6a_pB1F.

“IOTA’s tangle constitutes an abstract machinery of a rhizomatic type, “ceaselessly establishing connections between semiotic chains”. Serguei Popov, a Moscow University Mathematics Ph.D. and something of the core founders of the IOTA task published a follow up document on the 12th of May.” https://iota-news.com/everything-you-need-to-know-about-directed-acyclic-graphs-dags/

Current Iota r&d projects - https://blog.iota.org/whats-next-current-iota-r-d-projects-eeb8cc03adb5

1. **Coordicide:** Analysis, modeling, and simulations for coo-less IOTA.
2. **Autopeering:** Understanding the risks involved with automatic peer discovery and user-friendly alternatives.
3. **Economic Incentives:** Understanding how the Tangle works at scale from a game theoretic perspective.
4. **Consensus Spec:** A detailed spec of the consensus mechanism, building on the basic outline in the whitepaper, intended for peer review.
5. **Crypto Spec:** A detailed spec of cryptography in IOTA, also intended for peer review.
6. **Attack Analysis:** Thorough simulation and analysis of known network attack vectors.
7. **Exchange Hub:** Formerly known as IXI Hub; enables exchanges to integrate IOTA in days or weeks instead of months (already in closed beta with several exchanges!)
8. **IRI:** Ongoing maintenance and improvements to the *de facto* IOTA node software.
9. **Coo-free IRI:** Rebuilding IRI to allow for alternate consensus mechanisms.
10. **Qubic:** Enabling oracles, outsourced computations, and smart contracts on the Tangle.
11. **Local Snapshots & Permanodes:** Enabling node operators to maintain or dispose of the Tangle history as they see fit.
12. **C Client:** Preparation for deep dives into embedded devices.
13. **iota.js:** Out with *iota.lib.js*, in with *iota.js;* fully modularized for npm and fully typed for safety.
14. **Tanglescope:** Enabling deeper insights into Tangle performance and metrics through monitoring.
15. **MAM+:** A fully spec’d, full-featured rewrite of MAM—if all goes well, including PKI out of the box.
16. **IOTA Controlled Agent:** A prototype; early stage implementation of Economic Clustering and swarm logic.
17. **Trinary hash function:** The replacement for Curl-P, built by world renowned cryptographers, and optimized for the IoT.
18. **Protocol finalization:** On IoT, the IOTA protocol can’t easily be changed for devices that are “out there in the wild.”

Monero (XMR)

At present, XMR is the 10th-largest cryptocurrency with a $1.4 billion market cap.

Monero: Unsung Crypto Developer Wins Prestigious Award
https://www.ccn.com/monero-unsung-crypto-developer-wins-prestigious-award/

RingCT (as it is colloquially known) has since become most famous due to its implementation within Monero, the most well-known anonymity-centric cryptocurrency.

Over 90% of Monero's Block Reward Has Been Mined
https://www.ccn.com/over-90-of-moneros-block-reward-has-been-mined/

See also: Fortnite

Stablecoins

https://www.technologyreview.com/s/611370/stablecoins-are-trending-but-they-may-ignore-basic-economics/
"Stablecoins" are trending, but they may ignore basic economics. Pegging cryptocurrencies to "real" money could stabilize them—or ruin them entirely.

three broad categories:

- Back up the tokens with cash in a bank account. This is how Tether, the most popular dollar-pegged coin, works.
- Back up the tokens with other cryptocurrencies.
- Create an "algorithmic central bank." - forthcoming project called Basis, which raised $133 million in April from several big-name Silicon Valley VC firms. Basis's white paper (PDF)

State of Stablecoins, 2018
https://media.consensys.net/the-state-of-stablecoins-2018-79ccb9988e63
"The Definition of Stablecoin: Stablecoins are crypto-assets that maintain a stable value against a target price (e.g. USD)."

- Mappings of sytablecoings - image: https://cdn-images-1.medium.com/max/1600/0*teynSGK5IzyAGcC9.png

Shining light on The State of Stablecoins
https://blog.blockchain.com/2018/09/26/the-state-of-stablecoins/

- Link - https://www.blockchain.com/research
- Diagram - https://blog.blockchain.com/content/images/2018/09/Stablecoin-Social-Images-03.jpg

IOU Centralized, Collateral-Backed Stablecoins

Backed by fiat (or traditional assets) reserves

LIVE PROJECTS

AAA Reserve

Cryptocurrency (AAA) backed by cash, gilts and AAA-rated credit investments and stable against fiat currencies. Focus on large fiat amounts(>$25k).

[Live since January 2018]

Digix Gold Tokens

Gold-Stable tokens *(DGX)*. 1DGX = 1 gram of gold in a Singapore vault.
[Live since Q1 2018–1st crowdsale on the Ethereum blockchain in 2016, raised +465K Ether]

EURS (by Stasis)

Fiat-collateralized EIP-20 stable token backed by EUR, with verification streams, supported by STASIS.
[Live since July 2018]

Tether

Tether (ex Realcoin)

USD-backed stable tokens (*USDT*) built on Omni, market-leader.
[Live since February 2015]

The Mystery Behind Tether, the Crypto World's Digital Dollar
https://www.wsj.com/articles/the-mystery-behind-tether-the-crypto-worlds-digital-dollar-1534089601
""There are a couple of forces in this market that if they failed, it would be catastrophic. Tether is one of them." —Ding'An Fei, a managing partner at Beijing-based digital asset investment firm Ledger Capital, to the Wall Street Journal ($). A recent piece in the Journal takes an in-depth look at the mysterious crypto-token, supposedly backed by US dollar reserves, that has become a "cornerstone" of the cryptocurrency market."

USD Coin

USD Coin (by Circle & CENTRE)

Fiat tokens (USDC) for crypto payments and trading (using CENTRE, a framework for stablecoins project involving real-world asset reserves, issued by CENTRE network members and audited by CENTRE).

USD Coin Arrives: Circle's Crypto Stablecoin Is Now Trading
https://www.coindesk.com/usd-coin-arrives-circles-crypto-stablecoin-is-now-trading/

Others

TrueUSD (by TrustToken Team)

USD-backed stable cryptocurrency (*TUSD*) focusing on transparency, built on Ethereum.
[Live since March 2018]

PROJECTS IN DEVELOPMENT

Globcoin.io

Stablecoins *(GLX)* pegged to a basket of fiat currencies held in custody.
[Launch by the end of 2018]

Jibrel (by Jibrel Network)

Stablecoins (jUSD, jEUR…) backed by a wide range of assets, built on the Ethereum blockchain
[Alpha—Launch TBD]

PHI (by dfinity-network)

IOU stablecoins *(PHI)* backed by loan collaterals maintained algorithmically.
[Launch TBD]

Saga

Asset-backed cryptocurrency *(SGA)* maintained with a reserve held in a regulated banking institution, stable against SDR (basket of currencies).
[Launch TBD]

Stably, Inc.

Reserve-backed stablecoins *(StableUSD)* with a supply adjusted via open market operations.
[Beta—Launch TBD]

Stronghold USD (by Stronghold & IBM)

USD token backed by multiple fiat currencies based on the Stellar network, guaranteed by the Federal Deposit Insurance Corporation. *[Launch TBD]*

X8currency

Stable cryptocurrency *(X8X)* backed by a basket of fiat currencies and physical gold reserve. *[Launch TBD]*

IOU "Semi-Decentralized," Collateral-Backed Stablecoins

Backed by crypto-assets.

LIVE PROJECTS

Bitshares

Stable cryptocurrency (*Smarctoins: BitUSD, BitCNY*) with value backed by multiple assets (including cryptos) using derivative instruments.
[Live since 2014—1st historic stablecoins projects]

Havven.io

Stablecoins (*nUSD*) backed by fees, a distributed collateral pool and issuance mechanisms (similar to seigniorage shares model—see 3).
[Live since June 2018]

MakerDAO

Decentralized system issuing stablecoins (*DAI*), stable against ETH and backed by multiple assets (only ETH for now but aim to open a multi-collateral version). Maintained by MKR holders. Assimilable to derivatives instruments.
[Live since December 2017]

StatiCoin

Stablecoins backed by ETH with a system matching speculators to buy tokens against hedgers who buy "stablecoins" *(Staticoin)* to create stability.
[Live since October 2017]

PROJECTS IN DEVELOPMENT

Alchemint

Stablecoins *(SDUSD)* built on top of NEO, backed by a pool of assets (fiats and cryptocurrencies).
[Launch planned Q3 2018]

Augmint

Digital tokens (*A-EUR,* their € stable token) targeted to fiat currencies copycatting their mechanisms using stability reserves and smart contracts.
[Launch planned on Q3 2018—Q2 2019]

Boreal (by aurora-dao)

Stable crypto-assets (*Boreals*) backed by a combination of ether reserves, debt from loans, and dapp endorsement.
[Launch planned Q3 2018]

Celo

Stable tokens pegged to fiat currencies, backed by a diversified, overcollateralized, and auditable crypto-asset reserve.
[Launch TBD]

Reserve (by Reserve Research Team)

Tokens stabilized by crypto-assets locked in a smart contract, "fully" decentralized.
[Launch TBD]

Sweetbridge

On-chain collateral-backed stablecoins *(Bridgecoins).*
[Launch TBD]

Unum

Stablecoins backed by multiple cryptocurrencies and simple reserve mechanisms.
[Beta—Launch TBD]

Seigniorage Shares

Acting as a (partially) decentralized bank and incorporating elastic supply mechanisms. Often involve some collateral positions, algorithmic regulations and complex stability mechanisms [Further readings here]:

LIVE PROJECTS

BitBay Official

Cryptocurrency (BAY) aimed to be stabilized via a dynamic peg using "liquid" and "frozen" tokens and decentralized governance mechanisms.
[Live since 2015]

NuBits

Cryptocurrency *(USNBT)* stabilized by issuance mechanisms and custodial grants.
[Live since 2014]

SteemDollar (by Steemit)

Tokens (SBD) to be stabilized on the Steem blockchain with a 1:1 USD conversion rate—based on a convertible notes system.
[Live since 2016]

PROJECTS IN DEVELOPMENT

Basis

(ex Basecoin)**:** To issue stablecoins via smart contracts acting as a central bank to inflate and deflate prices by issuing bonds.
[Launch TBD]

Carbon

Cryptocurrency monitored (Carbon) by an elastic supply through market participants, powered by Hedera Hashgraph.
[Launch TBD]

Corion

Cryptocurrency whose price is maintained by an automated inflation/deflation control.
[Beta—launch TBD]

Fragments

Stable (low-volatility) tokens (*USD Fragment*) with an auditable reserve and monetary supply policy.
[Launch TBD]

Kowala (by Kowala Tech)

Cryptocurrency (*kCoin*) to be stable against fiats, cryptos and other types of assets maintained with algorithms and market-based oracles.
[Beta—launch TBD]

Topl

Stable cryptocurrency (*Polys)* backed by a basket of assets stabilized by the Topl foundation that issues and redeems tokens.
[Launch TBD]

Stable

Tokens (*STB*) to be stabilized through a flexible supply and demand with inflation containment mechanisms.
[Launch TBD]

StableUnit

Tokens whose price is maintained via multiple stabilization mechanisms involving a DAO, cryptocurrencies reserves applying various monetary systems.
[Launch planned on Q1 2019]

TerraMoney

Cryptocurrency pegged to a basket of currencies (e.g. SDR) and assets with its value algorithmically stabilized; involves decentralized elastic supply mechanisms.
[Launch TBD]

Stakenet

Stakenet (XSN) Blockchain Architecture
https://medium.com/@jstarhead/stakenet-xsn-blockchain-architecture-8c17f6467e3
https://medium.com/@jstarhead/stakenet-xsn-blockchain-architecture-2-2-f1438406de86
Stakenet is a trustless PoS blockchain, which provides a truly decentralized, highly secured and profit driven inter chain meta network for cryptocurrencies. Stakenet is powered by its native coin XSN and is managed by its own masternodes.

- "Because XSN is based on Bitcoin.core, all the achievements of Bitcoin development, like SegWit and the Lightning Network, can be integrated in the Stakenet blockchain architecture without much effort."
-

Mining and Miners

(Maybe not enough here for a whole section)

Mining Overview

Any node can announce a new block, there's nothing special about that process, you just need a new block.

Crypo Mining—ETH—Not Worth Starting
https://medium.com/@cryptoTweeg/crypo-mining-eth-not-worth-starting-9890461c36fb
Don't start! If you're already mining, keep at it. If you're looking to start, don't. Buy crypto instead or build a gaming PC and have some fun.

Mining Software

Mining Software - https://www.techradar.com/news/the-best-cryptocurrency-mining-software-2018

- CGMiner - A flexible mining program that supports almost every platform
- Bitminter - Another cross-platform program with an easy-to-use UI
- BFGMiner - A focused mining client which is a tinkerer's paradise
- MultiMiner - FGMiner made easier for the less tech-savvy
- EasyMiner - User-friendly GUI frontend for a pair of mining programs

Bitmain

Chinese cryptocurrency mining company Bitmain has been valued at $12 billion in a new funding round. (CoinDesk)

https://en.wikipedia.org/wiki/Bitmain

Bitmain Technologies Ltd., or Bitmain, is a privately owned company headquartered in Beijing, China. They are a bitcoin miner and designer of ASIC chips.[1]

Crypto Mining Giant Bitmain to Open Data Center in Small Texas Town
https://www.financemagnates.com/cryptocurrency/news/crypto-mining-giant-bitmain-to-open-data-center-in-small-texas-town/ Bitmain is planning on opening a new data center in Rockdale, Texas, near Waco.

Bitmain Sells Bitcoin, Buys Bitcoin Cash – Now Holds 5% of Circulation
https://www.financemagnates.com/cryptocurrency/news/bitmain-sells-bitcoin-buys-bitcoin-cash-now-holding-5-of-circulation/

Bitmain's Equihash ASIC
https://blockexplorer.com/news/bitmain-begin-shipping-equihash-asic-miners-june/
Bitmain's Latest Crypto ASIC Can Mine Zcash
https://www.coindesk.com/bitmains-latest-crypto-asic-can-mine-zcash/

Cryptocurrency giant Bitmain chooses Hong Kong for IPO
https://www.reuters.com/article/us-bitmain-ipo/cryptocurrency-giant-bitmain-chooses-hong-kong-for-ipo-idUSKCN1M627L

Mining Pools

Bitmain operates Antpool, historically one of the largest bitcoin mining pools.[2]
https://www.blockchain.com/pools

Mining pool: Many miners do this, and they connected their specialized hardware directly to a mining pool using an entirely different protocol call the Stratum mining protocol. You can mine without running a node, and many miners do exactly that.

The Mining Industry

The Bitcoin Boom Reaches a Canadian Ghost Town
https://medium.com/@bloomberg/the-bitcoin-boom-reaches-a-canadian-ghost-town-ff6cbe48522
“The Bitcoin mine has come to Ocean Falls after almost four decades of false starts. The town went dormant once the paper industry left, but it wasn’t dead, exactly. The dam that powered the mill was still capable of producing about 13 megawatts of electricity.”

Exchanges

Activity

Only a handful of crypto exchanges have published their total user stats & user growth statistics.
Graphs:

- User growth - https://cdn-images-1.medium.com/max/800/1*eVIos6qm2s91nf_sI6_3fg.png
- Market share of exchanges - https://cdn-images-1.medium.com/max/800/0*vSfK_7rqtM4faurM.
- Volume - https://cdn-images-1.medium.com/max/800/1*z9R5TMkO9rVzSL1mcfLQ_A.png

Kiosks

https://www.badgercoin.com/
“HoneyBadger is Canada's most reliable network of bitcoin kiosks. Established in August 2016, with a passion for bitcoin and cryptocurrency, we began with 1 kiosk in Vancouver to now 45+ kiosks across Canada and select international locations. We are also excited to

offer LiteCoin and Ethereum at our kiosks! Check back here often for our new locations and to see what we are up to."

- Faq - https://www.badgercoin.com/faq/

Cryptocurrency Indexes

A Guide to Major Cryptocurrency Indexes
https://medium.com/datadriveninvestor/a-guide-to-major-cryptocurrency-indexes-15c3ea60543

Cryptocurrency Index 30 (CCi30)

https://cci30.com/
Perhaps one of the oldest Crypto indexes out there & the one that I have been following the longest. The Cryptocurrencies Index 30 (CCi30) was launched on Jan. 1, 2015

Bloomberg Galaxy Crypto Index (BCGI)

https://www.bloomberg.com/professional/product/indices/bloomberg-galaxy-crypto-index/
A more recent but a significant addition to the index list has been the Bloomberg Galaxy Crypto Index (BGCI), which tracks the performance of the largest cryptocurrencies traded in the US Dollar. It was launched on May 03, 2018

Coinbase Index

https://am.coinbase.com/
The U.S based digital exchange giant introduced their very own Coinbase Index which tracks the performance of the Crypto assets listed on the exchange only.

Huobi Index (HB10)

https://www.huobi.com/en-us/huobi_index/
To help make Cryptocurrency trading easier for the investors Huobi—the third largest Crypto exchange by volume decided to launch its own HB10 Index consisting of the 10 most highest volume coins traded against USDT. The index was launched on May 23, 2018

Bitmain Big 10 Index (BLC10)

https://doc.btc.com/bitmain-index/Index-Methodology.pdf
Most recently on Nov. 28 2018, Beijing-based Bitmain & one of the biggest Crypto miners in the World, launched its own BLC 10 index which tracks ten of the most largest, most liquid digital assets in the market, denominated in US dollars.

Centralized Exchanges

Vitalik Buterin: “I definitely hope centralized exchanges go burn in hell as much as possible”
https://techcrunch.com/2018/07/06/vitalik-buterin-i-definitely-hope-centralized-exchanges-go-burn-in-hell-as-much-as-possible/

Bakkt

https://www.bakkt.com/index

Bitcoin Sees Wall Street Warm to Trading Virtual Currency
https://www.nytimes.com/2018/05/07/technology/bitcoin-new-york-stock-exchange.html “The parent company of the New York Stock Exchange has been working on an online trading platform that would allow large investors to buy and hold Bitcoin, according to emails and documents viewed by The New York Times and four people briefed on the effort who asked to remain anonymous because the plans were still confidential.”

Intercontinental Exchange Announces Bakkt, a Global Platform and Ecosystem for Digital Assets
https://ir.theice.com/press/press-releases/all-categories/2018/08-03-2018-133022149
“ Intercontinental Exchange (NYSE:ICE), a leading operator of global exchanges, clearing houses, data and listings services, announced today that it plans to form a new company, Bakkt, which intends to leverage Microsoft cloud solutions to create an open and regulated, global ecosystem for digital assets. The new company is working with a marquee group of organizations including BCG, Microsoft, Starbucks, and others, to create an integrated platform that enables consumers and institutions to buy, sell, store and spend digital assets on a seamless global network.”

New Bakkt Venture Could Make Bitcoin As Mainstream As Starbucks
https://www.forbes.com/sites/norbertmichel/2018/08/13/new-bakkt-venture-could-make-bitcoin-as-mainstream-as-starbucks/#4d27136736c8

Sorry, But Starbucks Will Not Be Accepting Bitcoin
https://motherboard.vice.com/en_us/article/43pq8p/starbucks-will-not-be-accepting-bitcoin?utm_campaign=152aa73dff-EMAIL_CAMPAIGN_2018_08_07_04_25 “Contrary to numerous news reports, Starbucks’ new cryptocurrency partnership with Microsoft and Intercontinental Exchange doesn’t mean you’ll be able to spend your bitcoins at the coffee retailer’s locations.”

Coinbase

Coinbase Announces Custody Plans for 40 Digital Assets, Including XRP
http://fortune.com/2018/08/03/coinbase-custody/
Coinbase announced it is exploring plans to expand its custody service to include 40 more assets, including XRP, which is the third biggest cryptocurrency by market cap.

Institutional funds are required by law to use a custodian to hold their assets and protect them from theft. In return, the custodians charge a fee to keep the assets secure.

Coinbase is Making $2.7 Million a Day
https://medium.com/@Michael_Spencer/coinbase-is-making-2-7-million-a-day-afa95dd52b42

Coinbase Custody is Officially Open For Business
https://blog.coinbase.com/coinbase-custody-is-officially-open-for-business-182c297d65d9

Coinbase's institutional product has begun accepting deposits starting this week, called Coinbase Custody, the service targets institutional investors. It's aimed at major institutional hedge funds and other big-time clients who can deposit a minimum of $10 million.

Coinbase Becomes Electronic Money Institution Under U.K.'s FCA Regulations & Adds Support For Faster Payments
https://medium.com/the-crypto-times/coinbase-becomes-electronic-money-institution-under-u-k-s-107838c2135f

Binance

https://www.binance.com/

Scaled back - Bloomberg-
https://www.bloomberg.com/news/articles/2018-06-04/binance-s-venture-fund-head-is-waiting-for-ico-bubble-to-burst ""We'd like the bubble to break," said Zhang, who joined cryptocurrency trading platform Binance to lead its venture incubator Binance Labs less than two months ago. "We still see a lot of hype in the market, valuations are high and unreasonable. We really think if the bubble bursts, it's a good thing for the industry.""

Screenshot: https://cdn-images-1.medium.com/max/1600/1*VnqB6Hrm75LpsP9YmChYGg.png from https://cryptocurrencyhub.io/i-bought-my-first-bitcoin-now-what-fdf7dc9ad150

ErisX

https://www.cnbc.com/2018/10/03/td-ameritrade-bets-on-a-new-cryptocurrency-exchange.html "The U.S. brokerage firm announced a strategic investment Wednesday in an exchange called ErisX, which offers both bitcoin spot and futures trading. High-speed trading company Virtu Financial will also back the exchange."

eToro

eToro launches new 'pro' cryptocurrency exchange – and 8 stablecoins (Hard Fork)

https://thenextweb.com/hardfork/2019/04/16/etoro-launches-new-cryptocurrency-exchange-for-pros-and-8-stablecoins/

Others

Bittrex: https://bittrex.com
OkEx: https://www.okex.com/
Coss.io: https://exchange.coss.io/
Cryptopia: https://www.cryptopia.co.nz/
Bit-Z: https://bit-z.com/
UpBit: https://upbit.com/
LiteBit: https://www.litebit.eu
CoinSpot: https://www.coinspot.com.au/
CryptoMate: https://cryptomate.co.uk/
CoinSwitch: https://www.coinswitch.co/
SimpleSwap: https://www.simpleswap.io/

BitThumb - https://www.bithumb.com/

Decentralized Exchanges

https://decentralize.today/the-rant-76727cdf27f3
"This is where DEX come in. Decentralized exchanges are the next logical step for adoption and kicking out the middleman. One project which will certainly make waves in the DEX and crypto world will be Altcoin.io."

Diagram: https://cdn-images-1.medium.com/max/2000/1*_lHzstUbCVDomTzbo7y-SA.png
From: https://blog.altcoin.io/why-decentralized-exchanges-need-a-liquidity-strategy-51dfd75876eb

About Decentralized exchanges
https://hackernoon.com/understanding-decentralized-exchanges-51b70ed3fe67

https://blog.altcoin.io/why-decentralized-exchanges-need-a-liquidity-strategy-51dfd75876eb
For a decentralized exchange (DEX) to succeed, you need three things:
- Traders. Lots of them.
- The ability to scale.
- A user experience that sets you apart.
A robust liquidity strategy is at the top of this list for a reason.

Analyzing Activities on Decentralized Exchanges
https://media.consensys.net/analyzing-activities-on-decentralized-exchanges-847e95570444
"most cryptocurrency trading is still performed through centralized exchanges such as Coinbase and Binance. These exchanges store their customers' KYC data, facilitate their tradings, and fully control

their funds. Several high profile attacks on traditional exchanges have been reported in previous years [2], exhibiting a need for exchanges that operate in a more trustless and secure way. These new exchanges are known as Decentralized Exchanges (DEXes) and put the control of funds and trading back in the hand of their users."

