Blockchain in Fintech

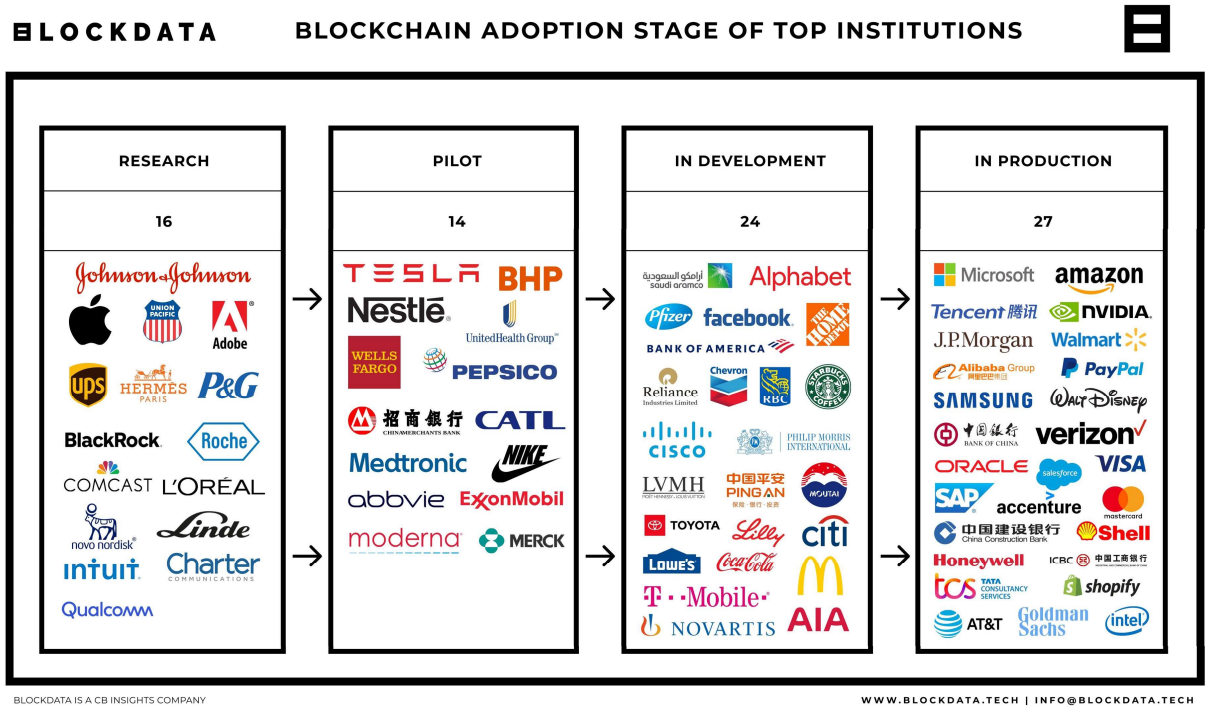
An Overview

Duc Phong Le

FinTech Research, Bank of Canada

Content

Blockchain Technology



(Statistics in Sep 2021):

- 81 of top 100 companies are using blockchain
- **Microsoft, Amazon, Tencent, Nvidia, J.P. Morgan, Walmart, Alibaba, PayPal, Samsung and the Bank of China** are among the 27 companies with live blockchain operations

Source: blockdata.tech

Blockchain for Payments

Nakamoto (2008)

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments …

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.

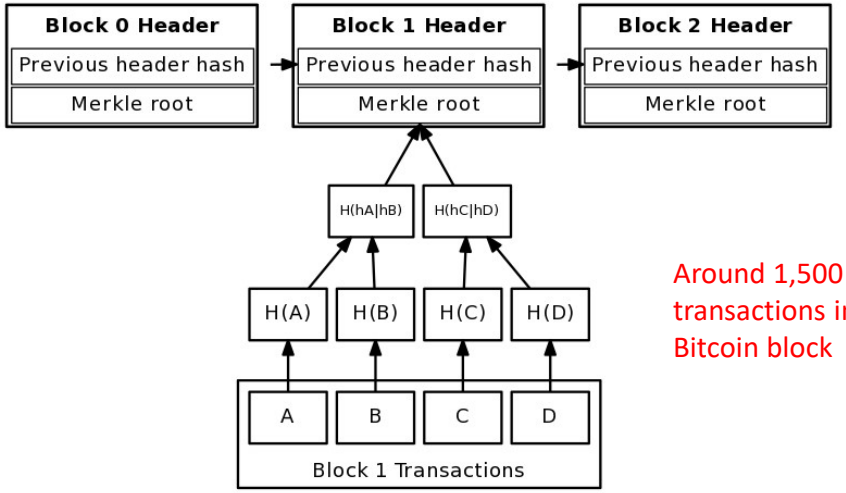
A brief history:

