Distributed Ledger Technology

Assembled by Stephen Downes

Future?	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?

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