Why creating great user experiences is crucial to blockchain adoption
https://blog.altcoin.io/why-creating-great-user-experiences-is-crucial-to-blockchain-adoption-d65afc1ce460

- most blockchain applications—including some DEXs—are complicated, falling short of what we've come to expect from "Web 2.0".
- Our vision is to empower everyone, regardless of market knowledge, to trade altcoins securely and with confidence… By including social trading in our DEX.

Decentralized Crypto Exchange is Solution to Hacks, Will They be Ready?
https://www.ccn.com/decentralized-crypto-exchange-is-solution-to-hacks-will-they-be-ready/
"On a decentralized exchange like IDEX, users trade crypto with non-custodial wallets like Trezor, Ledger, and MetaMask. Hence, at all times, users have complete control over their funds by connecting their non-custodial wallets to exchanges."

An Overview of Decentralized Trading of Digital Assets
https://collaborate.thebkp.com/project/TL/document/9/version/10/

- Good general article

Altcoin.io

https://altcoin.io/
"The decentralized exchange of the future. Launching 2018. A truly decentralized and secure cryptocurrency exchange powered by Plasma."
"What makes Altcoin.io unique? Imagine having the speed, ease of use and the UI of a centralized exchange with all the security advantages of a decentralized one. That is Altcoin.io."

LitePaper: https://www.preview.altcoin.io/lite-paper.pdf

https://decentralize.today/the-rant-76727cdf27f3

https://blog.altcoin.io/why-decentralized-exchanges-need-a-liquidity-strategy-51dfd75876eb
Altcoin.io is releasing an SDK to help get other decentralized exchanges off the ground. - https://altcoin.io/sdk.html

IDEX

- - https://idex.market/eth/aura - decentralized exchange for trading Ethereum (ERC-20) tokens. IDEX combines the speed of centralization with the security of blockchain settlement.

0x

- - https://0xproject.com/ - Order Books & Relayer - 0x (Zero X). The aim of the project is to provide an open protocol for decentralized exchanges on top of Ethereum. They've also done a token sale of the $ZRX token that's trading at a $542M market cap currently.
    - read the 0x white paper

EtherDelta

- https://etherdelta.com/#PPT-ETH - Order Books & Relayer - EtherDelta is one of the first decentralized exchanges that has gained some traction out there. It runs mostly on Ethereum and there is about $1.4BN USD in the most recent version of its smart contract.

  Image:
  https://cdn-images-1.medium.com/max/1600/1*v83xj39vRYb8JOBBMCmbwQ.png

  The Solidity code for the EtherDelta contract is freely available on Etherscan here.

  Funds Management
  leaves control of funds completely in control of the users. - two mechanisms for moving funds. One is for moving ETH—the native currency of Ethereum. The other is for moving ERC20 tokens.

  Trading Logic.
  A person can submit open buy or sell orders for a given ERC20 token—in exchange terminology this person is the *Maker*. Another trader can browse these orders and choose to execute on them—this is called the *Taker*.
  Image:
  https://cdn-images-1.medium.com/max/1600/1*sBtSlovC2FPxKWll6hrq4A.png

  the special sauce that makes off-chain order books work comes right from the heart of blockchain—an Elliptic Curve Digital Signature Algorithm—or ECDSA for short.

The Ocean

- - https://oceanprotocol.com/ - tokenized service layer that exposes data, storage, compute and algorithms for consumption

Airswap Protocol

- - https://www.airswap.io/ - Trading Through Peer-to-Peer Protocol

Bancor

- - https://www.airswap.io/ - In-Wallet Trading

Kyber Network

- - https://kyber.network/ - Ecosystem of Reserves

Definitions

taker: the one who fills the order
maker: the one who creates the trade order
maker token: maker's ERC20 token contract address
taker token: taker's ERC20 token contract address
maker amount: amount of maker token that maker offers to taker
taker amount: amount of taker token that taker offers to maker
block number and time: block number and associated timestamp of the block where the trading was recorded in.

Networks

Towards a Design Philosophy for Interoperable Blockchain Systems, Thomas Hardjono, Alexander Lipton, Alex Pentland
https://arxiv.org/abs/1805.05934
"In this paper we discuss a design philosophy for interoperable blockchain systems, using the design philosophy of the Internet architecture as the basis to identify key design principles. Several interoperability challenges are discussed in the context of cross-domain transactions. We illustrate how these principles are informing the interoperability architecture of the MIT Tradecoin system." - Good very detailed article.

Aion

Aion launches first public blockchain network - https://techcrunch.com/2018/04/25/aion-launches-first-public-blockchain-network/
"The company wants to be the underlying infrastructure for a network of blockchains in a similar way that TCP/IP drove the proliferation of the internet. To that end, the company, which originally began as a for-profit startup called Nuco, has decided to become a not-for-profit organization with the goal of setting up protocols for a set of interconnected blockchains. They now see their role as something akin to the Linux Foundation, helping third-party companies build products and creating an ecosystem around their base technology."

dIAGRAM: https://techcrunch.com/wp-content/uploads/2018/04/aion-net-2018-04-24.png?w=680

https://aion.network/

Essentia

Essentia (a new Block Chian) claims so far 17 blockcahon could interoperate using their framework
https://essentia.one/

“Essentia is a modular decentralised interoperability and data management framework.

Although it may sound complicated, it’s composed of two main components: Essences and Synergies.

In Essences, entities own their data, interlinking them across multiple services. They can be of individuals, companies, groups or organisations, effectively creating decentralised internet users, making interoperability between them also possible by subIDs, permissions and self-triggering, information related, smart contracts.

Synergies are the connective tissue of operations. They link different platforms, resources and modules together for them to be able to interoperate.”

Whitepaper: https://essentia.one/whitepaper.pdf

ICOs

The Plain English Guide to Initial Coin Offerings (ICOs)
https://blog.hubspot.com/marketing/initial-coin-offering-ico
“An initial coin offering is when startups raise money by creating their own digital tokens or digital coins that can be spent to use the company’s current or future service. The company sells a limited number of their newly minted cryptocurrency to investors in exchange for established cryptocurrency like Bitcoin or Ether.”

https://www.technologyreview.com/the-download/611080/this-visualization-shows-just-how-crazy-and-explosive-the-ico-market-has-become/
Saved tokensalemarket.JPG

The next generation of ICOs will actually have to follow the rules
https://www.technologyreview.com/s/610513/the-next-generation-of-icos-will-actually-have-to-follow-the-rules/

- Also: charges against a pair of companies for conducting illegal digital token sales. The two initial coin offering (ICO) projects, called Airfox and Paragon - https://www.sec.gov/news/press-release/2018-264

Tokens are Eating the World
https://medium.com/futuresin/tokens-are-eating-the-world-a52ac885109c
"Tokens aren't just incentivizing tech startups to grow faster, but are also empowering solutions in which blockchain is bringing many ethical upgrades to our planet. To invest in crypto is therefore like signing a petition that the world needs to be improved and giving distributed ledger technologies a chance."

2017 Was the Year of the ICO—Now What?
https://medium.com/mit-technology-review/2017-was-the-year-of-the-ico-now-what-b67d14ce99e5
"An ICO involves selling digital units of value, called tokens, that can be passed between users of a blockchain network, the same way Bitcoin users move bitcoins"

The Next Generation of ICOs Will Actually Have to Follow the Rules
https://medium.com/mit-technology-review/the-next-generation-of-icos-will-actually-have-to-follow-the-rules-de0a6dec4db5

The Problem with ICOs Is That They're Called ICOs
https://medium.com/mit-technology-review/the-problem-with-icos-is-that-theyre-called-icos-2ffc594419b5
Robleh Ali, former crypto specialist for the Bank of England, on why initial coin offerings are dangerous and how to make them more useful

Tokens

What is a token?

Tokens can come in various different forms and functions and are therefore hard to define. Some represent a user's reputation within a system (augur), a deposit in US dollars (tether), the quantity of files that are saved in it (filecoin) or the balance in some internal currency system (bitcoin)
Thus, a token can fulfil either one, or several of the following functions:

- A currency, used as a payment system between participants
- A digital asset (a digital right like land ownership)
- A means for accounting (number of API-calls, volume of torrent uploads)
- A share (stake) in a company
- A reward for contributors (i.e. Steemit)
- Payment for using a system/product/service

https://medium.com/@argongroup/8-important-things-to-know-about-security-tokens-token-regulation-3d548a1a6367

Utility Tokens

“Through the ICO fundraising model, startups can raise capital by issuing crypto tokens on a blockchain — most commonly Ethereum — and distributing them to token buyers in exchange for making a financial contribution to the project.” … “Utility tokens, also called user tokens or app coins, represent future access to a company’s product or service.”
https://strategiccoin.com/ico-101-utility-tokens-vs-security-tokens/

6 Key Differences Between Security and Utility Tokens
https://medium.com/datadriveninvestor/6-key-differences-between-security-and-utility-tokens-d89c65901af8
“The Munchee case—and others such as BitConnect– have raised several important questions surrounding the nature of tokens being issued by new blockchain-based companies”

Security Token (a)

Security token trading is a multi-trillion dollar blockchain opportunity
https://blog.altcoin.io/security-token-trading-is-a-multi-trillion-dollar-blockchain-opportunity-2f4d0b5b2c73

- “Securities represent something valuable in the real world, such as stocks, bonds, or other assets. They often come with benefits like voting rights, equity, and dividends, and are easily converted to cash.”
- “Security tokens, on the other hand, are digital contracts that divide securities into cryptographic segments, which can be traded independently. If you want to buy a stake in a property, artwork, or business, for example, you could purchase digital tokens that prove your ownership with blockchain certainty.”
- “Most importantly, security tokens are SEC compliant. “
-

https://blog.polymath.network/what-the-is-a-security-token-f4ff987620e8
What the !@#$ is a Security Token?
“These projects will allow owners to fractionalize the ownership of any asset using blockchain tokens, after which they can trade seamlessly and legally between verified investors anywhere in the world.”

(As contrasted with a utility token - see ICO, above)
“If a crypto token derives its value from an external, tradable asset, it is classified as a security token and becomes subject to federal securities regulations.”
https://strategiccoin.com/ico-101-utility-tokens-vs-security-tokens/

The Security Token Thesis
https://hackernoon.com/the-security-token-thesis-4c5904761063
“I define security tokens as any blockchain based representation of value that is subject to regulation under security laws. That includes tokens representing traditional assets like equity, debt, derivatives, and real estate, and it also includes pre-launch utility tokens that are deemed securities by the SEC.”
Diagram: https://cdn-images-1.medium.com/max/800/0*QlsjVNlgBPZyN0OA.

Benefits:

- 24/7 Markets
- Fractional ownership
- Rapid settlement
- Cost Reduction
- Liquidity and Market Depth
- Automated compliance
- Asset Interoperability
- Design space expansion

Further reading:
Traditional Asset Tokenization (McKeon)
Liquidity is about market depth, not magic (McKeon)
The Promise of Automated Compliance (McKeon)
The Official Guide to Tokenized Securities (Pompliano)
Official Guide to the Security Token Ecosystem (Koffman)
The Future of U.S. Securities Will Be Tokenized (Marks)

Difference between security token and utility token - diagram - https://cdn-images-1.medium.com/max/1000/0*XEKsMplOHqdieHJY. On https://medium.com/@argongroup/8-important-things-to-know-about-security-tokens-token-regulation-3d548a1a6367

"I define security tokens as any blockchain based representation of value that is subject to regulation under security laws. That includes tokens representing traditional assets like equity, debt, derivatives, and real estate, and it also includes pre-launch utility tokens that are deemed securities by the SEC." https://hackernoon.com/the-security-token-thesis-4c5904761063

- The Howey Test - defines what a security is

Prepare Yourself! The Security Token Tsunami Is About To Hit - https://medium.com/crypto-oracle/prepare-yourself-the-security-token-tsunami-is-about-to-hit-9d5517caff49

- The simplest argument for Security Tokens is from the Harbor Whitepaper
- Firms like Tokensoft, OpenFinance Network, Teknos, Polymath, Verify Investor, Start Engine, tZERO, Templum, Kingdon, Blackmoon, Securitize, and Harbor, are just a small fraction of the companies building standardized, interoperable, and scalable Security Token solutions.

- https://hackernoon.com/security-tokens-will-transform-traditional-finance-31427343d7de "Securities tokens are digital tokens that represent ownership of an underlying asset or security—subject to a nation's federal securities regulations. These digital tokens will soon be issued on public networks like Ethereum or Bitcoin with in-built compliance features."

Jasper

Jasper Phase III: Securities settlement using distributed ledger technology
https://www.payments.ca/sites/default/files/jasper_phase_iii_whitepaper_final_0.pdf
"Securities and cash were brought on-ledger through the issuance of Digital Depository Receipts (DDRs) by CDS and the Bank of Canada, respectively, allowing POC participants to settle securities against central bank cash on the distributed ledger."

Societe General

Societe General Issues First Bond Security Token on Ethereum
https://www.societegenerale.com/en/newsroom/first-covered-bond-as-a-security-token-on-a-public-blockchain
Baby got bonds...Societe General, a French investment bank issued 100 million euros of covered bonds as security tokens on the public Ethereum blockchain. Covered bonds are backed by loans made by a bank and remain on the bank's balance sheet. These loans, such as mortgages are relatively liquid and can be sold off gradually, making this type of bond an ideal candidate for security tokenization.

The other Triple-A...The bond has also been rated Aaa / AAA by Moody's and Fitch, respectively. While these are the highest ratings of each firm, this is fairly typical for these types of bonds.

Polymath

Polymath is building a protocol coded to allow compliant trading of security tokens on the Ethereum blockchain.

AirSwap

AirSwap, a Brooklyn-based technology company, has successfully built a decentralized platform that will soon allow peer to peer trades of security tokens on the Ethereum blockchain.

Activity

https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp

- "The CEO of Causam eXchange Inc. is perfectly willing to refer to the company's upcoming sale of blockchain-based assets to investors as a securities offering." https://www.investopedia.com/news/equity-ethereum-firm-offers-real-stock-through-ico/

- "Munchee, a blockchain-based app for posting restaurant reviews, intended to raise funds by distributing a coin called MUN. According to a whitepaper issued by the startup, MUN was

to be used as currency within the Munchee app to incentivize restaurants and reviewers to purchase services or earn rewards." https://www.investopedia.com/news/icos-beginning-end/

- OmiseGO was one of the biggest Ethereum ICOs of 2017 and raised $25 million. - the company aims to develop a platform that allows for value exchange and various payment solutions across different currencies (both cryptocurrencies and fiat currencies like the dollar). https://kingpassive.com/what-is-ethereum/
-
- "Online retailer Overstock recently announced that tZERO, one of its portfolio companies, will hold an ICO to fund the development of a licensed security token trading platform. The tZERO tokens will be issued in accordance with SEC regulations, and Overstock CEO Patrick Byrne has stated that token holders will be entitled to quarterly dividends derived from the profits of the tZERO platform."
  https://strategiccoin.com/ico-101-utility-tokens-vs-security-tokens/

- A Japanese village of 1,500 people is planning an ICO. -
  https://www.coindesk.com/japanese-village-to-launch-nations-first-municipal-ico/

The ICO Process

The Initial Coin Offering, One Year Later
https://hackernoon.com/the-initial-coin-offering-one-year-later-6b5f836c2b
"Truth is there is no iron-clad, compliant path to a token sale or ICO for a U.S.-based business. Lawyers are only selling their version and hoping they're right. (This is why many companies have gone to a Private Placement Memorandum, but more on that another time.)"

The Mechanics of the Token Launch
https://blog.fractalblockchain.com/the-mechanics-of-the-token-launch-92f186a597f5

- Diagram -
  https://cdn-images-1.medium.com/max/1600/1*nGjT49C2krhXsKHTUMmICA.jpeg

Fractal. Fractal is an end-to-end token launch service provider and offers user-friendly experience with a compliant onboarding process. http://trustfractal.com/

The Future of ICOs

- ICOs: Beginning Of The End? - https://www.investopedia.com/news/icos-beginning-end/
  "largely unknown entity at the start of 2017. Toward the end of the year, however, they have reportedly raised $3.25 billion…. According to a report by research firm Smith + Crown, only 69 of the 169 ICOs in October 2017 managed to reach their fundraising goals.
- The amount of money raised in initial coin offerings (ICOs) in the first quarter of 2018 has blown past the amount raised throughout all of 2017, according to data from Coindesk. In the first three months of the year, a total of $6.3 billion raised from digital coin offerings represented 118% more than that of last year's total, suggesting that despite increased scrutiny

on the cryptocurrency space, ICOs aren't going anywhere soon.
https://www.investopedia.com/news/already-more-icos-2018-all-2017-63b/

The ICO market is not collapsing. It's maturing.
https://hackernoon.com/the-ico-market-is-not-collapsing-its-maturing-c11bfd4cdfe8
"The most striking geographic trends in recent months are a shift away from the U.S., ostensibly due to increased regulatory scrutiny, and a shift toward Singapore."

New Weapon for Blockchain Startups: Nobel Prize-Winning Brains
https://medium.com/bloomberg/new-weapon-for-blockchain-startups-nobel-prize-winning-brains-c24731883dc "With cryptocurrency mania over for now, blockchain startups need to dig a little deeper to attract attention. Their latest secret weapon: Nobel laureates."

Platforms, Hosting and Support

Fabric

-

Hyperledger Fabric

- Private business networks, IBM Bluemix hosting, or Docker containers
- Emphasizes open governance, open standards & open source

Hyperledger is:
- a Linux Foundation Project
- Hyperledger Fabric
- Hyperledger composer
- A collaborative effort created to advance cross-industry blockchain technologies for business, announced December 2015, now over 140 members. Open source, open standards, open governance. One active framework ("Fabric") and seven projects in incubation.

See also:
https://blog.acolyer.org/2018/06/04/hyperledger-fabric-a-distributed-operating-system-for-permissioned-blockchains/
Fabric is a permissioned blockchain system with the following key features:
- A modular design allows many components to be pluggable, including the consensus algorithm

- Instead of the *order-execute architecture* used by virtually all existing blockchain systems, Fabric uses an *execute-order-validate* paradigm which enables a combination of passive and active replication. (We'll be getting into this in much more detail shortly).
- Smart contracts can be written in any language.

Frabric - protocol specification on GitHub - https://github.com/hyperledger-archives/fabric/blob/master/docs/protocol-spec.md

- "The fabric is a ledger of digital events, called transactions, shared among different participants, each having a stake in the system."

Wikipedia article - https://en.wikipedia.org/wiki/Hyperledger

Hyperledger Composer modelling language

(This is probably a specific instantiation of more general concepts, but I'll leave it here until I know this)

Business Network Definitions

Business Network Definitions are composed of:

- a set of model files
- a set of JavaScript files
- an Access Control file

Diagram: https://hyperledger.github.io/composer/v0.16/assets/img/Composer-Diagram.svg

---

https://hyperledger.github.io/composer/v0.16/reference/cto_language

Model Files

A Hyperledger Composer CTO file is composed of the following elements:

- A single namespace. All resource declarations within the file are implicitly in this namespace.
- A set of resource definitions, encompassing assets, transactions, participants, and events.
- Optional import declarations that import resources from other namespaces.

Resources in Hyperledger Composer include:

- Assets, Participants, Transactions, and Events - these are resources.
    - Belongs to a namespace
    - a name, and an identifying field
    - an optional supertype, which the resource extends

        - An optional ‘abstract’ declaration (indicates this resource cannot be created, can only be extended)
        - a set of named properties, designated by o
        - a set of relationships, designated by -->
- Enumerated Types.
    - types.
- Concepts - abstract classes, eg. Address, .
    - Resources can have properties which are these

There’s more about data types, arrays, field validators (regex used to validate field), decorators (used to annotate a model with metadata)

Access control file

Access control language (defines what people can see) - standard.
Example:

```
rule SimpleRule {
    description: "Description of the ACL rule"
    participant: "org.example.SampleParticipant"
    operation: ALL
    resource: "org.example.SampleAsset"
    action: ALLOW
}
```

Queries:

Queries in Hyperledger Composer are written in a bespoke query language. Queries are defined in a single query file called (queries.qry) within a business network definition.
https://hyperledger.github.io/composer/v0.16/reference/query-language

Transaction processor functions

A transaction processor function is the logical operation of a transaction defined in a model file. For example, a transaction processor function of a Trade transaction, might use JavaScript to change the owner property of an asset from one participant to another.

Azure Blockchain Development Kit

https://github.com/Azure-Samples/blockchain/tree/master/blockchain-development-kit
Version 1 - November, 2018

Azure Blockchain Workbench Documentation
https://docs.microsoft.com/en-us/azure/blockchain/workbench/

Introducing the Azure Blockchain Development Kit
https://azure.microsoft.com/en-us/blog/introducing-the-azure-blockchain-development-kit/

- Aligned with Truffle

Truffle

https://truffleframework.com/
Blog - https://truffleframework.com/blog
Boxes: https://truffleframework.com/boxes

- Truffle - https://truffleframework.com/truffle - Truffle takes care of managing your contract artifacts so you don't have to.
- Ganache - https://truffleframework.com/ganache - one-click blockchain
- Drizzle- A collection of front-end libraries that make writing dapp user interfaces easier and more predictable.
-

Truffle—a development framework for Ethereum - http://truffleframework.com/ - Requires NodeJS 5.0+. Works on Linux, macOS, or Windows.

- "API which abstracts developers from low-level Ethereum stuff (like assembling and signing raw transactions, compiling Solidity code, working with smart contract ABIs, etc.)" https://hackernoon.com/ethereum-blockchain-in-a-real-project-with-500k-users-f85ee4821b12

- Partnership with Microsoft - https://twitter.com/trufflesuite/status/1063524049475665920 and https://www.youtube.com/watch?v=myOczdMt4Wg

v5.0.0-beta.2 – Bento Box of Candy
https://github.com/trufflesuite/truffle/releases/tag/v5.0.0-beta.2

DFINITY

https://dfinity.org/
"A blockchain supercomputer designed to host the next generation of software — Cloud 3.0"
"DFINITY is building a new kind of public decentralized cloud computing resource. This rests upon a new blockchain computer that is similar in concept to Ethereum but has vastly improved performance and, ultimately, unlimited capacity. Business applications running on this computer will be unstoppable and won't need to involve complex components such as databases, backup and restore systems or Amazon Web Services, allowing costs to be cut by 90% or more by reducing the supporting human capital required. Of course, such a powerful public resource requires governance."

- White paper - https://dfinity.org/pdf-viewer/pdfs/viewer?file=../library/dfinity-consensus.pdf

DFINITY vs. Ethereum

https://medium.com/futuresin/dfinity-vs-ethereum-44c97b4ad55b
According to CryptoBriefing, the foundational layer provided by Nervos is completely decoupled from the dApp on which it runs. Five basic components comprise the system:

1. Cells
2. Cell Types
3. Validators
4. Generators
5. Identity

Both DFINITY and Nervos give some concept of the blockchain being like a nervous system. Jan(Xie Hanjian) speaks about blockchain not just being about a trusted "engraving on the stone" metaphor, but as smart contracts that can punish bad actors. That is a new kind of automated security.

Software developer Adam Taché wrote the best intro to DFINITY I've ever read. You can read it here.
https://hackernoon.com/state-of-cryptocurrencies-summer-2018-932016549375

Quorum

https://www.jpmorgan.com/global/Quorum - by JP Morgan
"Enterprise-ready distributed ledger and smart contract platform"

- Download from GitHub https://github.com/jpmorganchase/quorum
- "Quorum supports both transaction-level privacy and network-wide transparency, customizable to business requirements"
    - All public and private smart contracts and overall system state derived from a single, shared, complete blockchain of transactions validated by every node in the network.
    - Private smart contract state is known to and validated by only parties to the contract and approved third parties, like regulators.
    - Smart contracts written for an existing Ethereum implementation remain network-transparent on Quorum out of the box.
    - Enhancing many existing smart contract designs to meet privacy requirements is simple and straightforward.
    - The Zero-knowledge Security Layer allows for cryptographically assured, private settlement of digitized assets on Quorum.
-
-

Multichain

https://www.multichain.com/
Open platform for building blockchains

Chaincode

"**Chaincode** is a program, written in Go, node.js, and eventually in other programming languages such as Java, that implements a prescribed interface. **Chaincode** runs in a secured Docker container isolated from the endorsing peer process."
https://hyperledger-fabric.readthedocs.io/en/release-1.1/chaincode.html

- Chaincode for Developers, and the other, Chaincode for Operators
- Github - https://github.com/IBM-Blockchain-Archive/learn-chaincode

Baidu - Super Chain

Baidu Blockchain as a service:
https://technode.com/2018/01/12/baidu-launches-blockchain-open-platform/

Baidu is apparently creating a blockchain system called "Super Chain," which it says will be super-fast and super-efficient.