- **D. Chaum** (1990): DigiCash from cryptographic algorithms
- **S. Haber & W. S. Stornetta** (1991): using Merkle tree creating "blocks" to timestamp documents
- **C. Dwork** (1992): Proof of work – punish spammers with computational processing
- **A. Back** (1997): Proof of work system via hashcash, limiting email spam & DoS attacks without requiring a central server
- **N. Szabo** (1997): smart contracts - a distributed trust model

Source: bitcoin.org

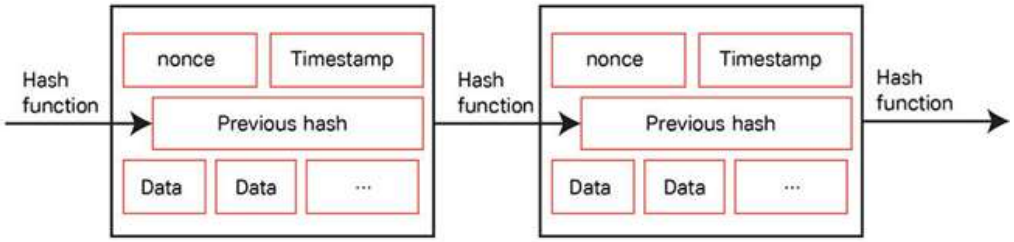
How the blocks are created & chained

- Each block contains transactions data, hash of block, and hash of previous block
- Hashes link blocks, forming a chain
- Timestamps, Hashes make more difficult for an adversary to manipulate the blockchain
- Bitcoin groups transactions into blocks about every 10 minutes



Merkle tree connecting block transactions to block header merkle root

Around 1,500 transactions in each Bitcoin block



Basic blockchain principle

Source: NIST

What is Blockchain?

