Distributed Ledger Technology

Assembled by Stephen Downes

Advanced Concepts	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?

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The Data Encryption Standard (DES) is an outdated symmetric-key method of data encryption.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."