"Super Chain can 'insert and remove consensus mechanisms to solve the current energy consumption problem," Wei explained, and is also "compatible with the development system of Bitcoin and Ethereum.'"

Alibaba - Ant Financial

Alibaba's Ant Financial has used blockchain technology (in Chinese) on its donation platform in Alipay as early as July 2016.

Ark

"ARK provides users, developers, and startups with innovative blockchain technologies. We aim to create an entire ecosystem of linked chains and a virtual spiderweb of endless use-cases that make ARK highly flexible, adaptable, and scalable. ARK is a secure platform designed for mass adoption and will deliver the services that consumers want and developers need." https://ark.io/ - explorer: https://explorer.ark.io/

- Ark! The wordpress of crypto! https://decentralize.today/some-great-projects-are-out-there-they-just-dont-talk-about-them-21d677e29ecf
- ARK Desktop Wallet is natively built for all major Operating Systems. Our full HD wallet meets the top security standards in the industry and supports the Ledger Nano S secure hardware wallet.
- Integration of Inter-planetary File System (IPFS). (See below)
- Research, Sourcing, and Development of various Smart Card/NFC materials.
- Partnerships and R&D for NFC/contact less chip and wearable devices. With optional hardware wallets.

https://decentralize.today/the-rant-76727cdf27f3
“This is a system where your grandmother can create her own blockchain-based token, when the bar next door can create their reward program with it, when the man in the street can easily create his own vision with one click.”

https://decentralize.today/ark-opportunity-knocks-12a1d62afe12
Ark—Opportunity Knocks
Web: https://ark.io/
News: https://blog.ark.io/
Forum: https://forum.ark.io/
Facebook: https://www.facebook.com/arkecosystem
Twitter: https://twitter.com/ArkEcosystem
YouTube: https://www.youtube.com/channel/UCpc2k6zOOutGT9y56urDClg
Reddit: https://www.reddit.com/r/arkecosystem
Github: https://github.com/ArkEcosystem

ARK Core v2—MainNet Launch!
https://blog.ark.io/ark-core-v2-mainnet-launch-95a5b621f6f7
ARK Core v2 is now ready for launch. We are proud to announce the final and now official release date of Wednesday, November 28th.

- Dynamic fees
- Plugin system
- Increased TPS (Transactions per Second) and TPB (Transactions per Block)
- JSON-RPC Docs : https://docs.ark.io/guidebook/core/json-rpc.html#installation
- JSON-RPC API: https://docs.ark.io/api/json-rpc/
-

Particl

https://particl.io/
Privacy-Focused Marketplace & Decentralized Application Platform

- “focus is on something called dapps which are Decentralized Applications, with the first one being a decentralized marketplace”
- “Every coin, regardless if it’s Dash, Monero, Ethereum or Bitcoin; you name it and it can be used on the marketplace. “

https://decentralize.today/some-great-projects-are-out-there-they-just-dont-talk-about-them-21d677e29ecf

“Particl is another project which powers the vision of Satoshi with its crypto agnostic Marketplace! It is a project just like Amazon but it accepts every coin and every token. This is where Blockchain is being used at its best!”

Particl—New Status Report Released
https://decentralize.today/new-status-report-released-7d24cbaaa33f

https://particl.io/status-report/
“we can announce that we have started working on an integration to the Trezor hardware wallet!”

Particl Platform: The intrinsic value of the blockchain
https://decentralize.today/particl-platform-the-intrinsic-value-of-the-blockchain-7ff12d5e6a45
“A Privacy coin in the heart of a decentralized market without intermediaries”
-m diagram - https://cdn-images-1.medium.com/max/1600/1*rzh3oUA93iNHZVgEr4tWEQ@2x.jpeg

R3 - Corda

https://www.r3.com/
Previously: R3CEV

Corda White Paper -
https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/57bda2fdebbd1acc9c0309b2/1472045822585/corda-introductory-whitepaper-final.pdf

“Corda offers the universal interoperability of public networks with the privacy of private networks”

Code on Github - https://github.com/corda/corda

https://itnext.io/whats-up-with-r3cev-f2dfccffe5b9
R3CEV-consortium consists of more than 70 of the world’s largest financial institutions. It is developing Corda, a platform that is using a “permissioned” blockchain

Meta Mask

https://metamask.io/

- MetaMask is a bridge that allows you to visit the distributed web of tomorrow in your browser today. It allows you to run Ethereum dApps right in your browser without running a full Ethereum node.
- MetaMask includes a secure identity vault, providing a user interface to manage your identities on different sites and sign blockchain transactions.
- You can install the MetaMask add-on in Chrome, Firefox, Opera, and the new Brave browser. If you’re a developer, you can start developing with MetaMask today.

Rootstock

https://www.rsk.co

“RSK is the first open-source smart contract platform with a 2-way peg to Bitcoin that also rewards the Bitcoin miners via merge-mining, allowing them to actively participate in the Smart Contract revolution. RSK goal is to add value and functionality to the Bitcoin ecosystem by enabling smart-contracts, near instant payments and higher-scalability.”
Resources

- Source code at https://github.com/RSKSmart
- RSK Stats: https://stats.rsk.co
- RSK Explorer: https://explorer.rsk.co/
- RSK Faucet: https://faucet.rsk.co/
- RSK Network status: https://twitter.com/RskSmartNetwork
- White Paper - https://docs.rsk.co/RSK_White_Paper-Overview.pdf
- Sidechains and Drivechains - https://docs.rsk.co/Drivechains_Sidechains_and_Hybrid_2-way_peg_Designs_R9.pdf
- Lumino Transaction Compression Protocol White Paper - https://docs.rsk.co/LuminoTransactionCompressionProtocolLTCP.pdf
-

Catena

https://explorecatena.com/about?lng=en
The Catena Blockchain Suite is an industry first product to quickly enable publishing of complex datasets onto public or private blockchains. Utilising smart contracts and hardware security modules, Catena enables a new level of data consistency and integrity.

- The Catena Blockchain Suite is a set of software components, and integration services, to allow organizations and governments to interface with public or private blockchains. Catena allows for public information to be permanently embedded on a private or public blockchain.
- Source code: https://github.com/explorecatena
- API - https://etherscan.io/address/0xff77e51f2c6473f72392865e0a0000de19af774a#code

Brave

This isn’t really blockchain, but I speculate here that it’s only a matter of time before someone develops a browser that mines and sends profits to websites browsed.

https://brave.com/
Brave is a free and open-source pay-to-surf[4] web browser based on the Chromium web browser and its Blink engine, announced by the co-founder of the Mozilla project and creator of JavaScript, Brendan Eich. It claims to block website trackers and remove intrusive Internet advertisements, replacing them with ads sold by Eich's company

How blockchain can help advertisers combat ‘ad blindness’
https://venturebeat.com/2018/08/12/how-blockchain-can-help-advertisers-combat-ad-blindness/
“Basic Attention Token is a known name in the young industry due to its Brave internet browser, which essentially acts like any other browser but features a more sophisticated advertising model. The browser’s 3.1 million+ monthly active users can choose to block ads entirely, filter some of them, or view them all and get paid in BAT tokens for letting the browser measure their “attention.””

Decentralized Storage

From: http://decentralized.blog/picking-a-decentralized-storage-system.html

- Decentralized Storage: The Backbone of the Third Web
- HTTP is obsolete. It's time for the distributed, permanent web
- What is the difference between Swarm and IPFS?

Decentralized storage systems (all descriptions from http://decentralized.blog/picking-a-decentralized-storage-system.html):

- Storj
- SIA
- MaidSafe
- IPFS
- ZeroNet
- Ethereum Swarm
- BigchainDB

Core Concepts

Data Structures

The basics - https://medium.freecodecamp.org/the-top-data-structures-you-should-know-for-your-next-coding-interview-36af0831f5e3

Distributed Hash Tables

- - https://en.wikipedia.org/wiki/Distributed_hash_table - “DHT research was originally motivated, in part, by peer-to-peer systems such as Freenet, gnutella, BitTorrent and Napster, which took advantage of resources distributed across the Internet to provide a single useful application. In particular, they took advantage of increased bandwidth and hard disk capacity to provide a file-sharing service.”
    - Eg. Pastry,- https://www.freepastry.org/
        - - videos where the routing (how to find values) and the dynamics
        - Applications:
            - SCRIBE group communication/event notification.
            - PAST archival storage.
            - SQUIRREL co-operative web caching.

        - SplitStream high-bandwidth content distribution.
        - POST co-operative messaging.
        - Scrivener fair sharing of resources.
    - Eg. Kademlia - white paper - https://pdos.csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf
        - Wikipedia - https://en.wikipedia.org/wiki/Kademlia
        - Overview - https://www.youtube.com/watch?v=kXyVqk3EbwE
        - the DHT protocol that is used in many popular P2P systems
    - Eg. Coral DSHT: this improves the lookup performance and decreases resource use.
    - Eg. S/Kademlia: makes Kademlia more resistant against malicious attacks.

Block Exchanges

- BitTorrent
    - Introduction - https://www.youtube.com/watch?t=961&v=kxHRATfvnlw
-

Self-Certified Filesystems - SFS

- used to implement the IPNS name system for IPFS.
- Self-Certified Filesystems: addressing remote filesystems using the following scheme: /sfs/<Location>:<HostID> where Location is the server network address, and: HostID = hash(public_key || Location)

- Thus the name of an SFS file system certifies its server.

Image of stack: http://decentralized.blog/img/ipfs-based-on.png

Directed Acyclic Graph - DAG

- **DAG stands for Directed Acyclic Graph**. In Ethereum, a DAG is created every epoch using a version of the Dagger-Hashimoto Algorithm combining Vitalik Buterin's Dagger algorithm and Thaddeus Dryja's Hashimoto algorithm. - https://ethereum.stackexchange.com/questions/1993/what-actually-is-a-dag

Explaining Directed Acylic Graph (DAG), The Real Blockchain 3.0 - https://www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acylic-graph-dag-the-real-blockchain-3-0/#44762f1f180b

- "DAG is a directed graph data structure that uses a topological ordering. The sequence can only go from earlier to later. DAG is often applied to problems related to data processing, scheduling, finding the best route in navigation, and data compression." See also image: https://thumbor.forbes.com/thumbor/960x0/https%3A%2F%2Fblogs-images.forbes.com%2Fshermanlee%2Ffiles%2F2018%2F01%2F2018-01-17-10.07.43.jpg

- "IoT Chain (ITC), IOTA, and Byteball are the blockless projects currently shining in the market. With Bitcoin or Ethereum, the block creation speed is a bottleneck. Bitcoin generates a new block every 10 minutes. Ethereum is better, but it takes around 15-20 seconds for block validation."

https://steemit.com/cryptocurrency/@heiditravels/more-than-blockchains-how-hashgraph-and-dags-are-different
Swirlds' Hashgraph isn't the only platform that's focusing on changing how a blockchain can be tweaked. Byteball and other cryptos using DAGs are more or less on the same page in regards to their ideas for providing alternative options. These are also called blockchain-free cryptocurrencies. The list of these types of cryptocurrencies includes Byteball, as I mentioned before, IOTA, and DagCoin.

Everything You Need to Know About Directed Acyclic Graphs (DAGS) - https://iota-news.com/everything-you-need-to-know-about-directed-acyclic-graphs-dags/

- **Acyclicity:** Time flows in a single direction. Newer transactions reference older ones, however, not another way around. In cycles band of tasks depend on one another (if there have been cycles there wouldn't be topological ordering). In a DAG, every node depends upon previous ones referencing it. This enables that transactions could be executed locally as well as off-line and processed, confirmed or finalized at later points.
- **Latency:** Speed of execution and confirmation times aren't constrained by block-size, but bandwidth between communicating peers. There is absolutely no theoretical limit to just how much the system can scale.
- **Feeless** ("pre-mined"): Fixed supply, no mining involved. Every transaction issuer is simultaneously a validator, or elsewhere you can find representatives or witnesses involved with cases of conflicts or disputes. This permits feeless micro and nano transactions limiting environmental impact.
- **Zero-value transactions:** E.g. messages, or non-value transactions if requiring digital signatures and fitting in a UDP packet.
- **Database pruning:** Called pruning in Nano and snapshotting in IOTA. No such mechanism yet with Byteballs. It permits keeping database slim and various nodes can save only the annals they are thinking about or is relevant in their mind.

Version Control Systems - GIT

- Blockchain: Under the Hood - Justin Ramos
- Is a Git Repository a Blockchain? - Danno Ferrin
- Is Git a Blockchain? - Dave Mercer
- The Blockchain, From a Git Perspective - Jackson Kelley

Merkle Trees

- https://hackernoon.com/merkle-trees-181cb4bc30b4 - “A Merkle tree summarizes all the transactions in a block by producing a digital fingerprint of the entire set of transactions, thereby enabling a user to verify whether or not a transaction is included in a block.” Diagram: https://cdn-images-1.medium.com/max/1000/1*UrjiK3IjdbgoV2dyKRvAGQ.png
- What is a Merkle DAG - https://github.com/ipfs/faq/issues/31 - “A Merkle DAG is a Merkle directed acyclic graph. That is a data structure similar to a Merkle tree but not so strict: such DAG does not need to be balanced and its non-leaf nodes are allowed to contain data.” - spec of IPFS Merkle DAG - https://github.com/ipfs/specs/tree/master/merkledag
- Ralph Merkle - http://www.merkle.com/ - papers - http://www.merkle.com/merkleDir/papers.html

Merkle DAG object model

- Git provides a powerful Merkle DAG object model that captures changes to a filesystem tree in a distributed-friendly way.
    - Immutable objects represent Files (blob), Directories (tree), and Changes (commit).
    - Objects are content-addressed, by the cryptographic hash of their contents.
    - Links to other objects are embedded, forming a Merkle DAG. This provides many useful integrity and workflow properties.
        - A Merkle tree is a binary tree where the parent contains the hash of the concatenation of the hashes of the two children.
        - Merkle DAG is more general as it is not a binary tree but a graph, and any node can contain data, not just the leaf nodes as in the Merkle Tree. https://github.com/ipfs/faq/issues/31
        - See: https://bmcorser.github.io/2014/12/22/merkle-dag.html
        -
    - Most versioning metadata (branches, tags, etc.) are simply pointer references
        - See: http://eagain.net/articles/git-for-computer-scientists/
    - Distributing version changes to other users is the transferring of objects and updating of remote references.

Patricia Trie (or Tree)

A *trie* (from re**trie**val), is a multi-way tree structure useful for storing strings over an alphabet. It has been used to store large dictionaries of English (say) words in spelling-checking programs and in natural-language "understanding" programs. http://www.allisons.org/ll/AlgDS/Tree/Trie/

PATRICIA - Practical Algorithm to Retrieve Information Coded in Alphanumeric, D.R.Morrison (1968). http://www.allisons.org/ll/AlgDS/Tree/PATRICIA/

https://xlinux.nist.gov/dads/HTML/patriciatree.html

- Definition: A compact representation of a *trie* in which any *node* that is an only *child* is merged with its *parent*.
- Also known as radix tree.

Patricia tree. Definition: A compact representation of a *trie* in which any node that is an only child is merged with its parent. Note: A compact directed acyclic word graph (DAWG) merges common suffix *trees* to save additional space. A *radix tree* is taken to be a binary *Patricia tree*.

- https://medium.com/coinmonks/data-structure-in-ethereum-episode-3-patricia-trie-b7b0ccddd32f Patricia trie is the main trie used in Ethereum to store data. It is a mixture of Radix trie and Merkle trie.

Patricia Tree - https://github.com/ethereum/wiki/wiki/Patricia-Tree

Hashgraph

An Overview Of Hashgraph
https://hackernoon.com/an-overview-of-hashgraph-b0900a1fd7bf
Diagram - https://cdn-images-1.medium.com/max/1600/1*SL6_XYbZit4fvIntQtnxoA.png

- Gossip Protocol - Hashgraph achieves this speed through what's called the "gossip protocol"
- Secure - The consensus algorithm of hashgraph is asynchronous byzantine fault tolerant (asynchronous BFT).
- Fair - Hashgraph also provides fair ordering and fair timestamps.

Note: Hashgraph does NOT have a cryptocurrency. Secondly, it does not have a public ledger. Instead, Hashgraph is a *permissioned* ledger.

https://ezradigital.com/blockchain-technology-hashgraph/
"Hashgraph: What is it? It's a data structure and consensus algorithm invented by Leemon Baird, the co-founder and CTO of Swirlds. It is fast (hundreds of thousands of transactions per second), secure, and evenhanded (consensus time-stamping)."

Is The Future Of Blockchains DAGs ?— 5 Takeaways From The Hashgraph Event In NYC on March 13th -
https://medium.com/crypto-oracle/is-the-future-of-blockchains-dags-5-lessons-from-the-hashgraph-event-in-nyc-on-march-13th-ff0f7e0fa510

- Hashgraph is solving for the scaling problem through their DAG (Direct Acyclic Graph), which works by combining the gossip protocol with a voting algorithm that enables Hashgraph to to reach consensus quickly and securely without proof of work.
- the organization will be overseen by a governance model mirrored after that of Visa, which was conceived by Dee Hock in the 60s. There are 39 organizations that will make up the governing council. The governance terms are being finalized, after which the 39 members will be announced.

More Than Blockchains: How Hashgraph & DAGs are Different

https://steemit.com/cryptocurrency/@heiditravels/more-than-blockchains-how-hashgraph-and-dags-are-different

Criticisms:
https://medium.com/safenetwork/parsec-a-paradigm-shift-for-asynchronous-and-permissionless-consensus-e312d721f9d8

- the Hashgraph consensus is closed source, restricting its use significantly.
- It is also unusable for our purposes as it requires a fixed set of known nodes.
- a network using the Hashgraph consensus is only proven to reach agreement if it is guaranteed that there is no sophisticated adversary on the Network.
- it has only been shown to work so far on a network in which the nodes are identified and do not change—in other words, a *permissioned network*

Hedera Hashgraph

https://www.hederahashgraph.com/

- White Paper - https://www.hederahashgraph.com/whitepaper
- "Hedera has Permissionless Consensus (or Open Consensus) with a closed Governance Model. This separation of governance from consensus is designed to ensure continued decentralization over time."

DLT Platform Hedera Hashgraph Completes $100 Million Raise
https://www.coindesk.com/dlt-platform-hedera-hashgraph-completes-100-million-raise/

Users
From:
https://medium.com/crypto-oracle/is-the-future-of-blockchains-dags-5-lessons-from-the-hashgraph-event-in-nyc-on-march-13th-ff0f7e0fa510

- Xtremepush is leveraging Hedera to solve for click fraud. - https://xtremepush.com/
- CU Ledger is serving 250 million credit union members around the world and using Hedera to solve for a part of the cross border international payments process. http://culedger.com/
- Intiva Health is using Hedera to solve for the ongoing credentialing of doctors, nurses and other health care professionals - https://intivahealth.com/
- The game studio Machine Zone, with over hundreds of millions of game downloads, is leveraging Hedera to solve for Satori, a distributed AI Mesh, which can process 500 million events a second. A highlight of the Hadera conference was the thirteen minute talk given by Machine Zone CEO. - https://www.mz.com/

Tangle

Fabric

(Not to be confused with Fabric, the blockchain project by the Linux Foundation)

https://fabric.fm/

“Everything is content-addressable, so links are generally fabric://<sha256>, where <sha256> is the hash of the requested document — this way, any peer in the network can respond to a request” (Gitter Solid/Chat July 5, 2018 Eric Martindale)

SAFE / PARSEC

https://safenetwork.org/
“The SAFE Network is a decentralized data storage and communications network that provides a secure, efficient and low-cost infrastructure for everyone.”
SAFE browser - https://safenetwork.org/downloads/
SAFE API - https://forum.safedev.org/t/safe-network-api-getting-started-draft/726

- 24 may 2018:
- Introducing PARSEC: A paradigm shift for highly asynchronous and permissionless consensus. https://medium.com/safenetwork/parsec-a-paradigm-shift-for-asynchronous-and-permissionless-consensus-e312d721f9d8
- White paper - http://docs.maidsafe.net/Whitepapers/pdf/PARSEC.pdf

Peer-to-Peer (P2P) Technologies

Kademlia

Kademlia is a distributed hash table for decentralized peer-to-peer computer networks designed by Petar Maymounkov and David Mazières in 2002.[1][2] It specifies the structure of

the network and the exchange of information through node lookups. Kademlia nodes communicate among themselves using UDP. A virtual or overlay network is formed by the participant nodes. Each node is identified by a number or *node ID*. The *node ID* serves not only as identification, but the Kademlia algorithm uses the *node ID* to locate values (usually file hashes or keywords). In fact, the *node ID* provides a direct map to file hashes and that node stores information on where to obtain the file or resource. - from https://en.wikipedia.org/wiki/Kademlia

Decentralized Semantic Web applications

- identity, authentication, and authorization
- improving the onboarding experience for new users
- client-side Linked Data access and manipulation
- applications of Linked Data Notifications
- provenance, trust, and claim verification
- http://iswc2018.desemweb.org/

-

Inter Planetary File System (IPFS)

Overview

IPFS white paper: IPFS - Content Addressed, Versioned, P2P File System (DRAFT 3).
Diagrams of stack:

- http://decentralized.blog/img/ipfs-stack.jpg
- http://decentralized.blog/img/thin-waist.jpg
    - *both images from presentations by Juan Benet (the BDFL of IPFS).*

“a new Internet protocol initially designed by Juan Benet in 2014 with the goal of storing data permanently, remove duplications across the network, and obtain addresses to information stored on network computers.”
https://blog.rubiksdigital.com/how-ipfs-is-disrupting-the-web-e10857397822

On GitHub: https://github.com/ipfs/ipfs

IPFS Introduction by Example
https://whatdoesthequantsay.com/2015/09/13/ipfs-introduction-by-example

10.05: Break on through (to the other side)
https://mailchi.mp/technologyreview/93-cloudflares-gateway-to-a-user-run-internet?e=859794f490 - overview of IPFS and Cloudflare

Core Concepts

From http://decentralized.blog/getting-to-know-ipfs.html :

- IPFS consists of a network of peer-to-peer nodes (aka computers that talk to each other directly)
- These nodes can store content (any type of file)
- Content is represented by a hash and is immutable (if the content changes, so does the hash) - In the case of IPFS, the key of the distributed hash table is a hash over the content.
- A node can request content from other nodes by using this hash. This is pretty cool: **there is a permanent relation between the hash and the content itself.** Unlike the current web where the content behind a URL can change.
    - Example:
      http://decentralized.blog/understanding-the-ipfs-white-paper-part-1.html
      $ ipfs dht findpeer
      QmYebHWdWStasXWZQiXuFacckKC33HTbicXPkdSi5Yfpz6

      /ip4/176.92.234.78/tcp/4001
      /ip4/85.74.239.218/tcp/38689
      /ip4/127.0.0.1/tcp/4001
      /ip4/192.168.1.30/tcp/4001
      /ip6/::1/tcp/4001
      /ip4/192.168.1.3/tcp/4001
      /ip4/176.92.234.78/tcp/40443
    -
- Nodes can decide to store a copy of any content
- The more nodes store a piece of content the harder it is to get rid of it (the permanent web).
- The network also gets faster that way, similar to bittorrent getting faster when the number of seeders goes up (IPFS is partly based on the bittorrent protocol, but one of the differences is that it prevents duplicate pieces of identical content)
    - The IPFS BitTorrent variety is called **BitSwap**
    - two BitTorrent features that IPFS uses: (http://decentralized.blog/understanding-the-ipfs-white-paper-part-1.html)
        - tit-for-tat strategy (if you don't share, you won't receive either)
        - get rare pieces first (improves performance and more, see the first PDF above)
        - where in BitTorrent each file has a separate swarm of peers (forming a P2P network with each other) where IPFS is one big swarm of peers for all data.