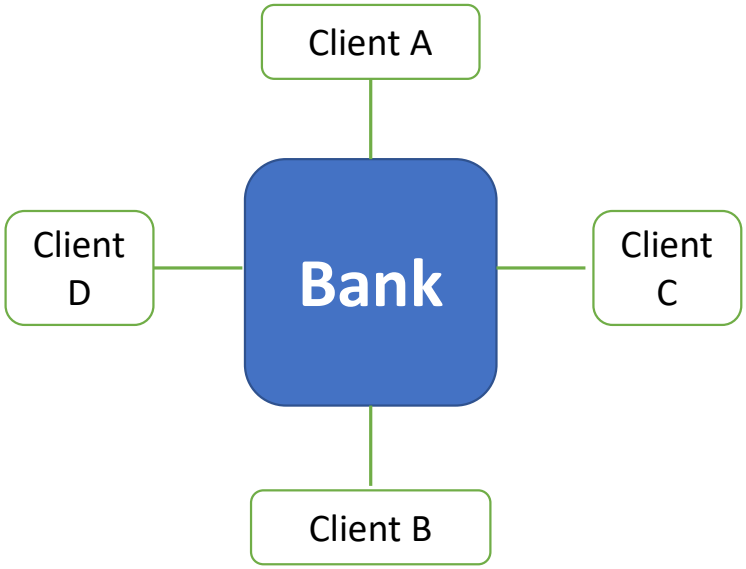
A technology or type of database

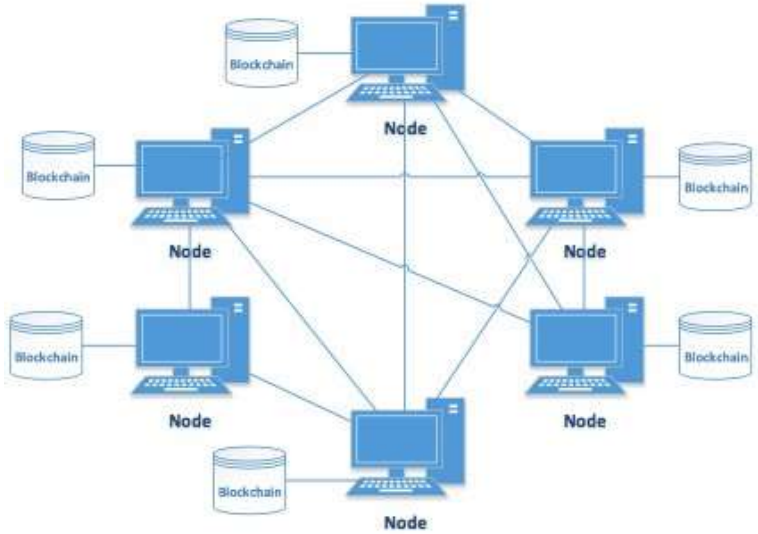
permits transactions to be gathered into blocks and recorded;

cryptographically chain blocks in chronological order; and

allows the resulting ledger to be accessed by different servers, but not by copied

Centralized vs. Distributed Ledger





- Multiple ledgers, but Bank holds the "golden record"
- Client A must reconcile her own ledger against that of Bank, and must convince Bank of the "true state" of the ledger if discrepancies arise

- One ledger. All Nodes has access to that ledger
- All Nodes agree to a consensus protocol that determines the "true state" of the ledger

Evolution of Blockchain

- 1st generation (Bitcoin): introducing a cryptocurrency, a decentralized payment system, removing intermediaries
- 2nd generation (Ethereum): introducing the smart contract, adding “conditions” to transactions
  - Less like a cryptocurrency, more like an entire digital ecosystem
  - A platform for decentralized (dApps): DeFi, web browsing, gaming, identity management, supply chain management, etc.
- 3rd generation (Ethereum 2.0, Polkadot, Cardano, Solana):
  - Scalability: increasing the number of transactions
  - Interoperability: communication between different blockchain platforms, data shared across platforms

Types of Blockchain

	PUBLIC BLOCKCHAIN	PRIVATE BLOCKCHAIN
Access	Anyone	Single organization
Authority	Decentralized	Partially decentralized
Transaction Speed	Slow	Fast
Consensus	Permissionless	Permissioned
Efficiency	Low	High
Data Handling	Read and Write access for anyone	Read and write for a single organization
Immutability	Full	Partial