Hosting a website on IPFS - https://ipfs.io/ipfs/QmdPtC3T7Kcu9iJg6hYzLBWR5XCDcYMY7HV685E3kH3EcS/2015/09/15/hosting-a-website-on-ipfs/

-

IPFS Secure File Sharing

- Learn to securely share files on the blockchain with IPFS! https://medium.com/@mycoralhealth/learn-to-securely-share-files-on-the-blockchain-with-ipfs-219ee47df54c

KeySpace: End-to-End Encryption Using Ethereum and IPFS
https://medium.com/fluidity/keyspace-end-to-end-encryption-using-ethereum-and-ipfs-87b04b18156b
KeySpace is a trustless end-to-end encryption protocol that launched as part of AirSwap Spaces.

IPFS Crawling

- Writing a simple IPFS crawler - https://gkbrk.com/2018/03/writing-a-simple-ipfs-crawler/

Decentralized Documents

Open Document Repository - by Kubrick (might be dead)
https://github.com/DaMaHub/opendocumentrepository

Decentralized Databases

https://www.blockchainforscience.com/2017/02/23/blockchain-for-open-science-the-living-document/
Storj, filecoin, swarm and MaidSAFE are also interesting concepts. They can be seen as blockchain-based, distributed cloud services to store data, files (or to provide services…). Coins are used to incentivise resource providers who provide hard drive space and network bandwidth (‘the permanent web’ - ‘Web 3.0’ to stress some buzzwords).

Linked Data

Semantic Web

Yeah.. a level 4 heading for semantic web

JSON-LD

https://json-ld.org/
“JSON-LD is a lightweight Linked Data format. It is easy for humans to read and write. It is based on the already successful JSON format and provides a way to help JSON data interoperate at Web-scale.”

Linked Data and Distributed Ledgers

Jan, Z., Third, A., Ibanez, L., Bachler, M., Simperl, E. and Domingue, J. (2018) ScienceMiles: Digital Currency for Researchers Workshop: 3rd International Workshop on Linked Data and Distributed Ledgers at The Web Conference, Lyon, France, International World Wide Web Conferences Steering Committee, kmi Member Submission http://oro.open.ac.uk/54748/1/54748.pdf

Third, A. and Domingue, J. (2017) Linked Data Indexing of Distributed Ledgers Workshop: LD-DL@WWW 1st International Workshop on Linked Data and Distributed Ledgers at WWW 2017 The 26th International World Wide Web Conference, Perth, Australia http://papers.www2017.com.au.s3-website-ap-southeast-2.amazonaws.com/companion/p1431.pdf
“We have implemented a semantic index to the Ethereum blockchain platform, to expose distributed ledger data as Linked Data.”

English, M., Auer, S. and Domingue, J. (2016) Block Chain Technologies & The Semantic Web: A Framework for Symbiotic Development Computer Science Conference for University of Bonn Students, Bonn, Germany http://cscubs.cs.uni-bonn.de/2016/proceedings/paper-10.pdf “ we first demonstrate how block chain technologies can contribute toward the realization of a more robust Semantic Web, and subsequently we provide a framework wherein the Semantic Web is utilized to ameliorate block chain technology itself.”

LinkChains

Third, A. and Domingue, J. (2017) LinkChains: Exploring the space of decentralised trustworthy Linked Data Workshop: Decentralising the Semantic Web at International Semantic Web Conference, Vienna, Austria https://openreview.net/pdf?id=HJhwZNKIb “We describe potential approaches to the storage and querying of Linked Data with varying degrees of decentralisation and guarantees of integrity, using distributed ledgers, and discuss their a priori differences in performance, storage limitations and reliability, setting out a programme for future empirical research.”

OrbitDB

https://github.com/orbitdb - Peer-to-Peer Databases for the Decentralized Web

Decentralized Database Projects

IPLD - Inter Planetary Linked Data

- IPLD website (Inter Planetary Linked Data) - https://ipld.io/
- the IPLD specs and the IPLD implementations.
-

DAT Project

https://datproject.org/
“Modeled after the best parts of Git, BitTorrent, and the internet, the Dat Protocol is a peer-to-peer protocol for syncing files and data across distributed networks.”

Dat Base - Dat for Researchers

- Open Data: archive, catalogue, and share data pipelines.
- Public Archives: archiving public data at risk of being lost.

Dat Protocol - Build Custom Dat Apps

- Live Syncing: easy file transfers, distributed databases, p2p streams.
- Futuristic: interoperable and peer-to-peer by default.

Decentralized Web - Peer-to-peer websites

- Beaker Browser: browse, create, and host websites over Dat.
- Direct Sharing: share files a unique URL.

Repux.io

decentralised data marketplace - https://repux.io
https://www.reddit.com/user/RepuX_on_Reddit

Swarm

Swarm http://swarm-gateways.net/bzz:/theswarm.eth/
“Swarm is a distributed storage platform and content distribution service, a native base layer service of the ethereum web3 stack. The primary objective of Swarm is to provide a decentralized and

redundant store for dapp code and data as well as block chain and state data. Swarm is also set out to provide various base layer services for web3, including node-to-node messaging, media streaming, decentralised database services and scalable state-channel infrastructure for decentralised service economies."

- Alpha public pilot - https://blog.ethereum.org/2016/12/15/swarm-alpha-public-pilot-basics-swarm/
- Swarm Guide - https://swarm-guide.readthedocs.io/

A Swarm network is a network of nodes running a wire protocol called bzz using the ethereum devp2p/rlpx network stack as the underlay transport.

- The Swarm protocol (bzz) defines a mode of interaction.
- At its core, Swarm implements a *distributed content-addressed chunk store*. Chunks are arbitrary data blobs with a fixed maximum size (currently 4KB).
- Content addressing means that the address of any chunk is deterministically derived from its content.
- The addressing scheme falls back on a hash function which takes a chunk as input and returns a 32-byte long key as output. A hash function is irreversible, collision free and uniformly distributed (indeed this is what makes bitcoin, and in general proof-of-work, work).
- This hash of a chunk is the address that clients can use to retrieve the chunk (the hash's *preimage*).
- a chunk-to-be-stored or a content-retrieval-request message can always be efficiently routed along these peer connections to the nodes that are nearest to the content's address. This flavour of the routing scheme is called *forwarding Kademlia*.
- Swarm uses the Ethereum Name Service (ENS) to resolve domain names to Swarm hashes.

If you use the Swarm proxy for browsing, the client assumes that the domain (the part after bzz:/ up to the first slash) resolves to a content hash via ENS.

Storj

https://storj.io/
"We're building the next generation of decentralized object storage, end-to-end encrypted, where only you have access to your data. Powered by blockchain payments."
""Storj is like an Internet filesystem. Data blocks are encrypted and distributed across a globally distributed set of storage nodes using block-chain algorithm. It is quite impressive and much needed innovation in the storage space.""

- Blog: https://blog.storj.io/

Problems with Storj - https://medium.com/mobius-network/why-ethereum-should-be-worried-about-filecoin-ce9af5ecec6b

Filecoin

“Instead of Proof of Work (PoW) mining, Filecoin uses Proof of Storage (PoS) to secure the network! Pretty cool” - https://medium.com/mobius-network/why-ethereum-should-be-worried-about-filecoin-ce9af5ecec6b

- “In Filecoin the “gas” payments go to “miners” who instead of running massive computers doing useless mining are instead storing data that people are also paying them to store!”
- “Imagine if instead of the Ethereum miners doing useless work they were doing useful computation such as 3D rendering and Pixar was paying them to render the movies—yes that is what Filecoin is doing via file storage!”

https://filecoin.io/
“Put your unused storage to work by becoming a Filecoin miner. Use the Filecoin mining software to get paid for fulfilling storage requests on the Filecoin market.”
“Clients can tune their storage strategy to suit their needs, creating a custom balance between redundancy, speed of retrieval, and cost. The worldwide Filecoin storage and retrieval markets make vendors compete to give you flexible options at the best prices.”

- White Paper - https://filecoin.io/filecoin.pdf
- Blog - https://filecoin.io/blog/

Why Ethereum Should be Worried About Filecoin
https://medium.com/mobius-network/why-ethereum-should-be-worried-about-filecoin-ce9af5ecec6b

- “Filecoin improves upon Storj and Sia in two key ways:
    - Proofs of Replication (PoRep) allows U (and the public) to know that multiple copies of F are stored in the system without encrypting F with a secret key.
    - Proofs of Space Time (PoST) allow for less frequent question and answering of P to prove it has F stored

Mobius - working on this - https://mobius.network/

Maidsafe

https://maidsafe.net/
“Blockchain based storage solutions that store a data identifier (e.g. hash) in a blockchain, but store the data 'somewhere else' do not improve the security of our data. That 'somewhere else' still needs to be secured, and if this data can be deleted, or our access denied these 'solutions' are not fit for purpose. The SAFE Network removes people from the management of our information to protect the world's data.”

Not blockchain, not DAG

https://www.maidsafe.net/ - “The SAFE network is autonomous and decentralised. It is not a set of federated servers, or owned storage locations, or identifiable nodes, nor does it contain a blockchain.”

- PARSEC (Protocol for Asynchronous, Reliable, Secure and Efficient Consensus) white paper: http://docs.maidsafe.net/Whitepapers/pdf/PARSEC.pdf - “byzantine fault tolerant consensus algorithm withvery weak synchrony assumptions.”
- https://medium.com/safenetwork/parsec-a-paradigm-shift-for-asynchronous-and-permissionless-consensus-e312d721f9d8

Sia

https://sia.tech/
“Sia is a decentralized storage platform secured by blockchain technology. The Sia Storage Platform leverages underutilized hard drive capacity around the world to create a data storage marketplace that is more reliable and lower cost than traditional cloud storage providers.”

Token-Curated Registries

Token-Curated Registries 1.0
https://medium.com/@ilovebagels/token-curated-registries-1-0-61a232f8dac7
“Token-curated registries are decentrally-curated lists with intrinsic economic incentives for token holders to curate the list’s contents judiciously.”

“Levels” as an experiment for increasing participation in TCRs
https://medium.com/@mentapurpura/levels-for-tcrs-7816e38e0f95
Cryptosystems Productization Lab (part of ConsenSys), … recent forays into token-curated registries (AdChain, Delphi) have surfaced the particular importance of levels in our work.

- “how can we ensure that new, not-as-wealthy users have an active participation in token-curated registries, when whales tend to be over-represented?”

Distributed Applications -

Ethereum DApp

“A dapp is a decentralised app. For us old school web developers this can be hard to grasp: there is no server. Instead, “backend” code runs on a decentralised peer-to-peer network of nodes and “frontend” code is served from a distributed CDN.”
https://hackernoon.com/crossing-over-to-web3-an-introduction-to-decentralised-development-5eb09e95edb0
Image: https://cdn-images-1.medium.com/max/1000/1*GD9K6mnI7NhKSf6g5PpL_A.png

The dApp Design Pattern - https://medium.com/radarrelay/the-dapp-design-pattern-fe786b8da8a9

- “At Radar we consider dApps to be an application design pattern that augments modern web applications by distributing critical components across a network of peers or nodes.”
- Goals:
    - Mitigate Single Points of Failure (SPOF)
    - Reduce Reliance on Central Authorities

40 Ethereum Apps You Can Use Right Now
https://media.consensys.net/40-ethereum-apps-you-can-use-right-now-d643333769f7
“Although the blockchain ecosystem will take time to fully develop and enmesh with economies-at-large, we’re already seeing many organizations deliver applications that interact with the Ethereum blockchain to create new modes of creating and exchanging value.”

3rd Generation dAPPs

Third Generation Blockchains
https://medium.com/@Michael_Spencer/third-generation-blockchains-7d6137e3f78b
“we are entering a 3.0 phase, where features such as scalability, interoperability (side chains), treasury systems and on-chain governance play key roles; according to Charles Hoskinson.”

Toshi

- Toshi—Live Ethereum Dapp - “a WEB3 Browser that features a lot of Dapps that can be used today.” - https://medium.com/old-school/toshi-live-ethereum-dapp-d1922b792aa1
- closely related to Coinbase - fully owned project of Coinbase.

Metamask

- MetaMask—a browser extension allowing users to to run dApps without running an entire Ethereum node

- State of the DApps lists over 1,500 DApps (May 24, 2018), but those are only the ones that State of the DApps has chosen to highlight. There could be many more out there too.

Centrality

https://www.centrality.ai/

- White Paper - https://www.centrality.ai/wp-content/uploads/2018/01/Centrality-Whitepaper-final-2018020.pdf
- - Blog - https://medium.com/centrality

New Zealand-based Blockchain DApp platform Centrality announced a partnership with China tech giant InfiniVision and Japan-based Jasmy—

Nervos

“Nervos is network of scalable and interoperable blockchains built on top of an open network, built for the enterprise.”
http://www.nervos.org/

- White paper: https://github.com/NervosFoundation/binary/blob/master/whitepaper/nervos-ckb.pdf

Introducing Nervos Network
https://medium.com/futuresin/dfinity-vs-ethereum-44c97b4ad55b
Nervos, a network of interoperable protocols that allows enterprises to build and deploy decentralized applications (dApps) without committing their tech stack fully to the blockchain.

Nervos ICO Review And Token Analysis
https://cryptobriefing.com/nervos-ico-review-token-analysis/

Diagram - https://cdn-images-1.medium.com/max/800/1*kYjGgMEEGSlsGbT7tjyRNA.png

Nervos Common Knowledge Base (CKB)

The Layer 1 for All Layer 2 Protocols

Search

Nebulas (NAS): Creating A Search Engine For The BlockChain Community
http://todaysgazette.com/nebulas-nas-creating-a-search-engine-for-the-blockchain-community/

Distributed Computing

The Big Five Blockchain 3.0 Contenders: The crypto space is moving fast, and the pressure is on the big five: Ethereum, EOS, Cardano, Stellar and NEO.

DFINITY

https://dfinity.org/
“A public decentralized cloud designed to host the next generation of software and services.”

DFINITY is the Cloud 3.0 that Marries Crypto Valley with Silicon Valley

https://medium.com/futuresin/dfinity-is-the-cloud-3-0-that-marries-crypto-valley-with-silicon-valley-f44ae4bdfd11
DFINITY is building a new kind of virtual computer driven by blockchain technology. It's building an open, decentralized blockchain that runs smart contract software systems with vastly improved performance, capacity, and algorithmic governance.

Distributed Organizations

Distributed Business Models

---
https://medium.com/@RobinsonBenP/firms-need-business-model-change-not-blockchain-bc8b0b2466bb
Uber business model - diagram -
https://cdn-images-1.medium.com/max/800/1*IXUH5ynzMQ50JZ5K6y0Otw.jpeg

"It wasn't the smartphone that created Uber. Instead, it took business model change which exploited new technologies…. And so in banking we can safely predict that it won't be blockchain or APIs or AI that transform the industry. Instead, it will be new business models empowered by those technologies."

Technology and platforms have neutralized scale advantages
In their recent book, Unscaled, Hemant Taneja and Kevin Maney talk about how the technologies of cloud and AI have turned scale economies on their head.

Economies of scale graphs:
https://cdn-images-1.medium.com/max/800/1*3VPVMfKZBzcaDdvpUeHdqA.jpeg
https://cdn-images-1.medium.com/max/800/1*0-LwCJAAn8I4wIr8KND05w.jpeg

---

The aggregator model

https://medium.com/@RobinsonBenP/firms-need-business-model-change-not-blockchain-bc8b0b2466bb
The aggregator model is where a firm uses its grip over distribution to introduce the consumer to the right unbundled services.
Diagram: https://cdn-images-1.medium.com/max/800/1*kduCA8nGJGnZb_72rEQA-Q.jpeg

The Holding Company Model

https://medium.com/@RobinsonBenP/firms-need-business-model-change-not-blockchain-bc8b0b2466bb

The holding company model attempts to replicate the universal banking model—or conglomerate model in other industries—for the unscaled world and in a way that confers competitive advantage on the subsidiaries, especially by dint of network effects.
Diagram: https://cdn-images-1.medium.com/max/800/1*gpXJpdSUYpOkWC6rFlss7g.jpeg

Marketplaces

Data Marketplaces

https://medium.com/@FEhrsam/blockchain-based-machine-learning-marketplaces-cb2d4dae2c17
"No one has created a successful blockchain-based marketplace for data yet. The Ocean is an early attempt to outline one." (see The Ocean, above)

"A fascinating end state would be mutually owned metamodels which give data providers and model creators ownership proportional to how much smarter they've made them. The models would be tokenized, could pay dividends over time, and potentially even be governed by those who trained them. A sort of mutually owned hive mind. The original Openmined video is the closest construction to this I have seen so far."

Secure Computing

https://medium.com/@FEhrsam/blockchain-based-machine-learning-marketplaces-cb2d4dae2c17
Openmined is creating a multiparty compute network for training machine learning models on top of Unity that can run on any device, including game consoles (similar to Folding at Home), then expanding to secure MPC. Enigma has a similar tact.

Machine Learning Marketplaces

https://medium.com/@FEhrsam/blockchain-based-machine-learning-marketplaces-cb2d4dae2c17

"Machine learning models trained on data from blockchain-based marketplaces have the potential to create the world's most powerful artificial intelligences. They combine two potent primitives: private machine learning, which allows for training to be done on sensitive private data without revealing it, and blockchain-based incentives, which allow these systems to attract the best data and models to make them smarter."

"The base of this idea came in 2015 from talking with Richard of Numerai. Numerai is a hedge fund that sends encrypted market data to any data scientist who wants to compete to model the stock market. Numerai combines the best model submissions into a "metamodel", trades that metamodel, and pays data scientists whose models perform well."

Dragram: https://cdn-images-1.medium.com/max/600/1*Gijb5M3zuLRbXaDmVAS0JA.jpeg

“a major feature is privacy. It allows 1) people to submit data that otherwise would be too private to share and 2) prevents the economic value of the data and models from leaking”

Benefits

https://medium.com/@FEhrsam/blockchain-based-machine-learning-marketplaces-cb2d4dae2c17

“First, decentralized machine learning marketplaces can dismantle the data monopolies of the current tech giants. They standardize and commoditize the main source of value creation on the internet for the last 20 years: proprietary data networks and the strong network effects surrounding them. As a result, value creation gets moved up the stack from data to algorithms.
Diagram: https://cdn-images-1.medium.com/max/800/1*VVCasQUJ-YFSIpUOwROx-g.png

Second, they create the most powerful AI systems in the world

Third, as the recommender system example shows, search gets inverted. Instead of people searching for products, products search and compete for people

Fourth, they allow us to get the same benefits of the powerful machine-learning based services we are used to from companies like Google and Facebook without giving away our data.

Fifth, machine learning can advance more quickly, as any engineer can access an open marketplace for data, not just a small group of engineers in the large Web 2.0 companies.”

The ultimate recommender engine

https://medium.com/@FEhrsam/blockchain-based-machine-learning-marketplaces-cb2d4dae2c17

- - “More than any of the existing data silos of Google, Facebook, or others could ever be because it has a maximally longitudinal view of you and it can learn from data that otherwise would be too private to consider sharing”
- Google’s federated learning and Apple’s differential privacy are one step in this private machine learning direction, but still require trust, don’t allow users to directly examine their security, and keep data siloed.
- Diagram - https://cdn-images-1.medium.com/max/800/1*qzr0K7_EtraMhfUa2ywdSA.png

Numer.ai

https://numer.ai/homepage
“Because Numerai abstracts its financial data, data scientists do not know what the data represents and human biases and overfitting are overcome.”

White Paper - https://numer.ai/static/media/whitepaper.29bf5a91.pdf

---

Distributed AI Mesh

AI Mesh is a routing concept - https://www.asus.com/AiMesh/

Satori, a distributed AI Mesh

https://ezradigital.com/blockchain-technology-hashgraph/
“Keeping in the vein of smart technology, there’s Satori—the world’s decentralized AI mesh. It’s also a secure, distributed, artificial intelligence platform that offers real-time data analysis. Subscribers spend LIT Tokens which allow access to Streambots and live data streams.”

LIT, by Satori - https://lit.io/
“Evolving beyond smart contracts, LIT tokens open Satori, the world’s decentralized AI mesh, to the public.”

Powering the World’s Decentralized AI Mesh -
https://lit.io/uploads/littokenbysatori_summary.pdf
“Satori's AI Streambots effortlessly consume and process data, audio and video, from around the world to offer better real-time decision-making tools to businesses, consumers, and smart cities”

Satori is Powering the World’s Decentralized AI Mesh—Gabe Leydon explains
https://medium.com/hashgraph/satori-is-powering-the-worlds-decentralized-ai-mesh-gabe-leydon-explains-d6986a0011b2

- Satori is a distributed compute platform that is layered on top of the Hashgraph Consensus protocol

The Scoop on Blockchain Technology & Decentralized AI Mesh
https://ezradigital.com/blockchain-technology-hashgraph/

Subscriptions

Technical Deep Dive: Architecture Choices for Subscriptions on the Blockchain (ERC948)
https://medium.com/gitcoin/technical-deep-dive-architecture-choices-for-subscriptions-on-the-blockchain-erc948-5fae89cabc7a
“Subscriptions are one of the healthiest monetization methods on the legacy web. At Gitcoin, we believe this will prove to be so on Web 3.0, as well. Unlike surveillance capital based models, subscriptions still fit within the Web 3 ethos”

Participatory Design

Participatory Design for Cryptoeconomic Systems
https://medium.com/@mentapurpura/participatory-design-for-cryptoeconomic-systems-ab4d2eb5712
“Participatory design is characterized by an opening of the design process to non-designers. It is an active creation of spaces, moments, and methods that fosters and empowers users during the design process. In other words, the users get a say in what is being created by and for them.”
Example diagram:
https://cdn-images-1.medium.com/max/1000/1*NOXgm7wsSkpUTgIt6AS_NQ.png

DAO

“DAOs are decentralized and autonomous organizations that operate using smart contracts.
The smart contracts contain the rules and operating structure of the organization, eliminating the need for centralized control and leadership.” https://kingpassive.com/what-is-ethereum/

- Diagram - https://kingpassive.com/wp-content/uploads/2018/05/The-DAO-.jpg
-

DAO stands for “Decentralized Autonomous Organization” and a fund was created in Ethereum as a way to show what the platform could do. Users could deposit money to the DAO and get returns based on the investments that the DAO made.

https://medium.com/@jimmysong/the-truth-about-smart-contracts-ae825271811f

- Many called the person draining the DAO of money a “hacker”. In the sense that the “hacker” found a way to take money from the contract in a way not intended by the creators intended, this is true. But in a broader sense, this was not a hacker at all, just someone that was taking advantage of the quirks in the smart contract to their advantage.
- Ethereum decided that code no longer is law and reverted all the money that went into the DAO. In other words, the contract writers and investors did something stupid and the Ethereum developers decided to bail them out.

Distributed Social Networks

How the Blockchain Can Solve Social Media’s Biggest Problems
https://medium.com/forbes/how-the-blockchain-can-solve-social-medias-biggest-problems-e438f3132cd2 “By utilizing the private ledger the Ethereum blockchain provides, companies can better track user interaction with content. This will enable the quantification of user’s worth to the network, and therefore a better idea of how they should be compensated for their activity.”

Steemit

https://steemit.com/

https://angel.co/steemit

Built off the Steem blockchain, Steemit is a Reddit-esque social platform that as of now boasts nearly 800,000 registered users. Steemit's version of upvotes, however, are tokens that hold real market value. Users—not advertisers—are rewarded for engagement.

https://en.wikipedia.org/wiki/Steemit
"Steemit is a blogging and social networking website that uses its Steem blockchain-based rewards platform for publishers. The Steem blockchain produces Steem and Steem Dollars which are tradable tokens obtained for posting, discovering, and commenting on content."

Sapien

https://www.sapien.network/
"Sapien is a Web 3.0 social news platform that gives users control of their data, rewards content creators, and fights fake news."

https://angel.co/sapien-social-platform
Steemit is a social media platform where everyone gets paid for creating and curating content. It leverages a robust digital points system, called Steem, that supports real value for digital rewards through market price discovery and liquidity.

BUIDL

How to BUIDL a Mesh Network of Human Beings
https://medium.com/gitcoin/how-to-buidl-a-mesh-network-of-human-beings-a5293ecca60a
"Each node in this network is a full 3-dimensional human; with a diversity of backgrounds, experience, and culture. Every person in this network has their own personal preferences, ambitions, habits, hobbies, other time commitments, biases, family, & personal challenges."

Research Projects

Blockchain Research Institute

https://www.blockchainresearchinstitute.org/
The Blockchain Research Institute (BRI) is an independent, global think-tank, co-founded by Don and Alex Tapscott.

- Slides - https://blockchainwest.com/assets/client_files/files/presentation/Tapscott%20Blockchain.pdf

MIT Digital Tradecoin

https://tradecoin.mit.edu/

- *Breaking the Bank*, A. Lipton and A. Pentland, **Scientific American (PDF)** (January 2018) - good illustration comparing central bank, bitcoin, tradecoin
- *Digital Trade Coin (DTC): Towards a more stable digital currency*, A. Lipton, T. Hardjono and A. Pentland - **(PDF)** Full Paper (January 2018)
- MarketWatch (Feb 2018)
- *Narrow Banks and Fiat Backed Digital Coins*, A. Lipton, A. Pentland and T. Hardjono, Capco Institute Journal 47, April 2018. (**PDF**)

DreamTeam

"binding Ethereum blockchain to our product, DreamTeam, the first esports and gaming recruitment and management network."
https://hackernoon.com/ethereum-blockchain-in-a-real-project-with-500k-users-f85ee4821b12

Technology Stack

We use microservice architecture along with continuous integration, where the blockchain solution consists of four logical parts:

- Solidity with Truffle framework for development and deployment of Ethereum smart contracts.
- Geth blockchain client node.
- NodeJS backend with MongoDB.
- RabbitMQ message broker for all blockchain transactions.

Let's briefly walk through all technical internals and discuss why we have decided to build the platform this way.

Cryptokitties

CryptoKitties is an Ethereum-based game that allows players to buy, collect, breed, and even sell virtual cats. - https://kingpassive.com/what-is-ethereum/

https://www.howtogeek.com/354535/what-the-is-a-cryptokitty/

Cryptokitties may be going bust - http://fortune.com/2018/06/18/cryptokitties/

A cryptokitty is an ERC721 token
https://medium.com/crypto-currently/the-anatomy-of-erc721-e9db77abfc24
Detailed explanation: https://medium.com/crypto-currently/the-anatomy-of-erc721-e9db77abfc24

https://en.wikipedia.org/wiki/Cryptokitties
https://www.cryptokitties.co/Technical-details

https://thebitcoin.pub/t/cryptokitties-isn-t-about-the-cats-hint-erc-721/23883

CryptoKitties: Are blockchain Beanie Babies the future of e-commerce or a fad?
https://ca.finance.yahoo.com/news/cryptokitties-blockchain-beanie-babies-future-135159686.html

The weird, wild and expensive world of blockchain art
https://www.engadget.com/2018/08/30/cryptokitties-gods-unchained-blockchain-art/

Decentraland

https://decentraland.org/
Decentraland is a virtual reality platform powered by the Ethereum blockchain. Users can create, experience, and monetize content and applications

- White Paper - https://decentraland.org/whitepaper.pdf
- "Decentraland began as a proof of concept for allocating ownership of digital real estate to users on a blockchain. This digital real estate was initially implemented as a pixel on an infinite 2D grid, where each pixel contained metadata identifying the owner and describing the pixel's color."
- Docs - https://docs.decentraland.org/docs
- Blog - https://blog.decentraland.org/

CryptoPunks

https://www.larvalabs.com/cryptopunks
"10,000 unique collectible characters with proof of ownership stored on the Ethereum blockchain. Featured in Mashable, The Financial Times, The Paris Review, Salon and The New York Times."

- "CryptoPunks are almost an ERC20 token. We support the methods that provide your balance so you can watch CryptoPunks as a token in your wallet and see how many you own."
- GitHub - https://github.com/larvalabs/cryptopunks

Cryptostrikers

blockchain-based sports cards, starting with 2018 World Cup.
https://medium.com/cryptostrikers/why-were-putting-sports-cards-on-the-blockchain-c00112150033

Ripple Research Initiative

UW gets research funding for deep dive into blockchain technology
Waterloo is only Canadian institution to take part in $50-million Ripple research initiative

https://www.therecord.com/news-story/8653190-uw-gets-research-funding-for-deep-dive-into-blockchain-technology/

Bitnation

https://tse.bitnation.co/

Bitnation is the world's first Decentralised Borderless Voluntary Nation (DBVN). Bitnation started in July 2014 and hosted the world's first blockchain marriage, birth certificate, refugee emergency ID, World Citizenship, DBVN Constitution and more. The website proof-of-concept, including the blockchain ID and Public Notary, is used by tens of thousands of Bitnation Citizens and Embassies around the world. Bitnation is the winner of UNESCO's Netexplo Award 2017, and has been featured by the Wall Street Journal, Bloomberg, BBC, CNN, WIRED, VICE, TechCrunch, The Economist, Russia Today among many others.

KORD

(formerly META) https://github.com/kord-network/docs - https://github.com/meta-network

KORD is both a network of distributed, decentralised systems (the KORD network), and a protocol which governs how those systems communicate (the KORD protocol).

- JAAK announced META - https://cointelegraph.com/news/jaak-announces-meta-decentralized-network-backed-by-ethereum-and-swarm
- go-kord - The Go KORD library

Blockchain Center of Excellence

JP Morgan - The Blockchain Center of Excellence (BCOE) leads efforts for applications of distributed ledger technology (DLT) within J.P. Morgan. We are exploring blockchain use cases and piloting solutions across business lines. We are active in the blockchain ecosystem: developing technology, investing in strategic partnerships, and participating in cross-industry consortia. https://www.jpmorgan.com/global/blockchain

RCanopus Consensus Protocol

http://blizzard.cs.uwaterloo.ca/sirius/index.php/scalable-consensus/sirius-consensus-protocol/

- "The goal of the RCanopus consensus protocol is to allow Byzantine Fault Tolerance and high transaction rates (our target is 1 million transactions per second) with sub-second latency in a globally-distributed permissioned setting."
- "RCanopus is intended to be used as a part of a permissioned blockchain, such as Hyperledger Fabric or Parity Substrate's Ethereum PoA.RCanopus is intended to be used as a part of a permissioned blockchain, such as Hyperledger Fabric or Parity Substrate's Ethereum PoA.

Project Aiur

https://www.forbes.com/sites/kittyknowles/2018/06/13/blockchain-science-iris-ai-project-aiur-elsevier-academic-journal-london-tech-week-cogx/#2e046fa91e0a
Could blockchain be what brings science's untouchable publishing giants down? Norway's Anita Schjøll Brede, cofounder and CEO at Iris.AI - https://the.iris.ai

Schjøll Brede's new side project is called Project Aiur (a name which references the hit PC game StarCraft). Its aim? To use the blockchain to support a transparent AI peer review and publishing service with its own online economy.

Individuals can contribute in many ways, building useful research tools, publishing their own studies to the platform, peer reviewing work and training the platforms AI to automate the process.
In return, they earn "Aiur tokens," which can be spent on the use of research tools, including those which allow them to compare their papers with all other scientific research on the system (this today includes over 130 million open access studies and is expected to grow over time).

Aiur's €10 million ($11.7 million) token sale to 8,000 researchers who've worked on its machine learning, with a public token sale due to open later this month—this has a lower cap of €6 million ($7 million) and upper cap of €50 million ($59 million)

---

https://projectaiur.com/ We envision a world where the right scientific knowledge is available at our fingertips. Where all research is validated and reproducible. Where interdisciplinary connections are the norm. Where unbiased scientific information flows freely. Where research already paid for with our tax money is freely accessible to all.

Make-Your-Own-Blockchain

https://medium.com/@lhartikk/a-blockchain-in-200-lines-of-code-963cc1cc0e54

Activity

Adoption

Crypto and bitcoin adoption—How far along are we really in this rally?
https://medium.com/@dennyk/crypto-and-bitcoin-adoption-how-far-along-are-we-really-in-this-rally-79b5539dc222

Image: https://cdn-images-1.medium.com/max/800/1*0RCanopus is intended to be used as a part of a permissioned blockchain, such as Hyperledger Fabric or Parity Substrate's Ethereum PoA.Tsw7hH0rFOHq5kDXbgkUw.png

--

Bitnodes
https://bitnodes.earn.com/dashboard/?days=730#blocks-propagation
Bitnodes is currently being developed to estimate the size of the Bitcoin network by finding all the reachable nodes in the network.

From: https://media.consensys.net/the-state-of-the-ethereum-network-949332cb6895

Ethereum transaction chart: https://cdn-images-1.medium.com/max/2000/0*lGD8nGojqeEgLgdy

The Ethereum Enterprise Alliance (EEA) formed in March 2017 with 30 founding members committed to the integration of blockchain technology with enterprise establishments. Now, just over one year later, the EEA has grown to over 500 members.

- Brazil announced its intention to move petitions and popular voting onto Ethereum.
- Canada is testing out using Ethereum to provide transparency to the use of government grants to ease citizens' concerns of misappropriation and corruption.
- The city of Zug, Switzerland—a long-time crypto bastion—began offering digital IDs registered on Ethereum in 2017.
- Chile uses Ethereum to track the data and finances from the energy grid, hoping to combat corruption and exploitation through transparent, immutable data available for every citizen to see.
- Dubai is on the move to become an entirely integrated, blockchain-powered city by 2020.
- Estonia became the poster child of the distributed ecosystem and matured into a "digital republic" by moving many of its national systems onto the Ethereum blockchain.

Russian farmers are ditching the ruble for a new cryptocurrency -- the kolion - http://money.cnn.com/2018/06/04/technology/russia-cryptocurrency-farmer-kolion/index.html

Christine Lagarde compares the emergence of crypto-assets to that of the telephone. http://www.imf.org/external/pubs/ft/fandd/2018/06/how-policymakers-should-regulate-cryptoassets-and-fintech/straight.htm

Blockchain Patents are Soaring in 2018 as Adoption Accelerates

Forbes came up with a mega-list of the top 50 public companies who are exploring how to implement blockchain in their business model. Most of the companies on the list are worth several $Bn. dollars. You can see the list here. For anyone that doubts that blockchain is (going) mainstream, this is a good list to show to them.

Investment

"For the last few years, blockchain and Bitcoin have been hailed as "the next big thing," and there have been plenty of predictions about a coming boom in funding for the sector. The Bitcoin news site CoinDesk has compiled a database of investments in Bitcoin- and blockchain-related startups, and from that (in mid 2015) it created a list of the ten most influential venture capital firms in the industry.

"Those who also have substantial investments in education technology include Union Square Ventures, Khosla Ventures, Lightspeed Venture Partners, and Andreessen Horowitz." - 2016 - https://hackeducation.com/2016/04/07/blockchain-education-guide

Most tellingly, large investments in blockchain are being made. Venture-capital funding for blockchain start-ups consistently grew and were up to $1 billion in 2017.3 The blockchain-specific investment model of initial coin offerings (ICOs), the sale of cryptocurrency tokens in a new venture, has skyrocketed to $5 billion. Leading technology players are also heavily investing in blockchain: IBM has more than 1,000 staff and $200 million invested in the blockchain-powered Internet of Things (IoT). https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value

Ecosystem

http://blockchaincanada.org/ecosystem/

Consortia

https://cointelegraph.com/news/vitalik-buterin-to-advise-new-ethereum-community-fund-sponsoring-eth-infrastructure

Several large Ethereum-based projects have come together to create the Ethereum Community Fund (EFC), a vehicle to connect and fund the growth of Ethereum (ETH) infrastructure, according to the EFC website.
The founding members of the EFC are OmiseGo, Cosmos, Golem, Maker, Global Brain Blockchain Labs, and Raiden.

The Enterprise Ethereum Alliance (EEA) launched in Feb. 2017 is the world's largest open-source Blockchain initiative.
It is currently partnered with more than 200 organizations, including big financial institutions like JPMorgan, Santander, and Mastercard, Intel. The non-profit's aim is to bring privacy, scalability, and security to developing Ether and the Ethereum Blockchain.

https://www.the74million.org/article/ripple-blockchain-based-payment-network-to-grant-50m-to-17-universities-for-blockchain-cryptocurrency-research-workforce-development/
the launch of the University Blockchain Research Initiative. Through UBRI, Ripple will donate more than $50 million to 17 initial university partners around the world to "support academic research, technical development, and innovation in blockchain, cryptocurrency, and digital payments," the company said in a statement.

Chamber of Digital Commerce - https://digitalchamber.org/

- Blockchain Intellectual Property Council (BIPC)

https://medium.com/coinmonks/enterprise-blockchain-are-we-there-yet-7090b3841b11

- R3 was started in 2015 as a consortium of the financial services industry to build the open source DLT solution Corda. It has since evolved into a software startup that offers DLT-related services to the by now 100+ consortium members such as Bank of America, Deutsche Bank, RBC, or UniCredit, its business model is still in development though.
- The Blockchain Insurance Industry Initiative (B3i) is a consortium of insurers and reinsurers to explore the potential of DLT. It was founded in 2016 and currently comprises 15 members such as Allianz, Generali, Munich Re, or Zürich IG.
- The Hashed Health Consortium was launched by the DLT advisory and development firm Hashed Health in 2016 to advance the use of blockchain protocols in healthcare. Little is known about high-profile members though, and there are efforts for a different vendor-agnostic consortium from within the industry.
- The Mobility Open Blockchain Initiative (Mobi) was launched in 2018 as a consortium of the automotive industry comprising manufacturers and suppliers such as BMW, Renault, GM, or Bosch to explore DLT use cases around mobility services.
- The Hyperledger project was started by the Linux Foundation in 2015 to build open source blockchain platforms and related tools such as its flagship solution, the permissioned blockchain Fabric. Its members include e.g. Accenture, American Express, IBM, and SAP.
- The Ethereum Enterprise Alliance (EEA) is a community of enterprises that are building applications on the Ethereum platform that was founded in 2017 and quickly grew to 150+ members such as Accenture, Microsoft, JPM, or UBS.

- Founded in 2017, the Trusted IoT Alliance is a cross-industry consortium that develops use cases that leverage blockchain infrastructure to secure and scale IoT ecosystems. Its enterprise members include e.g. Bosch, Cisco, and UBS.
- The Decentralized Identity Foundation is a community of companies working on DLT-based identity management solutions that formed a consortium to improve interoperability in 2017. It includes e.g. Hyperledger, Microsoft, IBM, and Accenture.
- There are several further groups that look at DLT from different angles, such as the Chamber of digital commerce, PTDL, Blockchain Collaborative Consortium, Global Blockchain Business Council, Legal Consortium, and more.

Partnership between consulting firm EY and technology giant Microsoft.
https://qz.com/1310300/microsoft-is-deploying-what-could-become-the-biggest-enterprise-blockchain/

- "the network, initially to be used for rights and royalties processing by Microsoft's game publishers, will eventually have a much wider purpose. It's meant for any industry in which assets or intellectual property are licensed and royalties accrue based on contracts."
- The project between EY and Microsoft uses Quorum's permissioned distributed ledger and Microsoft's Azure cloud infrastructure.

Consultants

Vanbex

https://vanbex.com/
"Since 2013, Vanbex has been empowering bold ideas on the blockchain with deep industry experience and comprehensive consulting."

MLG Blockchain

https://mlgblockchain.com/
`We are blockchain agnostic and are experienced working with many blockchain fabrics including the Bitcoin Blockchain, Ethereum, Hyperledger, Ripple, Factom, Eris.

International

World diagram - regulations -
https://cdn-images-1.medium.com/max/800/0*gJkEf8nTVYg8mnj3.png from
https://medium.com/bloomberg/what-the-worlds-governments-are-saying-about-cryptocurrencies-9022db95c2d2

Africa

Diagram - https://cdn-images-1.medium.com/max/800/0*30SfwLP45fIUeOPf.png

South Africa

https://medium.com/bloomberg/what-the-worlds-governments-are-saying-about-cryptocurrencies-9022db95c2d2
South Africa's markets regulator doesn't oversee virtual currencies or digital-asset exchanges, though the central bank has said it will investigate an "appropriate policy framework and regulatory regime."

Kenya

https://medium.com/bloomberg/what-the-worlds-governments-are-saying-about-cryptocurrencies-9022db95c2d2
It's a similar story in Kenya, one of Africa's most tech-savvy nations. There, Bitcoin and other cryptocurrencies have grown in popularity even as officials have warned against trading them.

Nigeria

https://medium.com/bloomberg/what-the-worlds-governments-are-saying-about-cryptocurrencies-9022db95c2d2
In Nigeria, cryptocurrency markets aren't regulated, but the central bank, which likens Bitcoin trading to gambling, has said that will probably change.

Zimbabwe

https://medium.com/bloomberg/what-the-worlds-governments-are-saying-about-cryptocurrencies-9022db95c2d2
In Zimbabwe, where digital currencies are traded on exchanges and used for remittance payments, the monetary authority has warned about the risk of "money laundering, terrorism financing, tax evasion and fraud."

Argentina

In Argentina, Investors Flock to Safe-Haven Bitcoin
https://bitcoinist.com/in-argentina-investors-flock-to-safe-haven-bitcoin/
"The economic crisis in Argentina is driving investors to buy Bitcoin in order to protect their wealth, pushing the cryptocurrency's price higher in-turn. In parallel, to satisfy the increasing demand, the first of 12 Bitcoin ATMs has already begun to operate in a Buenos Aires mall. The number of stores accepting Bitcoin also continues to rise."

Asia

Diagrams -
https://medium.com/bloomberg/what-the-worlds-governments-are-saying-about-cryptocurrencies-9022db95c2d2

- https://cdn-images-1.medium.com/max/800/0*UKpN04Fekr05hO2m.png

- https://cdn-images-1.medium.com/max/800/0*Kz6hvqSfAHu5z3qz.png

Dubai

Dubai launches blockchain based payment system
http://egov.eletsonline.com/2018/09/dubai-launches-blockchain-based-payment-system/
Smart Dubai Office (SDO), in collaboration with Dubai Department of Finance has launched the 'Payment Reconciliation and Settlement' System based on blockchain technology.

Iran

Iran Plans National Cryptocurrency as New US Sanctions Loom
https://www.coindesk.com/iran-plans-national-cryptocurrency-as-new-us-sanctions-loom/

Iran's Crypto-Rial May Hit Banks Within 'Coming Days'
https://www.financemagnates.com/cryptocurrency/news/irans-crypto-rial-may-hit-banks-within-coming-days/

Japan

Japanese Financial Services Agency to Tighten Regulations on Crypto Investing
https://www.financemagnates.com/cryptocurrency/news/japanese-financial-services-agency-to-tighten-regulations-on-crypto-investing/

Japan's Bitcoin Law Goes Into Effect Tomorrow
https://www.coindesk.com/japan-bitcoin-law-effect-tomorrow/
"The country's legislature passed a law, following months of debate, that brought bitcoin exchanges under anti-money laundering/know-your-customer rules, while also categorizing bitcoin as a kind of prepaid payment instrument."

Korea

South Korean Telecoms Giant KT Has Built Its Own Blockchain
https://www.coindesk.com/south-korean-telecoms-giant-kt-has-built-its-own-blockchain/

https://medium.com/bloomberg/what-the-worlds-governments-are-saying-about-cryptocurrencies-9022db95c2d2 "South Korea, which became a hotbed of cryptocurrency activity last year, is also tightening oversight as it works on a comprehensive set of regulations, though it has allowed exchanges to keep operating for now."

South Korean Province to Issue its Own Local Cryptocurrency
https://www.financemagnates.com/cryptocurrency/news/south-korean-province-to-issue-its-own-local-cryptocurrency/ "The cryptocurrency will replace locally-issued giftcards."

Thailand

Thailand braces for surge of blockchain-enabled solar power

https://asia.nikkei.com/Business/Business-Trends/Thailand-braces-for-surge-of-blockchain-enabled-solar-power
“A growing number of listed companies are using blockchain to help homeowners profit from their own rooftop solar systems, in effect cutting EGAT and other agents out of the market.”

Thailand’s Blockchain Solar Power Producers Face Extra Fees to Offset State Utility Losses
https://www.ccn.com/thailands-blockchain-solar-power-producers-face-extra-fees-to-offset-state-utility-losses/

Australia-NZ

IBM Wins AUD $1 Billion Contract to Develop Blockchain, Tech Initiatives for Australia Govt.
https://www.ccn.com/ibm-wins-aud-1-billion-contract-to-develop-blockchain-tech-initiatives-for-australia-govt/ “The five-year, AUD $1 billion (~USD $740 million) contract is Australia’s latest attempt to make good on its goal to become one of the world’s “top-three digital governments” by 2025”

It only took Oz govt transformation bods 6 months and $700k to report that blockchain ain't worth the effort
https://www.theregister.co.uk/2018/10/24/oz_spent_700k_to_decide_that_blockchain_isnt_worth_the_hype/ "without standardisation, there is the challenge of blockchain becoming a little fragmented", and genuine opportunities to use the technology will have to wait until useful standards are in place.

Fake news site uses John Key image to endorse Bitcoin
https://www.stuff.co.nz/business/money/109748590/fake-news-site-uses-john-key-image-to-endorse-bitcoin A fake advertisement promoting crypto-currency has ripped off the image of former Prime Minister John Key.

Brazil

https://medium.com/bloomberg/what-the-worlds-governments-are-saying-about-cryptocurrencies-9022db95c2d2
“Brazil’s market regulator, meanwhile, has barred funds from investing in cryptocurrencies because they aren’t classified as financial assets.”

Canada

https://medium.com/bloomberg/what-the-worlds-governments-are-saying-about-cryptocurrencies-9022db95c2d2
In Canada, regulators have said that ICOs may be treated as securities and that products linked to cryptocurrencies should be considered high-risk. At the same time, the country’s stock exchanges have become popular destinations for crypto-related stocks and exchange-traded funds.

China

China and Blockchain Technology: An Introduction
https://media.consensys.net/china-and-blockchain-technology-an-introduction-9e12adf9fd52

- In 2013, China-based BTC Relay became the largest-volume bitcoin exchange on earth.

China Welcomes Synereo to Deliver Blockchain Tech to the Region
https://medium.com/synereo/china-welcomes-synereo-to-deliver-blockchain-tech-to-the-region-72c497d4ad8d "partnership with Qiyi Culture, one of China's top online professionally generated content production companies. In the coming months, the Shanghai-based company will introduce WildSpark to give China's online content creators new and innovative means to monetize their creations through our AMP token."

Synereo Aims to Put AMPs in the Hands of Every Internet User
https://medium.com/synereo/synereo-aims-to-put-amps-in-the-hands-of-every-internet-user-4565c405895d
Synereo's partnership with Shanghai-based production company, Qiyi Culture Communication Ltd. that was announced earlier this month. With 20 Content IPs per annum, and nine Original Content IPs, Qiyi Culture produces some of China's top Professionally Generated Content (PGC) such as "Sister Deformation," a talk show that has surpassed 10 million viewers per week, and many more.

Navigating Crypto Regulation: China
https://hackernoon.com/navigating-crypto-regulation-china-fbae88697a21

- "At the nation's peak, China accounted for three quarters of the world's bitcoin mining operations and over 95% of the bitcoin trading volume."
- Article contains a History of Crypto Regulation in China
- hy is China the world leader in crypto mining?
    - Cheap Electricity—electricity is far cheaper in China than in most other countries.
    - Leading Bitcoin Mining Pools
    - Top ASIC Hardware Manufacturers—top hardware manufacturers such as Bitmain (recently valued at $12 Billion) are based in China

https://medium.com/bloomberg/what-the-worlds-governments-are-saying-about-cryptocurrencies-9022db95c2d2 "China, once a global hub for cryptocurrency trading, now leads the world in cracking down. It has outlawed digital-asset exchanges and ICOs, blocked online access to overseas trading platforms and cut off power to Bitcoin miners."