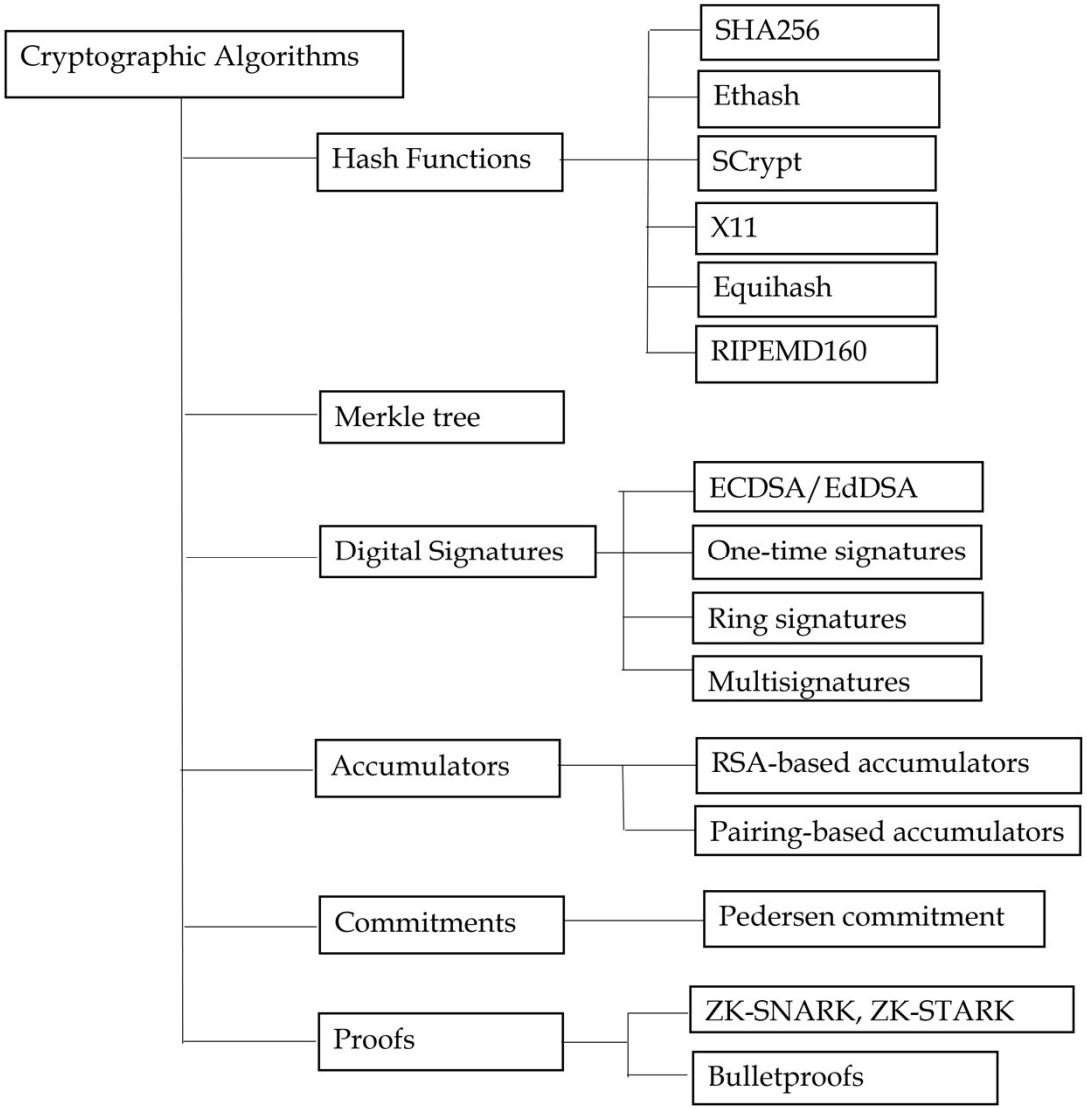
Blockchain Features

Properties of Distributed Ledger Technology

- **Distributed**: all participants have full copy of the full ledger
- **Immutable**: any validated records are irreversible and cannot be changed due to hash function
- **Ownership**: data is on the users' hand; each piece of information belong to <u>only</u> one user
- **Programable**: smart contracts enable the programmability of the blockchains
- **Time-stamped**: transaction timestamp is recorded
- **Anonymous**: the identity of participants is either pseudonymous or anonymous

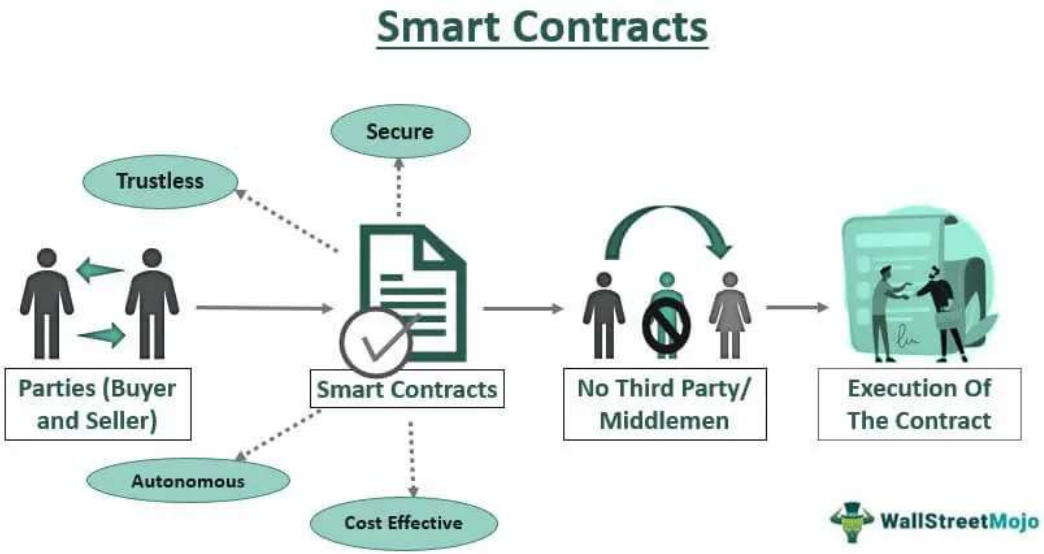
Cryptography in Blockchain Technology

- Hash function provides immutability
- Merkle tree compresses transactions into a block
- Digital signatures prove the ownership and authenticate the transactions
- Special signatures can enhance the security and privacy
- Other cryptographic algorithms provide privacy of sender, receiver and confidentiality of transactions