China Central Bank Warns of Cryptocurrency, ICO Risks in Public Notice
https://www.ccn.com/china-central-bank-warns-of-cryptocurrency-ico-risks/
"The Shanghai branch of the PBoC issued a public notice on Tuesday to "remind" consumers and investors to increase their risk awareness of ICOs … It's been a year since the PBoC issued a blanket ban on all ICOs, outlawing it as an illegal practice of fundraising."

Europe

22 Countries Sign Declaration For European Blockchain Partnership

- The European Commission's (EC) Digital Day 2018 has led to the signing of a Declaration to create a European Blockchain Partnership made of up 22 countries, according to an April 10 European Commission press release. https://cointelegraph.com/news/22-countries-sign-declaration-for-european-blockchain-partnership
- European Blockchain Partnership and the EU Blockchain Observatory https://www.idgconnect.com/blog-abstract/30732/european-blockchain-institutions-welcome-input-it-professionals

EU members cannot have their own cryptocurrency - https://www.reuters.com/article/us-ecb-bitcoin-estonia/ecbs-draghi-rejects-estonias-virtual-currency-idea-idUSKCN1BI2BI

Estonia

Estonia cryptocuirrency?
The idea floated:
https://medium.com/e-residency-blog/estonia-could-offer-estcoins-to-e-residents-a3a5a5d3c894

France

https://medium.com/bloomberg/what-the-worlds-governments-are-saying-about-cryptocurrencies-9022db95c2d2
French authorities have said that online platforms for crypto-derivatives should face tough reporting and business conduct standards.

Germany

https://medium.com/bloomberg/what-the-worlds-governments-are-saying-about-cryptocurrencies-9022db95c2d2
Germany has cracked down on trading venues that lack permission to offer brokerage services

Gibraltar

Gibraltar's Official Cryptocurrency Exchange is Open to the Public
https://www.financemagnates.com/cryptocurrency/news/gibraltars-official-cryptocurrency-exchange-is-open-to-the-public/

Ireland

Anti-money laundering laws introduced to help gardai target crooks using cryptocurrency to hide criminal cash
https://www.irishmirror.ie/news/irish-news/crime/anti-money-laundering-laws-introduced-13809037
New sweeping anti-money laundering laws will help gardai target crooks using cryptocurrency to hide their criminal cash.

Malta

Binance Moves To Malta In Hopes Of Collaborating With Regulators
https://medium.com/the-crypto-times/cat-mouse-binance-moves-to-malta-in-hopes-of-collaborating-with-regulators-4de0442688b2 "Since Binance hopes to add fiat-to-cryptocurrency trading pairs soon, the move rests in part upon negotiations with Maltese banks, which are required as partners to open up fiat deposits and withdrawals."

The Daily: Malta Sees No Issue With Unlicensed Crypto Firms, Valletta Mansion on Sale for Crypto
https://news.bitcoin.com/the-daily-malta-sees-no-issue-with-unlicensed-crypto-firms-valletta-mansion-on-sale-for-crypto/

Russia

https://medium.com/bloomberg/what-the-worlds-governments-are-saying-about-cryptocurrencies-9022db95c2d2
Russia's finance ministry unveiled draft legislation in January that would ban cryptocurrency payments while allowing ICOs and the exchange of virtual currencies into the traditional sort. To make the rules permanent, the ministry may have to overcome opposition from the nation's central bank.

- an adviser to Vladimir Putin publicly stated that a Crypto-Ruble could be created and used to evade sanctions - https://www.financemagnates.com/cryptocurrency/news/cryptocurrencynewsaxis-corruption-countries-using-crypto-evade-international-sanctions/

Switzerland

Swiss City Plans Blockchain Voting Pilot Using Ethereum-Based IDs
https://www.coindesk.com/swiss-city-plans-to-vote-on-blockchain-using-ethereum-digital-id/
a Swiss city looking at using Ethereum based Uport for digital identity and voting.

Swiss Tax Haven Town of Zug will Implement Voting on the Blockchain with Ethereum

Top 6 Swiss Blockchain Startups with Potential
https://nulltx.com/top-6-swiss-blockchain-startups-with-potential/

- Alethena - ICO and blockchain-asset rating agency

- Dfinity - cloud computing and building the cloud 3.0 through decentralized technologies.
- MindFire - manage research events, collect intellectual property, and storage
- Proxeus - aid in asset tokenization, as well as building new dApps
- SwissBorg - regulated wealth management platform
- Tend - letting users buy and sell fractional ownership of luxury assets and offer experiences connected to these assets

UK

https://medium.com/bloomberg/what-the-worlds-governments-are-saying-about-cryptocurrencies-9022db95c2d2
In the U.K., a parliamentary committee is looking at how to police digital currencies.

Coinbase Becomes Electronic Money Institution Under U.K.'s FCA Regulations & Adds Support For Faster Payments
https://medium.com/the-crypto-times/coinbase-becomes-electronic-money-institution-under-u-k-s-107838c2135f

Can Brexit Save Blockchain? Reactions From The Industry
https://www.forbes.com/sites/ginaclarke/2018/11/16/can-brexit-save-blockchain-reactions-from-the-industry/

India

Cryptocurrency Virtually Outlawed in India as Top Court Backs Ban
https://www.bloomberg.com/news/articles/2018-07-03/india-s-banking-ban-on-cryptocurrency-survives-court-challenge

India's cryptocurrency exchanges face another 50 days of uncertainty
https://qz.com/1333763/indian-supreme-court-to-rule-on-cryptocurrency-case-on-sept-11/

- On July 20, after a short hearing, India's supreme court set Sept. 11 as the date for the final hearing.

https://medium.com/bloomberg/what-the-worlds-governments-are-saying-about-cryptocurrencies-9022db95c2d2 "India, where crypto-mania has been relatively subdued, the government has said it doesn't consider digital currencies to be legal tender and will take measures to curb their use."

India's top court strikes down ban on cryptocurrency trading
https://www.cnn.com/2020/03/04/tech/cryptocurrency-india-ban-struck-down/index.html
The Supreme Court of India on Wednesday overturned a 2018 ruling by the Reserve Bank of India (RBI), which prohibited Indian banks from dealing with cryptocurrency exchanges over "concerns of consumer protection, market integrity and money laundering, among others."

USA

Camp C-Block Introduces Blockchain Technology to Black Girls

http://www.gettingsmart.com/2018/07/camp-c-block-introduces-blockchain-technology-to-black-girls/

Delaware

Delaware Awards IBM $738,000 Contract to Develop Prototype Blockchain Filing System https://www.ccn.com/delaware-awards-ibm-738000-contract-to-develop-prototype-blockchain-filing-system/ “Delaware’s blockchain project has faced some challenges. Earlier this year, the state paid IBM $49,000 for consulting on a project involving a blockchain startup called Symbiont that eventually fell apart. Symbiont CEO Mark Smith said state officials played politics by raising concerns that the blockchain filing system could impede the activities of corporate attorneys and registered agents. He said the system, built for the state archives, never launched.”

Illinois

Urban Array, a social entrepreneurial enterprise in Chicago that utilizes blockchain in community development. - https://urbanarray.org/

New York

BitLicense, New York state’s licensing regime for cryptocurrency businesses - https://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm

- has been “an absolute failure,” said Erik Voorhees, CEO of the popular cryptocurrency exchange ShapeShift at 2018 Consensus conference in New York City - http://fortune.com/2018/05/25/bitcoin-cryptocurrency-new-york-bitlicense/
- https://www.coindesk.com/bitlicense-refugees-kraken-shapeshift-ceos-talk-escape-new-york/ - Bitlicense Refugees panel - video
- Voorhees and others on a panel of “BitLicense refugees” who had decided to take their companies out of the state lamented the fact that only four companies had secured licenses in the three years since the policy was adopted. Less than a month later, though, the number is up to seven, and payment app Square is the latest to receive the state’s blessing.”
- Square and Xapo receive licenses - “Perhaps it was premature to declare the regulations a failure?”

https://campustechnology.com/articles/2018/07/23/columbia-u-opens-research-center-devoted-to-blockchain-tech.aspx
https://people.uis.edu/rschr1/onlinelearning/?p=45759

New York’s Damning Report on Crypto Exchanges Will Be Good for the Industry
https://medium.com/mit-technology-review/new-yorks-damning-report-on-crypto-exchanges-will-be-good-for-the-industry-452d82569671
“The new report hammers exchanges for lacking “robust real-time and historical market surveillance capabilities, like those found in traditional trading venues, to identify suspicious trading patterns.””

New York creates cryptocurrency task force

https://www.verdict.co.uk/electronic-payments-international/news/new-york-creates-cryptocurrency-task-force/ The team will assess various aspects of the crypto space such as energy cost of mining cryptocurrencies as well as their effect on the tax system.

Oklahoma

Oklahoma is ready for Blockchain for Business
https://www.ibm.com/blogs/blockchain/2019/09/oklahoma-is-ready-for-blockchain-for-business/
September 17, 2019, in the heart of the Oklahoma City Innovation District, OG&E and IBM are presenting the first Blockchain for Business in Oklahoma conference.

Puerto Rico

The perfect storm: building a crypto-utopia in Puerto Rico – video
https://www.theguardian.com/changingmediasummit/video/2018/aug/09/the-perfect-storm-building-a-crypto-utopia-in-puerto-rico-video
Crypto developers and investors are moving to Puerto Rico , attracted by lucrative tax regimes They plan to regenerate the island using blockchain technology.

West Virginia

West Virginia to introduce mobile phone voting for midterm elections
https://money.cnn.com/2018/08/06/technology/mobile-voting-west-virginia-voatz/index.html
“Ballots are anonymized, the company says, and recorded on a public digital ledger called blockchain. Although that technology is most often associated with Bitcoin and other cryptocurrencies, it can be used to record all manner of data.”

Venezuela

http://www.europarl.europa.eu/cmsdata/149900/CASE_FINAL%20publication.pdf
Venezuela was the first country in the world that issued a sovereign virtual currency

Venezuela's New National Currency Will Be Tied to the Petro, Says President
https://www.coindesk.com/venezuelas-new-national-currency-will-be-tied-to-petro-says-president/

To Evade U.S. Sanctions, Venezuela Launches the World’s First National Cryptocurrency
http://www.defenddemocracy.org/media-hit/yaya-j-fanusie-to-evade-us-sanctions-venezuela-launches-the-worlds-first-national-crypto/
—the “petro”, which was widely interpreted as an attempt to circumvent the economic sanctions imposed by the US (Fanusie and Frai, 2018). In response to the plans of the Venezuelan government to issue the petro, the President of the United States, Donald J. Trump, issued an executive order banning any transactions related to any VC issued by or on the behalf of Venezuelan government.
https://www.whitehouse.gov/briefings-statements/presidential-message-congress-united-states-2/

Why Third Generation Cryptocurrencies Are Game-Changers for Venezuela
https://hackernoon.com/why-third-generation-cryptocurrencies-are-game-changers-for-venezuela-cb8c9b016f9d "a new project named "Adopt a Family" kicked off. The goal of the project is to help families from Venezuela with NANO donations. You can find more information about the project in its official thread."

In Venezuela, Cryptocurrency Is an Oppressor and a Lifeline
https://www.pcmag.com/feature/362486/in-venezuela-cryptocurrency-is-an-oppressor-and-a-lifeline
"Venezuela embodies the best and worst potential of blockchain technology. While the Maduro regime uses the Petro coin to fund authoritarian oppression and combat hyperinflation, crypto solutions give people a potential path to economic freedom."

Special Report: In Venezuela, new cryptocurrency is nowhere to be found
https://www.reuters.com/article/us-cryptocurrency-venezuela-specialrepor/special-report-in-venezuela-new-cryptocurrency-is-nowhere-to-be-found-idUSKCN1LF15U

Courses

https://nulltx.com/free-ethereum-developer-elearning-course-giveaway/
NullTX is offering our readers free access to premium blockchain elearning courses from Devslopes. Devslopes is a top online elearning instructor with over 300,000 students. The first course we are giving away is the Certified Ethereum Blockchain Developer.

Issues

Overviews

https://hackeducation.com/2016/04/07/blockchain-education-guide
"Gideon Greenspan, the CEO of a blockchain platform Coin Sciences, offered a list of eight conditions that should be met in order to avoid "pointless blockchain projects." These include needing a database, having multiple people writing to that database, having some interactions between transactions, operating with an absence of trust, and not needing a trusted intermediary. Riffing on that article, BadgeChain team member Doug Belshaw recently wrote a follow-up about "Avoiding pointless (Open Badges-related) blockchain projects," in which he used Greenspan's list to argue that, indeed, Open Badges meets all the Coin Sciences' requirements to move forward with the blockchain."

Investment Theses - good overview of issues -
https://medium.com/@pierre_rochard/bitcoin-investment-theses-part-1-e97670b5389b

Conceptual Issues

Locus of value

https://twitter.com/ricburton/status/987706443896967169

- Fat Protocol Thesis: Dapps capture minimal value. Invest in protocols.
- Fat Dapp Thesis: Great dapps capture people's attention. Invest in dapps.
- Fat Wallet Thesis: Great wallets hold keys to dapps and protocols. Invest in wallets.

Which thesis would you pick?

Fat Protocols vs Fat Dapps vs Fat Wallets
https://medium.com/lightspeed-venture-partners/fat-protocols-vs-fat-dapps-vs-fat-wallets-4d33ead29130
He frames the question by breaking value creation in the crypto ecosystem into three layers:
1) Base protocols (like ethereum)
2) Decentralized applications (like CryptoKitties)
3) Companies building products (like wallets)

Economic Incentives

University of Chicago's Eric Budish. In a new paper (PDF) Budish concludes, based on a model of Bitcoin's incentive system, that there are "intrinsic economic limits to how economically important it can become.":
https://faculty.chicagobooth.edu/eric.budish/research/Economic-Limits-Bitcoin-Blockchain.pdf
"Bitcoin's must simultaneously satisfy two conditions in equilibrium: (1) a zero-profit condition among miners, who engage in a rent-seeking competition for the prize associated with adding the next block to the chain; and (2) an incentive compatibility condition on the system's vulnerability to a "majority attack", namely that the computational costs of such an attack must exceed the benefits. Together, these two equations imply that (3) the recurring, "flow", payments to miners for running the blockchain must be large relative to the one-off, "stock", benefits of attacking it. This is very expensive!"

- the new paper has gotten a fair amount of praise from other economists, some cryptocurrency enthusiasts have been dismissive.

Nothing-at-Stake Problem

https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb

- The main issue with PoS is the so-called nothing-at-stake problem. Essentially, in the case of a fork, stakers are not disincentivized from staking in both chains, and the danger of double spending problems increase. More on that here.
- In order to avoid that, hybrids consensus algorithms appeared, such as the PoW-PoS combination used by Decred. Active research towards a secure and decentralized Proof of Stake protocol is being done by the Ethereum Foundation with Casper The Friendly Ghost and Casper The Friendly Finality Gadget.

Immutability

Good discussion of this here:
https://www.bankofcanada.ca/wp-content/uploads/2018/03/san2018-5.pdf

"Bitcoin's virtual immutability comes not only from encryption but also from the incentives embedded in the system. What makes the ledger immutable is the fact that adding a block to the blockchain is costly. A network participant (say, a Bitcoin miner) needs to expend significant resources to win the tournament (to be the quickest to find a solution to a puzzle), which awards that participant the right to add a new block of transactions to the blockchain. This cost also makes rewriting the history of the blockchain expensive, resulting in virtual immutability."

"blockchain applied outside of Bitcoin (or other native cryptocurrency) loses its desired properties. It is no longer permissionless and immutable without the need for trusted third parties."

"outside of Bitcoin (or other cryptocurrencies) we do not have a technology that offers 'permissionless distributed ledgers that cryptographically assure immutability without a need for trusted third parties.'"

Centralization

- A few powerful players having a concentration of mining power
    - Bitmain's two mining pools account for approximately 40 percent of the total computing power on the Bitcoin network.
    - https://motherboard.vice.com/en_us/article/3kj5dw/what-is-an-asic-miner-bitmain-monero-ethereum

    - What Happens When a Chinese Giant Swoops In on Your Tiny Cryptocurrency
    - Bitmain maintains a near-monopoly on Bitcoin hardware, now it's coming for Siacoin.
    - in the world of ASIC cryptocurrency mining, a Chinese hardware company called Bitmain is king. Not only is Bitmain a chief supplier of ASICs, but it also

operates two of the world's largest Bitcoin mining operations that together account for 39 percent of the entire network's mining power.
- https://motherboard.vice.com/en_us/article/ev59dz/bitmain-siacoin-obelisk-asic-vorick

- https://www.coindesk.com/bitcoin-code-defend-against-asic-mining-threat/
- Crypto Needs More Than Code to Beat the ASIC Mining Threat
- Vertcoin: the vertcoin community has also informally agreed upon a kind of pact to fork the code if and when a vertcoin ASIC appears.

http://donaldclarkplanb.blogspot.com/2018/06/blockchain-got-married-on-it-but-fell.html
Sure Blockchain was created to democratise, decentralise and disintermediate institutions, so why keep it locked up within institutions? Much of the interest I now see is from traditional purveyors trying to lock down the technology for their own ends. A private Blockchain isn't really a decentralised Blockchain, in that it is 100% owned. It's basically a transaction ledger for interested parties, not the democratising, decentralising, deintermediating force many imagined.

Why the Blockchain Promises a Safer Future and how big Business Will try to Kill it
https://medium.com/@ChrisHerd/why-the-blockchain-promises-a-safer-future-and-how-big-business-will-try-to-kill-it-f7d4d630fa95 "Big business are trying to craft the blockchain in their own image, diluting its potential for good by trying to implement private blockchains which they own. Instead of allowing it to remain a private utility which ensures trust between strangers they are redeploying the technology under their own banner."

Here Are the World's Virtual Currency Billionaires (or at Least They Were)
https://medium.com/the-new-york-times/here-are-the-worlds-virtual-currency-billionaires-or-at-least-they-were-8953c7bbfd59
Meet The Crypto Billionaires Getting Rich From Ripple's XRP
https://medium.com/forbes/meet-the-crypto-billionaires-getting-rich-from-ripples-xrp-b5fce50c84c1
"XRP, being issued by a company, is less decentralized than many other cryptocurrencies. For instance, Ripple itself holds 61.3 billion XRP, including 55 billion that it keeps in escrow. Only 38.7 billion XRP tokens have been distributed."

Decentralization

Is Crypto's Decentralization a Bug, Not Just a Feature?
https://medium.com/forbes/is-cryptos-decentralization-a-bug-not-just-a-feature-691398d623f7

Sybil Attacks

Sybil and Satoshi
https://medium.com/cyber-capital/sybil-and-satoshi-fbc58ee13924

In 2012 Microsoft mathematicians wrote a paper called "On Bitcoin and Red Balloons". In this paper they proved that any network architecture that requires 3 or more hops can be Sybil attacked.
Sybil Attack: An attack by which an attacker is able to overpower a network that is dependent on identities.

In a cryptocurrency network this is either done via double spends or manipulating the coin generation mechanism, both of which are dependent on identities.

a simple set of guidelines stipulating that incentives of any Sybil resistant network must have the following features:

- An incentive to propagate information.
- No incentive for duplication of identities.
- The reason that bitcoin is Sybil resistant is because the identities are tied to the proof of work mechanism which cannot be faked.

Exploiting Trust and Distrust Information to Combat Sybil Attack in Online Social Networks
https://pdfs.semanticscholar.org/30e4/1ec151d1499b580155be4dee168530d80145.pdf
"Due to open and anonymous nature, online social networks
are particularly vulnerable to the Sybil attack, in which a malicious user
can fabricate many dummy identities to attack the systems"

Anonymity

Bitcoin Thieves Threaten Real Violence for Virtual Currencies
https://medium.com/the-new-york-times/bitcoin-thieves-threaten-real-violence-for-virtual-currencies-93a4a29a67c1 "Virtual currencies can be easily transferred to an anonymous address set up by a criminal. While banks can stop or reverse large electronic transactions made under duress, there is no bitcoin bank to halt or take back a transfer, making the chances of a successful armed holdup frighteningly enticing."

Technical Issues

Technology Standards

- Diagram p.8
  http://www.ey.com/Publication/vwLUAssets/Blockchain_in_wealth_and_asset_management/$FILE/ey-blockchain-innovation-wealth-asset-management.pdf

Software Reliability

Bitcoin and Software Reliability
https://hackernoon.com/bitcoin-and-software-reliability-d681367a49b2

Centralization

Bitcoin's Biggest Rival Faces Overhaul as Computing Power Rises
https://medium.com/bloomberg/bitcoins-biggest-rival-faces-overhaul-as-computing-power-rises-3b9e2a4fdf4f
"The range of participants could be about to shrink, as Bitmain and others move in with a new type of computing hardware that could give them disproportionate power when it comes to confirming transactions. The new hardware, which should become available in July or sooner, could push out smaller miners and is "a nightmare for decentralization," said Lucas Nuzzi, a senior analyst at Digital Asset Research.
"Ethereum developers are rushing to stop the invasion. During a call last month, Ethereum co-founder Vitalik Buterin said that the risk will go away once the community deploys Casper—software that will get rid of miners altogether and confirm transactions in a different way, which would expand the number of people involved in the process. But the date of Casper's deployment is uncertain, with the project having already been delayed for months."

Cost

Energy Consumption

"While cryptocurrency might be virtual, all this mining and computational puzzle-solving obviously takes an enormous amount of energy. According to one Motherboard estimate, "each Bitcoin transaction uses roughly enough electricity to power 1.57 American households for a day." Bitcoin currently handles about 360,000 transactions per day. You do the math."
https://hackeducation.com/2016/04/07/blockchain-education-guide

Why I hate Bitcoin. 1 BC transaction can power 30 households for a day. As of now, Bitcoin uses an amount of energy that could power over 6,000,000 homes. It currently consumes the equivalent of 10% of Canada's total energy consumption. 1 BC transaction costs more than 100,000 Visa transactions. As the chain grows, so will the cost per transaction. It is simply unsustainable as is. And, "Bitcoin's biggest problem is not even its massive energy consumption, but that the network is mostly fueled by coal-fired power plants in China. Coal-based electricity is available at very low rates in this country. Even with a conservative emission factor, this results in an extreme carbon footprint for each unique Bitcoin transaction".
https://digiconomist.net/bitcoin-energy-consumption

https://www.coinwarz.com/calculators/bitcoin-mining-calculator

Some interesting links.

1. https://www.quora.com/What-is-the-major-limitation-of-blockchain-technology
2. https://www.coindesk.com/information/blockchains-issues-limitations/
3. https://www.kaspersky.com/blog/bitcoin-blockchain-issues/18019/

4. https://hbr.org/2017/01/the-truth-about-blockchain

https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb
"Proof of Work provides the needed security and has been proven to work pretty well so far. However, it is very energy consuming:" Diagram:
https://cdn-images-1.medium.com/max/1000/0*Axh0tQoXkXeJTiB_.png

https://www.bloomberg.com/news/articles/2018-06-19/quebec-hikes-power-prices-for-crypto-miners-to-halt-new-requests
Quebec will raise electricity prices for crypto-miners while it tries to figure out how to deal with exploding energy demands from the industry. (Bloomberg)

http://www.europarl.europa.eu/cmsdata/149900/CASE_FINAL%20publication.pdf
According to Digiconomist, on 7 May 2018 Bitcoin's estimated annual electricity consumption was 65.26 TWh, which is the same as that of the Czech Republic —an entire country with a population of over 10.5 million people.
https://digiconomist.net/bitcoin-energy-consumption

Cryptocurrency Miners Are Building Their Own Electricity Infrastructure
https://motherboard.vice.com/en_us/article/9kmnba/cryptocurrency-miners-canada-building-their-own-electricity-infrastructure-dmg "Canadian company DMG Blockchain is expanding its mining operation in British Columbia with its own electrical substation."

The fightback against the bitcoin energy guzzlers has begun
https://www.wired.co.uk/article/bitcoin-mining-energy-consumption-new-york
"The resident hobbyists are no problem," says Plattsburgh mayor Colin Read. "But when out of towners noticed cheap rates just as bitcoin prices began to spike they flocked here. Currently 15 per cent of our power supply is used by the large bitcoin operations – which pushes us over the city's quota on cold winter days – meaning we have to buy power on the open market to meet demand, increasing costs by 30 to 50 per cent."

What is Holding Back The Blockchain?
https://medium.com/@abhishekkothari/what-worlds-may-come-8f00e631ca31
"The Proof of Work (PoW) algorithm that the existing Blockchains including Bitcoin and Ethereum employ to validate transactions is extremely inefficient. Think of the inefficiency as the price to pay for decentralizing trust. As I described above, imagine the massive carbon footprint and electricity consumption required to maintain decentralization of trust."

Blockchain firm Soluna to build 900MW wind farm in Morocco: CEO
https://www.reuters.com/article/us-cryptocurrency-morocco-soluna-energy/blockchain-firm-soluna-to-build-900mw-wind-farm-in-morocco-ceo-idUSKBN1KU2BA?feedType=RSS&feedName=technologyNews

While Toronto Gears Up to Become A Smart City, Quebec is Being Killed By Bitcoin

https://medium.com/@trentonpaultramel/while-toronto-gears-up-to-become-a-smart-city-quebec-is-being-killed-by-bitcoin-4eda74e35700
“Quebec could become the new global hub of cryptocurrency mining. However, if it gave them access to its power supply, the entire process could be too much for Hydro-Québec to handle and it could crush under pressure.”

Employees connect nuclear plant to the internet so they can mine cryptocurrency - https://www.zdnet.com/article/employees-connect-nuclear-plant-to-the-internet-so-they-can-mine-cryptocurrency/

Fees

https://er.educause.edu/articles/2018/5/will-blockchains-revolutionize-education
“As processing costs have grown, miners have begun prioritizing transactions that pay a higher fee. User costs thus will continue to rise as long as processing power remains scarce relative to demand.”
“Other blockchains may be no more economical; as of late 2017, storing a small (1 KB) contract on Ethereum could cost almost $100.[8] “

Here is an article explaining the purpose of this thing:
https://www.blockstream.com/2018/03/25/paypercall-shows-the-full-power-of-lightning-charge.html

Paypercall fulfills the long-held promise of a next-generation web of micropayments, where web developers can request payments for specific, programmatic API actions. Want to require a micropayment when a user sends an SMS? Want to offer image processing services for a microfee? Paypercall allows developers to do so, and with Lightning’s instant payments, it enables instantaneous access to an API’s functionality.

On Jun 24, 2018, at 2:36 PM, Andriy Drozdyuk <andriy@drozdyuk.com> wrote:
Some libraries I found that allow to charge for HTTP calls in Lightning/Bitcoin.

This one is a general payment library:
https://github.com/ElementsProject/lightning-charge

This one is specific to charging per HTTP call (it uses lightning-charge underneath):
https://github.com/ElementsProject/paypercall

Scaling

https://medium.com/thunderofficial/2018-blockchain-scaling-all-else-7937b660c08
Bitcoin, designed to be the currency of the internet, is limited to 7 transactions per second. Ethereum manages fewer than 50 transactions per second. Now compare these to Visa’s 24,000 tx/s. Graph:
https://cdn-images-1.medium.com/max/800/0*dp1Ce7bNfuN1MFcV

- https://igniteoutsourcing.com/publications/blockchain-asset-management/
- The Bitcoin blockchain can achieve only seven transactions per second, while Visa blazes along at more than 24,000 per second.

"cryptocurrencies simply do not scale like sovereign moneys. At the most basic level, to live up to their promise of decentralised trust cryptocurrencies require each and every user to download and verify the history of all transactions ever made, including amount paid, payer, payee and other details. With every transaction adding a few hundred bytes, the ledger grows substantially over time. For example, at the time of writing, the Bitcoin blockchain was growing at around 50 GB per year and stood at roughly 170 GB. Thus, to keep the ledger's size and the time needed to verify all transactions (which increases with block size) manageable, cryptocurrencies have hard limits on the throughput of transactions (Graph V.4, centre panel)" https://www.bis.org/publ/arpdf/ar2018e5.pdf
Diagram: energy consumption and scaling issues, p. 99

"Another aspect of the scalability issue is that updating the ledger is subject to congestion. For example, in blockchain-based cryptocurrencies, in order to limit the number of transactions added to the ledger at any given point in time, new blocks can only be added at pre-specified intervals. Once the number of incoming transactions is such that newly added blocks are already at the maximum size permitted by the protocol, the system congests and many transactions go into a queue. With capacity capped, fees soar whenever transaction demand reaches the capacity limit (Graph V.5)." https://www.bis.org/publ/arpdf/ar2018e5.pdf
Diagram: p. 100

https://medium.com/thunderofficial/2018-blockchain-scaling-all-else-7937b660c08
"They don't yet work. One day they will, but because of their scalability failures, they cannot in their current form. Try to send even small sums of money with Bitcoin, and you could run into confirmation latencies of over an hour, and transaction fees over $20. Bitcoin is practically unusable for its original purpose. How can this be ready to become the world's currency?"

https://medium.com/thunderofficial/2018-blockchain-scaling-all-else-7937b660c08
"Cryptokitties, touted as a demonstration of Ethereum 's viability, actually illustrated its failure. The application's just 14,000 daily users were enough to double gas prices, contribute to a 6x increase in transaction latencies, and slow the network to a halt. Due to network issues, simple actions like creating ("breeding") a new cat increased from an already high $1 to an astounding $8. (This fee doesn't even include the siring fee charged by Axiom Zen—it was only the fee paid to Ethereum miners)" Graph: https://cdn-images-1.medium.com/max/800/0*kaDDc4MheFa2tBNh

Transition Costs

- https://igniteoutsourcing.com/publications/blockchain-asset-management/
- Blockchain promises/threatens to bring about rapid and radical changes to the venerable financial institutions upon which we have come to rely. How rapid and how radical the transformation may be is limited, in part, by the cost of implementation.

Social-Political Issues

Token Distribution

Token Distribution and Open Cryptoeconomic Networks
https://medium.com/@gruvydhruvy/token-distribution-and-open-cryptoeconomic-networks-3d6b9b842628 “most Bitcoiners (and cryptocurrency supporters in general) fail to understand how early adoption will impact the currency in the future. Even in the present, we can see how the Bitcoin protocol enables centralization through mining, while a capped supply fundamentally limits the amount of Bitcoin one person can hold. As more and more people join the cryptocurrency world, it is important to understand how the distribution of tokens in these networks will affect both their behavior and freedom of future participants.”

Extremes of capitalism

http://donaldclarkplanb.blogspot.com/2018/06/blockchain-got-married-on-it-but-fell.html
“You can’t go all ‘activist’ on me and blame the man, then use Bitcoin (therefor Blockchain). All you’re doing is playing around in the extremes of capitalism – the really bad bit, where capital is hidden, secret and not subject to tax. I said two years ago that the Wild West world of Bitcoin could do with some Sheriffs. I'm now of the opinion that it needs to be closed down.”

Regulation

- https://igniteoutsourcing.com/publications/blockchain-asset-management/
- distributed ledgers do not always lend themselves to meeting the regulations designed for siloed systems.

- Clinton government E-Commerce white paper - The Framework for Global Electronic Commerce https://clintonwhitehouse4.archives.gov/WH/New/Commerce/index.html

- Learn the lessons of Commerce One - https://en.wikipedia.org/wiki/Commerce_One

- Also - note Java - which got a billion of investment

- the *Wall Street Journal* reports that government investigators have demanded that four cryptocurrency exchanges—Bitsamp, Coinbase, itBit, and Kraken—turn over “comprehensive trading data” to assist a probe into whether manipulation is distorting recently-launched Bitcoin futures markets, which rely on an index derived from the prices at the four exchanges.

https://www.bis.org/publ/arpdf/ar2018e5.pdf p.105

- A first key regulatory challenge is anti-money laundering (AML) and combating the financing of terrorism (CFT).
- A second challenge encompasses securities rules and other regulations ensuring consumer and investor protection
- A third, longer-term challenge concerns the stability of the financial system.

https://www.bis.org/publ/arpdf/ar2018e5.pdf p.105 How can authorities implement a regulatory approach? Three considerations are relevant.

- First, the rise of cryptocurrencies and cryptoassets calls for a redrawing of regulatory boundaries - only globally coordinated regulation has a chance to be effective.
- Second, the interoperability of cryptocurrencies with regulated financial entities could be addressed.
- Third, regulation can target institutions offering services specific to cryptocurrencies.

Volatility

At least in crypto currencies - Bitcoin eg. training between $7K and $25K
https://technologyreview.us11.list-manage.com/track/click?u=47c1a9cec9749a8f8cbc83e78&id=21ed476afd&e=859794f490

BIS Annual Economic Report 2018 - Part V - https://www.bis.org/publ/arpdf/ar2018e5.pdf
"Sustained episodes of stable money are historically much more of an exception than the norm. In fact, trust has failed so frequently that history is a graveyard of currencies. … history proves that money can be fragile whether it is supplied through private means, in a competitive manner, or by a sovereign, as a monopolist supplier. Bank- issued money is only as good as the assets that back it."

- The 'Money Flower' diagram, p. 94

https://www.bis.org/publ/arpdf/ar2018e5.pdf
Diagram, volitility, p. 101

South Korea's central bank says issuing a digital currency could pose a "moral hazard" by risking the destabilization of the economy. (CoinDesk) -
https://www.coindesk.com/bank-of-korea-central-bank-cryptocurrencies-pose-moral-hazard/

https://medium.com/@Michael_Spencer/how-doomed-are-token-startups-129172d61031 "A Chinese government analysis has concluded the average lifespan of a blockchain project is 1.22 years, sources report May 28. (2018) … According to a recent report: 902 startups that launched ICOs last year, **46 percent** have already failed, despite having raised over US$104 million, according to a survey conducted by cryptocurrency news site Bitcoin.com. … For the over 80,000 blockchain projects ever launched globally, only 8% are still being actively maintained and the average life span is only around 1.22 years, says an official at the China Academy of Information and Communications Technology (CAICT)."

The Failure Rate of ICOs is Skyrocketing in 2018
https://medium.com/futuresin/the-failure-rate-of-icos-is-skyrocketing-in-2018-c6d2cb680807

Map: https://cdn-images-1.medium.com/max/800/1*NSitHlBo3UJHHANAnKUE5g.jpeg

Tax Trouble for Certain Bitcoin Traders
https://medium.com/forbes/tax-trouble-for-certain-bitcoin-traders-41414e4d47a8
"What do you do, come April 17, if you made a ton of money trading crypto last year and have since lost most of it? Panic, probably."

Dormant Wallets

Cumulative Sum in Dormant Bitcoin Wallets
https://bitinfocharts.com/top-100-dormant_5y-bitcoin-addresses.html

What Would Happen To Bitcoin If Satoshi Nakamoto's 1 Million Coins Moved
https://bitcoinexchangeguide.com/what-would-happen-to-bitcoin-if-satoshi-nakamotos-1-million-coins-moved/ "It's highly unlikely that no single other person in the world owns more bitcoin than Satoshi Nakamoto. Nobody has ever simultaneously moved one million bitcoin. Selling that much bitcoin would crash the market."

Are You Ready for What Happens If Satoshi's Coins Move?
https://news.bitcoin.com/are-you-ready-for-what-happens-if-satoshis-coins-move/

This Dormant $720 Million Bitcoin Wallet Has Woken Up – But Who Owns It?
https://www.ccn.com/dormant-720-million-bitcoin-wallet-owner/

It's a Bubble

https://medium.com/crypto-oracle/8-thoughts-on-blockchain-cryptocurrency-decentralization-after-another-three-months-down-the-448b916138b8

- Here's a great book on the last 800 years of people saying "it's different" this time to justify lofty valuations.
- Amara's Law: *We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run.* This is part of the reason we get bubbles.

Will The Bitcoin Bubble Pop? Or Will It Envelop Us All?
https://arcdigital.media/will-the-bitcoin-bubble-pop-or-will-it-envelop-us-all-5d5d9ed94503
"Timothy Morton uses a term to describe "events or systems or processes that are too complex, too massively distributed across space and time, for humans to get a grip on." He calls such things hyperobjects… Bitcoin is such a hyperobject, the first of its kind. "
Price chart: https://cdn-images-1.medium.com/max/1000/1*7mnGcxKSTATtENHTw8bm1g.png

Credentialism

http://donaldclarkplanb.blogspot.com/2018/06/blockchain-got-married-on-it-but-fell.html

But the main problem is that Blockchain in learning simply reinforces runaway credentialism. Bryan Caplan's book shows that Higher Education has expanded on the back of 'signalling'. This has resulted in credential inflation, where more and more young people stay at college for longer and longer, just to get the inflated paper they need for a job. If Blockchain simply makes credentialism easier, then forget it. Ah, I hear you say, but it's really about micro-credentialism. That's fine but I also think that this has had its day. The badges movement has run out of steam, as they turned out to be motivationally suspect, lack objectivity and therefore credibility, as well as the awful branding. It has flopped.

Market Failures

The market is dead: long live the market
https://wonkhe.com/blogs/the-market-is-dead-long-live-the-market/
Adam Wright says it all in the first paragraph: "There is no evidence that greater competition between higher education providers will improve the quality of provision. This is the conclusion of the Public Accounts Committee's (PAC) recent (21 page PDF well worth reading in its own right - SD) report into the higher education market. But, rather than question whether the government is right to keep pursuing a strongly market-based policy agenda in higher education, the committee appears to ignore the possibility that the market simply *doesn't work* in HE."

Bro Culture

As Bitcoin Sinks, Crypto Bros Party Hard on a Blockchain Cruise
https://medium.com/bloomberg/as-bitcoin-sinks-crypto-bros-party-hard-on-a-blockchain-cruise-ea4f815f5c95

I Attended a Crytocurrency Party and Stepped Into the Future.
https://medium.com/@chilee_22/i-attended-a-crytocurrency-party-and-stepped-into-the-future-64a83484e9f4

Libertarianism

Blockchain Could Reshape the World—and the Far Right Is One Step Ahead
Crypto technology is coming to a crossroads. Those who want to use it to radically redistribute wealth must take urgent action
https://medium.com/the-guardian/blockchain-could-reshape-the-world-and-the-far-right-is-one-step-ahead-6e83969904f8

Scams and Fraud

most ICOs are scams. https://kingpassive.com/what-is-ethereum/

- Diagram - https://kingpassive.com/wp-content/uploads/2018/05/download-1.jpeg

The 5 Worst Bitcoin Scams
https://www.digitaltrends.com/computing/worst-bitcoin-scams/

https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block "We now receive over 1,500 SARs per month describing suspicious activity involving virtual currency, with reports coming from both MSBs in the virtual currency industry itself and other financial institutions."

Top 10 "Stay Away" ICO Directions in 2018
https://medium.com/@bdaqio/top-10-stay-away-ico-directions-in-2018-117973fe8a66

- Diagram - types of frauds: https://cdn-images-1.medium.com/max/800/0*O4bikOndstExvkUA

http://donaldclarkplanb.blogspot.com/2018/06/blockchain-got-married-on-it-but-fell.html
"Serious problems have emerged with the technology. Bitcoin looks increasingly like a money laundering scam, wracked with hacks, fraud, theft, ransoms and Ponzi schemes. The hackless future that was promised turned out to be a bit of a dystopian Westworld. This should worry those who want it used in the public sector."

https://media.consensys.net/china-and-blockchain-technology-an-introduction-9e12adf9fd52
Chinese regulation stemmed from the November 2013 GBL incident. GBL was a bitcoin trading platform claiming to be based in Hong Kong. The site attracted more than 1,000 Chinese investors after its launch in May 2013. On October 26, GBL vanished.

https://www.bloomberg.com/news/articles/2018-05-11/cryptocurrency-exchange-upbit-raided-by-south-korean-authorities
South Korea Raids Largest Cryptocurrency Exchange (May 11th)**:** South Korean prosecutors raided the offices of Upbit, one of the world's largest cryptocurrency exchanges. The exchange hosted about $1.6 billion in cryptocurrency trades in the past 24 hours, making it the biggest in Korea and the fourth largest in the world among fee-charging venues tracked by Coinmarketcap.com. Regulators in South Korea have long been concerned about the potential for cryptocurrencies to be used to facilitate illegal activity via money laundering.

https://readwrite.com/2018/06/21/most-people-are-dead-wrong-about-bitcoin-and-criminals/
In early April, the Securities and Exchange Commission urged a federal judge to freeze $27 million that was allegedly garnered through the illegal sale of shares in LongFin — a company whose stock shot from $5 to $142 after announcing it was acquiring a cryptocurrency business. At the same time, the Federal Trade Commission charged a group of individuals with fraud. They're accused of promoting an allegedly deceptive investment scheme by fooling investors into paying them via bitcoin or Litecoin, while another defendant is also accused of promoting the allegedly deceptive cryptocurrency Jetcoin.

FBI Has 130 Cryptocurrency-Related Investigations, Agent Says
https://www.bloomberg.com/news/articles/2018-06-27/fbi-has-130-cryptocurrency-related-investigations-agent-says?srnd=cryptocurriences

http://www.europarl.europa.eu/cmsdata/149900/CASE_FINAL%20publication.pdf
"Financial regulators may dislike VCs because of their anonymity or cross -border circulation. They

tend to fear that VCs will facilitate money laundering, the financing of illegal activities, tax avoidance, the circumvention of capital controls (in countries where such controls are in place), and fraudulent financial practices. Such concerns may be legitimate in some instances but must not be generalised."

Responses:
https://readwrite.com/2018/06/21/most-people-are-dead-wrong-about-bitcoin-and-criminals/

Fake ICOs

https://medium.com/@Valore/most-common-cryptocurrency-scams-tips-to-avoid-them-81126c9f399a

- In a recent study 80% of the ICOs conducted in 2017 were identified as scams. One of the most popular was Confido.
- An even larger ICO scam was Centra, which raised $32M and was supported by celebrities Floyd Mayweather and DJ Khaled. In April 2018 the two founders were arrested,
- Other Fake ICO scams:
    - https://www.reddit.com/r/CryptoCurrency/comments/8kg1i5/scam_alert_goldunioncoin_whitepaper_lists_fake/
    - https://techcrunch.com/2018/04/13/exit-scammers-run-off-with-660-million-in-ico-earnings/

ReCoin
The Brazen Fraud Case That May Help Determine The Future Of ICOs
https://medium.com/fast-company/the-brazen-fraud-case-that-may-help-determine-the-future-of-icos-8c91bd477f71
Maksim Zaslavskiy's token sale lured scores of investors by boasting about real estate and diamonds. Now he's fighting securities fraud charges in one of the first sets of ICO cases pursued in the U.S.

3 Ways to Tell If Your Blockchain ICO Is a Scam
https://medium.com/inc./3-ways-to-tell-if-your-blockchain-ico-is-a-scam-592885339be7
Google and Facebook are cracking down on ICOs because of get-rich-quick schemes. This CEO wants to change the way you think about them.

Social media giveaway scams

https://medium.com/@Valore/most-common-cryptocurrency-scams-tips-to-avoid-them-81126c9f399a
Whenever you read "send 1 ETH to this address and receive X amount back", that ia a sure scam.

Market Manipulation

- The 50%+1 problem, for example
- around 1,600 wallets hold roughly a third of all available bitcoins. That means trades from just a few people (like a handful of colluding "whales," or individuals with large holdings) can heavily influence the price.

Survival guide on dump times for Bitcoin and CryptoCurrencies - https://blog.usejournal.com/survival-guide-on-dump-times-for-bitcoin-and-cryptocurrencies-fb542a31a5b1

Crypto Coin Tether Defies Logic on Kraken's Market, Raising Red Flags
https://www.bloomberg.com/graphics/2018-tether-kraken-trades/?srnd=cryptocurriences
"On June 13, University of Texas Professor John Griffin, known for flagging suspicious activity on Wall Street, released a research paper focusing on the use of Tether to buy Bitcoin on another exchange, Bitfinex. He concluded transactions elevating Bitcoin's price were "consistent with a manipulation hypothesis." Bitfinex disputed his findings. Bitcoin tumbled following the report. Read more about John Griffin's Bitcoin report"
\
https://medium.com/financial-times/who-really-owns-bitcoin-now-bcccc5aa0014
A small cluster of investors—known colloquially as "whales"—capture a hefty proportion of the market, which stands at odds with bitcoin's mission to democratise finance. This brings its own risks.

Pump and dumps
https://medium.com/@Valore/most-common-cryptocurrency-scams-tips-to-avoid-them-81126c9f399a

- Image Source: https://bitfalls.com/2018/01/12/anatomy-pump-dump-group/
- https://cointelegraph.com/news/pump-and-dump-in-crypto-cases-measures-warnings
- PnD Walkthrough: https://www.businessinsider.com/how-traders-pump-and-dump-cryptocurrencies-2017-11

Some Traders Are Talking Up Cryptocurrencies, Then Dumping Them, Costing Others Millions
https://www.wsj.com/graphics/cryptocurrency-schemes-generate-big-coin/ (paywall)

- An impressive investigation by the *Wall Street Journal* provides a glimpse of just how pervasive price manipulation schemes are in the cryptocurrency marketplace.

Bots Are Manipulating Price of Bitcoin in 'Wild West of Crypto'
https://www.wsj.com/articles/the-bots-manipulating-bitcoins-price-1538481600

The Bitcoin network at risk
https://medium.com/@francois.chollet/the-bitcoin-network-at-risk-bd54a1473a1d
"hardware is no longer scarce and mining has suddenly become a highly competitive market with virtually no barrier to entry…. which means that a bargain hunter could relatively easily assemble a mining fleet that would be sufficient to perform a 51% attack."

Money Laundering

http://www.europarl.europa.eu/cmsdata/149900/CASE_FINAL%20publication.pdf
Christine Lagarde, the Managing Director of the IMF, highlighted VCs' potential as a vehicle for money laundering and the financing of terrorism and called for "...policies that ensure financial integrity and protect consumers in the crypto world just as we have for the traditional financial sector" https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world/

Russian agents accused of using cyberattacks to interfere in the last US presidential election allegedly used Bitcoin to help fund the operation.
https://www.technologyreview.com/the-download/611648/russian-agents-allegedly-used-bitcoin-to-fund-the-dnc-hack/

- What the Russia Hack Indictments Reveal About Bitcoin - https://www.nytimes.com/2018/07/22/opinion/russia-hacking-indictments-bitcoin.html

G20 Eyes October Deadline for Crypto Anti-Money Laundering Standard
https://www.coindesk.com/g20-eyes-october-deadline-for-crypto-anti-money-laundering-standard/

Ponzi

Ethereum is full of ponzis, is that a problem?
https://jpkoning.blogspot.com/2018/05/ethereum-is-full-of-ponzis-is-that.html

Pomzi Games

- Fomo3D - http://exitscam.me/shakedown
- PoWH 3D - https://powh.io/index.html

Ethereum, FOMO3D, and Dangerous Game Theory
https://hackernoon.com/fomo3d-and-dangerous-game-theory-97bd5f47ab3b

Cloud Mining scams
https://medium.com/@Valore/most-common-cryptocurrency-scams-tips-to-avoid-them-81126c9f399a
A well known case is MiningMax, a cloud based mining service that was asking people to invest $3,200 for daily ROIs over two years, and a $200 referral commission for every personally recruited investor, making it a clear ponzi scheme.
More examples here:

- https://bitcoinist.com/mining-max-pyramid-scheme-comes-crashing-down/
- https://coincentral.com/the-past-and-present-of-bitcoin-mining-fraud/
-

The most notorious Ponzi scheme in crypto was Bitconnect.
https://thenextweb.com/hardfork/2018/01/17/bitconnect-bitcoin-scam-cryptocurrency/

Redditors compiled a list of Ponzi schemes in the cryptosphere
https://www.reddit.com/r/CryptoCurrency/comments/7r6chx/here_is_a_list_of_crypto_ponzi_schemes_and_people/

Bitcoin Savings and Trust

https://www.coindesk.com/bitcoin-ponzi-scheme-18-months-prison-bitcoin-savings-trust/

“Bitcoin Savings and Trust was even more blatant: It started out as an ICO scam based around a simple Ponzi scheme, and then…kept on going. Unwitting investors were promised amazing returns like 7 percent per week, and ultimately more than 265,000 bitcoins were stolen via fraud. The whole Savings and Trust scheme finally collapsed in 2012, and the organizer Trendon Shavers was caught up in court battles for years: This eventually led to his imprisonment and a $40 million fine”

Kodak Bitcoin mining 'scam' evaporates
https://www.bbc.co.uk/news/technology-44845291
“In its promotional material, Spotlite said an up-front investment of $3,400 would generate earnings of $375 a month for two years by mining Bitcoin. However, critics said the promised profits did not take into account that mining Bitcoin is becoming increasingly difficult.”