Smart Contracts

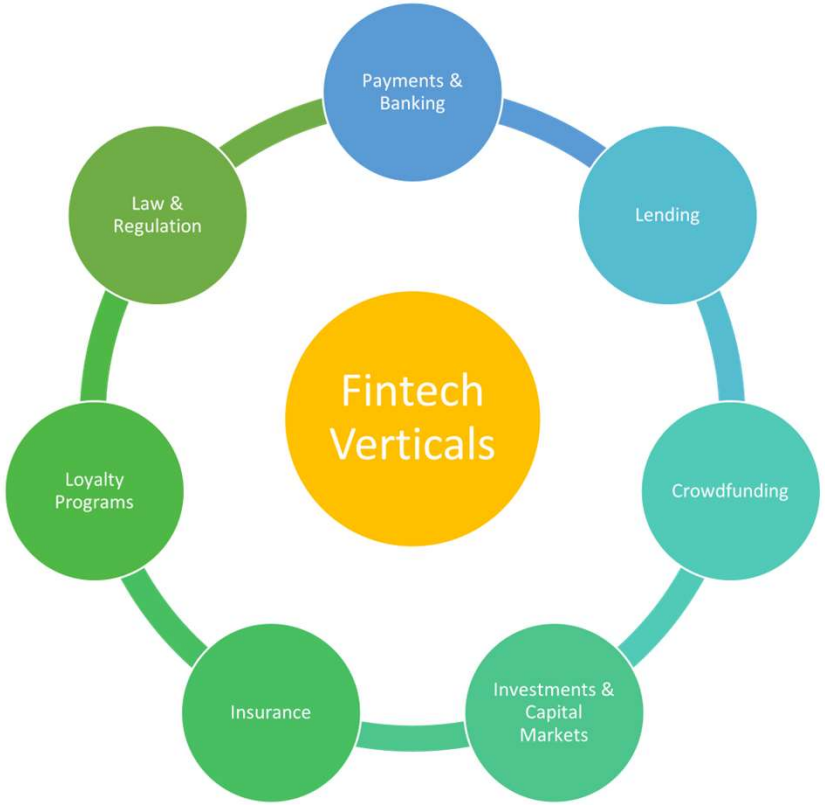
- Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met



Blockchain and Fintech

Fintech Ecosystem

- Fintech: Financial Technology
  - Enhance traditional services: using internet, mobile devices, SW or cloud services to perform or connect with financial services

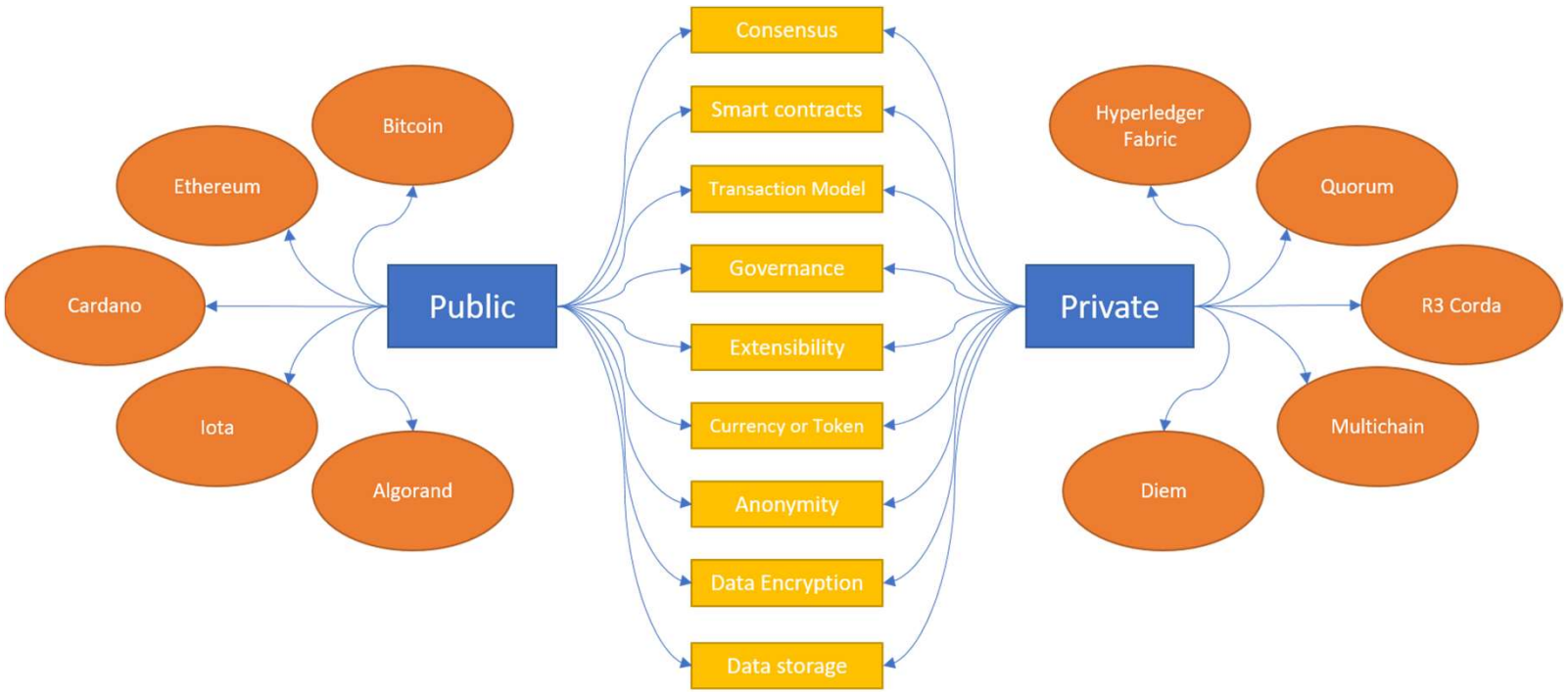


Benefits of Blockchain in Fintech

How blockchain transform Fintech?

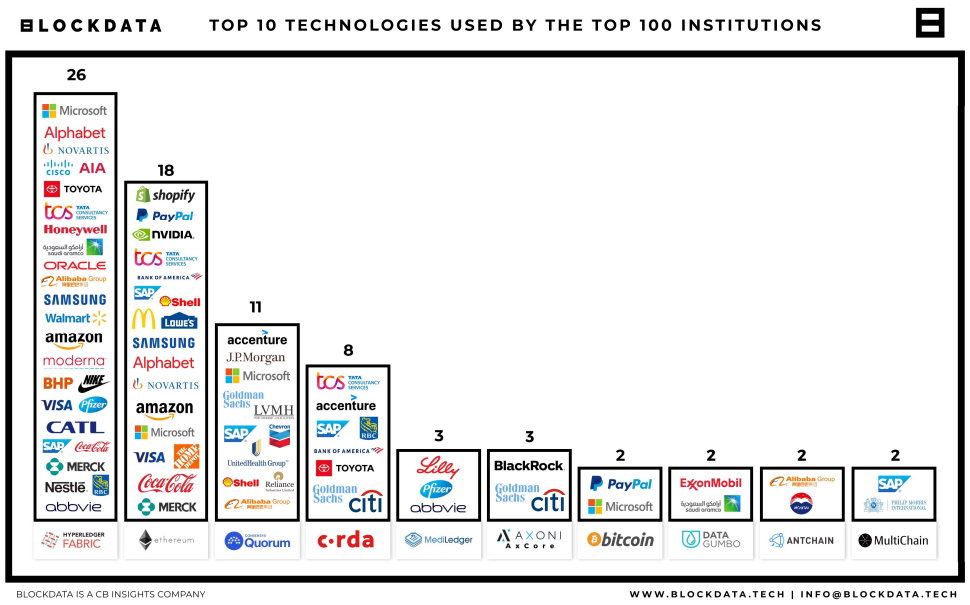
- Blockchain enhance Fintech
  - Disintermediation: Provide seamless and efficient transactions with reduction of the use of intermediaries
  - Provide better security and privacy
    - Records of transaction can not be altered
    - Easy to detect malfunction
  - Provides trust
    - Smart contracts guarantee peer integrity
    - Transparent and traceable
  - Accuracy, Speed and Cost Saving