QuadrigaCX

- The Royal Canadian Mounted Police, the FBI, an Australian investigative agency, and a fourth undisclosed agency are all apparently investigating QuadrigaCX, the defunct Canadian cryptocurrency exchange that collapsed earlier this year after the mysterious death of its founder.
  https://www.coindesk.com/4-agencies-are-investigating-crypto-exchange-quadrigacx-ey-report

Phishing

Dissecting a HitBTC phishing site
https://medium.com/mycrypto/dissecting-a-hitbtc-phishing-site-8e631a6c29a3

Cloned websites
https://medium.com/@Valore/most-common-cryptocurrency-scams-tips-to-avoid-them-81126c9f399a
“Exact clones of legitimate projects, generally exchanges or ICO websites, are used to steal funds and personal information.”

- examples:
  - https://thehackernews.com/2017/04/unicode-Punycode-phishing-attack.html
    https://www.reddit.com/r/CryptoCurrency/comments/7ykzar/be_careful_of_spoof_exchanges_would_you_have/
  - https://twitter.com/bitfinex/status/910289315829297152
  - https://www.reddit.com/r/CryptoCurrency/comments/7nwhgh/beware_of_fake_binance_sites_in_google_ads_as_i/

Ad scams
https://medium.com/@Valore/most-common-cryptocurrency-scams-tips-to-avoid-them-81126c9f399a
“ads leading to phishing sites. Recent examples include Google Ads to cloned exchanges and Reddit ads to Trezor hardware wallet sale offers.”

- Ad scam examples:
  - https://www.ccn.com/reddit-removes-fake-trezor-ad-soliciting-orders/

- https://www.reddit.com/r/CryptoCurrency/comments/72osg0/scam_alert_fake_shapeshift_site_suggested_by/
- https://www.reddit.com/r/CryptoCurrency/comments/8i96i8/scam_alert_ad_on_google_be_aware_dont_fall_for/

Email scams
https://medium.com/@Valore/most-common-cryptocurrency-scams-tips-to-avoid-them-81126c9f399a

- fake emails can redirect the users to fake websites where they attempt to steal funds and personal information.
- https://www.reddit.com/r/CryptoCurrency/comments/8c33ce/scam_alert_coinbase_erc20_support/

Fake Support Teams
https://medium.com/@Valore/most-common-cryptocurrency-scams-tips-to-avoid-them-81126c9f399a

Fake exchanges and apps
https://medium.com/@Valore/most-common-cryptocurrency-scams-tips-to-avoid-them-81126c9f399a

- BitKRX, a fake exchange that was discovered and seized in 2017: https://www.coinwire.com/south-korean-government-cracks-down-on-fraudulent-exchanges
- Another example from the Ukraine: https://news.bitcoin.com/six-fake-crypto-exchange-sites-busted-by-ukraines-cyberpolice/
- https://twitter.com/myetherwallet/status/939763116522344448
- https://www.reddit.com/r/CryptoCurrency/comments/7r4vcv/koinbi_another_fake_exchange_website_is_stealing/

MetaMask

https://medium.com/metamask/new-phishing-strategy-becoming-common-1b1123837168
MetaMask allows users to interact with Ethereum-compatible sites by putting users in control of their own account secrets, in the form of the 12 secret words the user is shown when first setting up.
This is very powerful, but also potentially dangerous, because each user is responsible for the secrecy of their own seed words. If a hacker can trick you into sharing those words, they can steal everything in your accounts.

Silk Road

https://www.digitaltrends.com/computing/worst-bitcoin-scams/
“The government agreed to auction offer the Bitcoins seized from Silk Road… a wave of scam emails sent to all these people who were already interested in buying Bitcoins. Phishing schemes like this one pretended to be from the government or related agencies”

Electrum Bitcoin

Electrum Bitcoin $BTC▲2.78% wallet users have lost 771 BTC
(approximately $4 million) since late December 2018, in an ongoing series of targeted phishing attacks.
https://thenextweb.com/hardfork/2019/04/16/behind-the-scenes-electrum-hackers-steal-4m-with-bitcoin-phishing-attacks/

Gambling

China breaks up underground $1.5 billion World Cup crypto-gambling ring
https://thenextweb.com/hardfork/2018/07/13/china-gambling-undergroind-world-cup/

Assassination black markets now available on the blockchain
https://www.patreon.com/posts/assassination-on-20327334
See also https://motherboard.vice.com/en_us/article/gy35mx/ethereum-assassination-market-augur

Insider Trading

Coinbase Finds No Insider Trading of Bitcoin Cash
http://fortune.com/2018/07/24/coinbase-insider-trading/

- A class action lawsuit filed by Coinbase customers is ongoing, and seeks damage from the company for negligence and violating consumer protection laws.

-

Crypto-Kidnapping

Via CBC newsletter:

> Cryptocurrency kidnappings are a growing trend.
>
> The first major incident involved Ryan Bate, a Canadian entrepreneur living in Costa Rica, who was snatched in January 2015 and ultimately ransomed for a reported $500,000 US in Bitcoin.
>
> In December 2017, a Ukraine-based employee of a British cryptocurrency company was released unharmed after a three-day ordeal and a $1 million U.S. Bitcoin payment.
>
> South Africa has seen at least three crypto-kidnappings in recent months, including the July abduction of the owner of a supermarket chain — ultimately freed for 50 Bitcoin (then worth more than $400,000 Cdn). Just this week, a gang issued a 5 Bitcoin ($26,400 Cdn) demand for the safe return of a missing nine-year-old girl.

Similar crimes have been reported in Turkey and India.

Control Risks, a global consulting firm, issued a report this past summer detailing incidents in at least a dozen nations, and noting a significant uptick over the first months of 2018.

The company said that those who flaunt their cryptocurrency wealth online are inviting targets.

But ultimately, it suggested that most kidnappings will remain tied to old school, hard currency ransoms.

"The unregulated and perceived anonymous nature of cryptocurrencies continues to attract the attention of organized criminal groups," the report notes, but "the majority of kidnappers will lack the necessary technical sophistication and are unlikely to move with any haste towards demanding crypto-ransom payments."

Anne-Elisabeth Falkevik Hagen, the wife of a Norwegian energy tycoon has been kidnapped, police revealed today, … the Norwegian daily *Verdens Gang* reports that the ransom demand was for €9m ($13.71 million Cdn) payable via Monero, a cryptocurrency that obscures both the source and destination of payments.

Enforcement

https://er.educause.edu/articles/2018/5/will-blockchains-revolutionize-education
"That is, blockchain records of off-chain assets might be immutable but not enforceable, or they might be necessary but not sufficient conditions for ownership exchange."

- Quality or value is a more serious issue
- statements that are now true but could later prove false can be immutably placed on the public blockchain.
- "To preserve this immutability, oracles have been suggested as intermediaries. Blockchains can guarantee immutability because they cannot access content outside their records. Oracles are agents associated with a blockchain that would be trusted to verify external data for blockchain decisions under specific conditions."
-

Cybersecurity

Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry March 2018

White Paper by Microsoft

https://digitalchamber.org/wp-content/uploads/2018/03/Blockchain-Cyber-Security_WhitePaper_Single-Page_Linked.pdf

https://www.reuters.com/article/us-crypto-currencies-ciphertrace/cryptocurrency-exchange-theft-surges-in-first-half-of-2018-report-idUSKBN1JT1Q5
$761 million has been stolen from cryptocurrency exchanges so far in 2018, versus $266 million in all of 2017.

How secure is blockchain really?
https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/

Software Bugs

Responsible disclosure in the era of cryptocurrencies: My experience disclosing a critical Bitcoin Cash vulnerability
https://medium.com/mit-media-lab-digital-currency-initiative/http-coryfields-com-cash-48a99b85aad4

Cryptojacking

Cryptojacking Malware: What It Is and How to Fix It
https://readwrite.com/2018/08/01/cryptojacking-malware-what-it-is-and-how-to-fix-it/
"Cryptojacking is a cyberattack like no other. Attackers don't steal your data or ransom off access to your network. Instead, they commandeer your hardware when you're not looking and redline the processors to mine cryptocurrency. Since 2017, cryptojacking's popularity has skyrocketed. Palo Alto Networks' WildFire platform has identified roughly 470,000 unique types of cryptomining malware, not including those delivered through web-based JavaScript activities. Together, these viruses have affected 40 percent of corporations across the globe."

DNS hacks

https://medium.com/@Valore/most-common-cryptocurrency-scams-tips-to-avoid-them-81126c9f399a
Both Etherdelta, a now almost defunct decentralized exchange, and MyEtherWallet were victims of DNS hacks

- https://www.ccn.com/cryptocurrency-exchange-etherdelta-hacked-in-dns-hijacking-scheme/
- https://bitcoinist.com/myetherwallet-users-lose-funds-to-dns-hack/).

Malware

The malware secretly uses the infected computer's resources to mine cryptocurrency, effectively creating a decentralized mining network
https://www.zdnet.com/article/why-cryptocurrency-mining-malware-is-the-new-ransomware/
Some more resources:
https://www.androidauthority.com/millions-android-phones-hijacked-mine-cryptocurrency-837374/

Two Romanian residents have been convicted of infecting over 400,000 individual computers with malware in order to mine cryptocurrency and steal victims' data to sell on the dark web. https://thenextweb.com/hardfork/2019/04/12/romanian-duo-convicted-in-us-for-using-cryptocurrency-malware-mining-to-steal-millions/

Phone hacks

https://medium.com/@Valore/most-common-cryptocurrency-scams-tips-to-avoid-them-81126c9f399a
"several prominent crypto influencers reported their assets stolen by the attacker taking over control of their phone number."

- https://fabricegrinda.com/hacked-cryptocurrencies-stolen/
- https://motherboard.vice.com/en_us/article/a3q7mz/hacker-allegedly-stole-millions-bitcoin-sim-swapping

Selfish Miner

https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really
"Emin Gün Sirer and his colleagues at Cornell University have shown that there is a way to subvert a blockchain even if you have less than half the mining power of the other miners. The details are somewhat technical, but essentially a "selfish miner" can gain an unfair advantage by fooling other nodes into wasting time on already-solved crypto-puzzles."

Eclipse Attack

https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really
"Nodes on the blockchain must remain in constant communication in order to compare data. An attacker who manages to take control of one node's communications and fool it into accepting false data that appears to come from the rest of the network can trick it into wasting resources or confirming fake transactions."

Cybersecurity Events

The Dao

- One third of The DAO's funds were stolen (valued at about $50 million at the time).
- The community was split with regards to how to deal with the hack, which led to the split of Ethereum - https://kingpassive.com/what-is-ethereum/

Parity Hacks.

- Parity is an Ethereum wallet provider that's had a run of bad publicity. July 2017, $30 million in Ether was stolen from Parity wallets. Not shortly after in November of that

year, $100 million in fund was frozen because of a coding issue.
https://kingpassive.com/what-is-ethereum/

Coinrail

- intruders stole nearly $40 million worth of digital coins from the Korean trading platform Coinrail.

Mt. Gox

Mt. Gox was the biggest bitcoin company in the world…until it lost everyone's money
https://moneybadger.stocktwits.com/history-of-mt-gox-bitcoin/
Mt. Gox began as Magic: The Gathering Online Exchange, a digital marketplace that allowed players of the online card game to trade in-game cards as if they were stocks. The founder, Jed McCaleb, then pivoted the site into a bitcoin exchange after learning about the growing popularity of the cryptocurrency…. In late February 2014, Mt. Gox disappeared overnight. The company allegedly lost 744,408 bitcoins in a major security breach, along with hundreds of thousands of the company's own bitcoin, rendering them insolvent.

Also: https://en.bitcoin.it/wiki/MtGox

Coincheck

https://readwrite.com/2018/06/21/most-people-are-dead-wrong-about-bitcoin-and-criminals/
Japan's Coincheck exchange service is the most recent large-scale hacking victim, losing $500 million worth of NEM coins. It's an alarming sum of money, to be sure, but even more alarming is the fact that Coincheck admitted to storing NEM funds in a "hot wallet" online instead of a "cold wallet" offline. It also failed to use multisignature wallets, which require at least two (and often more) signatures before funds are released.

What the Coincheck hack means for the future of blockchain security
https://www.technologyreview.com/s/610092/what-the-coincheck-hack-means-for-the-future-of-blockchain-security/

BitThumb

- https://www.bbc.com/news/technology-44547250 Bithumb: Hackers 'rob crypto-exchange of $32m'
- Hackers have stolen more than $31 million worth of cryptocurrency from the popular South Korean exchange Bithumb. (Reuters)

HoweyCoins

https://www.sec.gov/news/press-release/2018-88

SEC created a fake ICO site, HoweyCoins.com, as a way to demonstrate to investors that it is easy to create a fake project and website.

Bitfinance API

Binance API Attacked As Hackers Sell One Syscoin for 96 Bitcoins

July 4, 2018
https://btcmanager.com/binance-api-attacked-as-hackers-sell-one-syscoin-for-96-bitcoins/
The world's largest cryptocurrency exchange by trading volume, Binance, faced an embarrassing situation on July 3, 2018, as attackers took advantage of an API hack to sell a single Syscoin (SYS) for 96 bitcoins (BTC). Binance API Attacked Over a billion SYS were moved from a wallet, rumoured to be owned by Binance, after enterprising attackers took advantage of the…

Canadian Bitcoins

https://www.digitaltrends.com/computing/worst-bitcoin-scams/
Canadian Bitcoins, an exchange that was used to—as you might guess—manage Bitcoins for Canadian investors. Back in 2014, the exchange was expertly hacked, and at least $100,000 dollars worth of Bitcoins were stolen…. A hacker sent a message to Rogers Data Centre that (basically) said, "Hello, I am the CEO of Canadian Bitcoins. My name is James Grant. I need all your security codes." Rogers verified that the CEO of Canadian Bitcoins was indeed named James Grant, then sent the hacker all the security codes they needed."

Zaif - Japan

https://www.ccn.com/licensed-crypto-exchange-zaif-plans-compensation-after-6000-bitcoins-60-million-crypto-theft/ "In the second major hack of a Japanese cryptocurrency exchange this year, some 6.7 billion yen ($60 million) in cryptocurrencies were stolen from the wallets of Zaif of which 4.5 billion yen ($40 million) belonged to customers."

Coinbase

https://www.zdnet.com/article/firefox-zero-day-was-used-in-attack-against-coinbase-employees-not-its-users/
https://blog.coinbase.com/responding-to-firefox-0-days-in-the-wild-d9c85a57f15b
reported that hackers had targeted Coinbase employees with an attack designed to exploit zero-day vulnerabilities in Mozilla's Firefox browser.

Risks

https://edtechmagazine.com/higher/article/2018/06/cryptocurrencies-make-their-way-campus-bringing-flexibility-and-risks

If ransomware was the scourge of 2017, cryptocurrency mining could be the problem to watch this year — especially in higher education. In a recent Vectra analysis of the five industries showing cryptocurrency mining attacks, higher education had the majority of activity by far (85 percent).

Legal Issues

Blockchain and the Law: The Rule of Code Hardcover – April 9, 2018
https://www.amazon.com/Blockchain-Law-Rule-Primavera-Filippi/dp/0674976428

“two basic questions regarding the usefulness of cryptocurrencies. First, does this cumbersome way of trying to achieve trust come at the expense of efficiency? Second, can trust truly and always be achieved?” https://www.bis.org/publ/arpdf/ar2018e5.pdf

IP

A Blockchain Innovator’s Guide to IP Strategy
March 2018
A blockchain innovator’s guide to IP strategy, protecting innovation & avoiding infringement
https://digitalchamber.org/wp-content/uploads/2018/03/Blockchain-Intellectual-Property-Council-White-Paper-Electronic-FINAL.pdf

GDPR

Saving Private Ryan: Reconciling Blockchain technology with the GDPR’s “Right To Be Forgotten”
https://medium.com/gradbase-blog/saving-private-ryan-reconciling-blockchain-technology-with-the-gdprs-right-to-be-forgotten-d6da3d8ad600
“The solution to this conundrum lies in the GDPR legislation itself, which is not prescriptive in the way the erasure of data should be conducted. Companies, for example, could make the data permanently unintelligible by some cryptographic means that are controlled by the owner of the data. This solution enables the data to be stored permanently, but as nobody can have access to it, it would be equivalent to “being forgotten”.”

How to design a GDPR-compliant blockchain
https://venturebeat.com/2018/05/23/how-to-design-a-gdpr-compliant-blockchain/
“Encrypting all personal data with a key and deleting the key in response to a request for erasure would render the data inaccessible to anyone, which in layman’s terms is the same as deletion.”

The EU General Data Protection Regulation and The Blockchain

https://medium.com/@AngelaHabibi/the-eu-general-data-protection-regulation-and-the-blockchain-bc1c50186340 “Microsoft and Intel have joined GDPR Edge, a distributed ledger blockchain solution platform to provide technology support.”

GDPR Edge
https://gdpredge.com/
“GDPR Edge was built with each of the regulation's requirements in mind, which means it is the most effective and simplified tool to operationalize and manage your enterprise's GDPR compliance.”

Blockchain and GDPR - Chainfrog
http://www.chainfrog.com/wp-content/uploads/2017/08/gdpr.pdf

- The right to be forgotten
    - Do not record personal data on a blockchain
    - Record personal data pseudo-anonymously
    - Encrypt the data on the blockchain
    - Store the data in a referenced encrypted database
- Contesting automated decisions
    - Smart contract over-rides
    - Consent and contractual law
    - Decentralized apps and the GDPR

EU GDPR Portal:
http://www.eugdpr.org/eugdpr.org.html

GDPR legislation markup site:
https://www.privacy-regulation.eu/en/

UK ICO – getting ready for GDPR:
https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

Decentralizing Privacy: Using Blockchain to Protect Personal Data;
Zyskind, G., Nathan, O. and Pentland, A. : http://web.media.mit.edu/~guyzys/data/ZNP15.pdf

Blockchain, Personal Data and the GDPR Right to be Forgotten
https://www.blockchainandthelaw.com/2018/04/blockchain-personal-data-and-the-gdpr-right-to-be-forgotten/ “One potential solution to this conundrum might be to store all personal data off of the blockchain in separate “off-chain” databases, but to do so would sacrifice many of the benefits of using a blockchain in the first place.”

Blockchain and GDPR: Between a Block and a Hard Place
https://www.tripwire.com/state-of-security/security-data-protection/blockchain-gdpr/

Blockchains and Data Protection in the European Union by Michèle Finck.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322

Future?

Four Things Missing

https://blockchainatberkeley.blog/4-things-missing-in-the-blockchain-industry-50f97bec098c
The Four Major Things Missing in The Blockchain Industry

- No-knowledge wallets, interfaces, and exchanges - “Another key “bridge” required alongside user-centric infrastructure is the need for organic, frictionless custodial services, especially for non-commercial consumers”
- A Centralized Solution to Interoperability, Scalability, and Liquidity - “the path towards long-term, complete decentralization is often started with the creation of a hybridized service:
    - Interoperable standards that allow for user activity across supporting blockchains and decentralized applications
    - Friendly marketing language to incentivize legacy players to join the system
    - Portable reputation systems for people, contracts, and exchanges to ensure honest behaviour and accountability
    - Liquidity accessible to the public,
- Digital Reserves—taking people out of the “exchange” game into the “convert” game - “we need to have a system in place that takes the arbitrage out of exchanging” (Arbitrage: “the simultaneous buying and selling of securities, currency, or commodities in different markets or in derivative forms in order to take advantage of differing prices for the same asset.”)
- Functional Stablecoin that Supports Economic Growth - “e need some native asset that these people can use that they can have faith in vs their native fiat currency… one core economic issue to stablecoins is that they focus so much on maintaining stability as a transactional store of value that they forget to foster mechanisms for economic growth.”

Four waves of anticipated blockchain deployments

All from https://www.jpmorgan.com/global/cib/markets-investor-services/blockchain-economics

Information sharing

2016-19

- Blockchain used to share and communicate data
- Used internally and between trusted external organizations
- Distributed ledger solutions tested in parallel with current workflows as proof of concept
- Augmentation of existing processes

Data solutions

2017-25

- Blockchain enables an environment to store and manipulate data
- incorporation of distributed ledger technology as part of existing solutions, supporting new efficiencies in operations and workflows
- Initial pilots may run in parallel with existing processes until user confidence is high enough to begin migrating volumes
- Users are faced with a choice of infrastructures developed by providers

Critical infrastructure

2020-30

- Blockchain adopted by market participants as main infrastructure for critical functions
- Centralized authority still required for administrative functions (e.g., granting access rights, setting industry standards)
- Replacement of existing asset, transaction and payments infrastructure
- Participants forced to adopt and integrate new blockchain-based infrastructure

Fully decentralized

Uncertain

- Blockchain replaces centrally controlled infrastructure with fully decentralized solutions
- Direct engagement in digital asset transactions for organizations and individuals
- Legal and regulatory frameworks support asset ownership and transfers via distributed ledgers
- isintermediation of legacy infrastructure owners

The Internet of Value

https://media.consensys.net/the-value-of-being-stupid-about-blockchain-c46ba3c99cd6
Whether or not you really need a blockchain today, times are changing. Countless services are popping up on blockchains like Ethereum. Billions of connections between parties all over the world are surging as networks evolve to handle the load. And standards like ERC20 and ERC721 are making transactions, logic and data models compatible with each other by design.

In 2019, smart consortia won't start by stringing up private networks. They'll start by publishing something like an ERC, setting a standard for *interop* across all applications that implement it. That will help prevent the balkanization and network incompatibility that springs up as solutions that should have started out together come crashing into each other. This is what drives permanent employment and massive profits for system integrators (and bone-crushing costs for the rest of us).

By 2020, the concept of "public" versus "private" blockchain networks will be relegated to a historical footnote. We will not pit public networks against private networks. Instead there will be public *transactions* and private *transactions*, confidential *contracts* and open *contracts*, and they will coordinate their scope across bilateral, multilateral and public environments depending on the needs

of users—just as messages today pass between private and public environments using common Internet protocols.

Quantum-Proofing the Blockchain

Is Quantum Computing an Existential Threat to Blockchain Technology?

it might become possible for an entity exercising such computing power to generate a private key from the corresponding public key.
https://singularityhub.com/2017/11/05/is-quantum-computing-an-existential-threat-to-blockchain-technology/

Researchers in Russia say they've developed and tested the world's first blockchain that won't be vulnerable to encryption-breaking attacks from future quantum computers.
https://www.sciencealert.com/scientists-claim-to-have-invented-the-world-s-first-quantum-proof-blockchain Also
https://www.technologyreview.com/s/608041/first-quantum-secured-blockchain-technology-tested-in-moscow/

- Image - https://cdn.technologyreview.com/i/images/quantum-blockchain.jpg?sw=600&cx=0&cy=11&cw=600&ch=337

If quantum computers threaten blockchains, quantum blockchains could be the defense
https://www.technologyreview.com/s/611022/if-quantum-computers-threaten-blockchains-quantum-blockchains-could-be-the-defense/ “Their idea is to create a blockchain using quantum particles that are entangled in time. That would allow a single quantum particle to encode the history of all its predecessors in a way that cannot be hacked without destroying it.”

qBitcoin: A Way of Making Bitcoin Quantum-Computer Proof? - IEEE .
qBitcoin