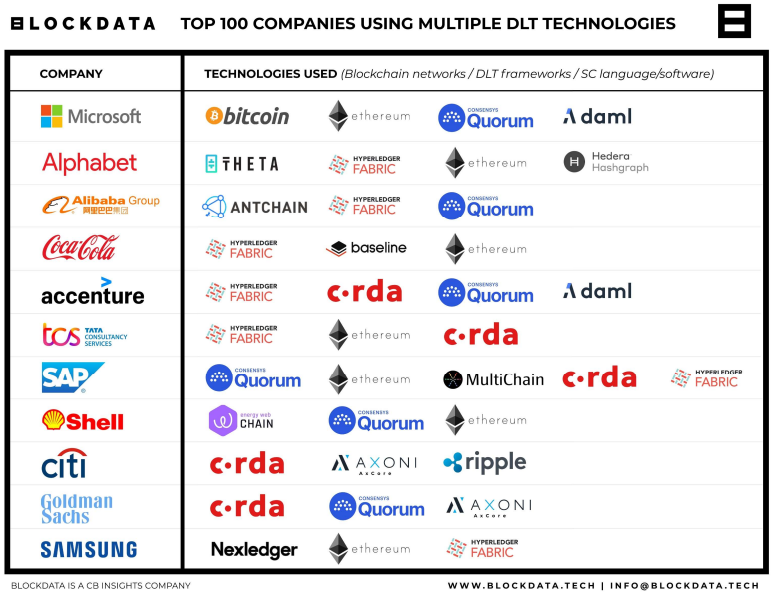
Classification of Blockchain Platforms used in Fintech



Classification of Blockchain Platforms used in Fintech

Platform	Consensus	Transaction Model	Throughput	Private Transactions	Currency/Token	Applications
Bitcoin	Proof of work	UTXO	7 TPS	Shadow Addresses and Mixing	BTC	Payments
Ethereum	Proof of work	Account	15 TPS	ZK Proofs	ETH	Dapps
Cardano	Ouroboros Proof of stake	UTXO	257 TPS	ZK proofs	ADA	Dapps
IOTA	Fast Probabilistic Consensus	UTXO	1500 TPS	CoinMixing	IOTA	IoT devices
Algorand	Pure proof of stake	Account	1000 TPS	None	ALGO	Payments
Hyperledger Fabric	CFT & BFT	Account	3000 TPS	Channels & ZK proofs	None	Enterprise
R3 Corda	Validity & Uniqueness consensus	UTXO	15-1678 TPS	Inherent support	None	Enterprise
Quorum	RAFT and IBFT	Account	900 TPS	ZK proofs	ETH	Dapps
Multichain	PBFT	UTXO	1000 TPS	Streams	Custom	Enterprise
Diem	DiemBFT	Account	3 TPS	None	DIEM	Payments





Use-cases of Blockchain-based Fintech

Taxonomy of Use Cases

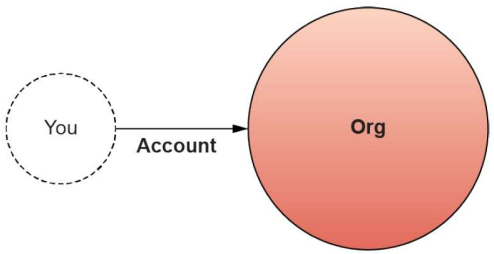
		Fintech Ecosystem Verticals					
		Payments & Digital Banking	Digital Lending & Borrowing/Insurance	Investments & Capital Markets & Trade Finance	Infrastructure and Value-add services	Marketplaces	Crowdfunding
Taxonomy of usecase	Digital Identity	✓	✓	✓	✓	✓	✓
	Cryptocurrencies	✓					
	CBDCs and Stablecoins	✓	✓	✓			
	Decentralized exchanges		✓	✓			
	Decentralized finance		✓	✓			
	Decentralized oracles				✓		
	Decentralized storage system				✓		
	Node as a service				✓		
	Online marketplaces					✓	
	Supply chain finance			✓		✓	
	Governance			✓			✓
	Crowdfunding						✓

Source: Netaturu et al., A Review of Blockchain-based Fintech Applications, Cryptography 2022

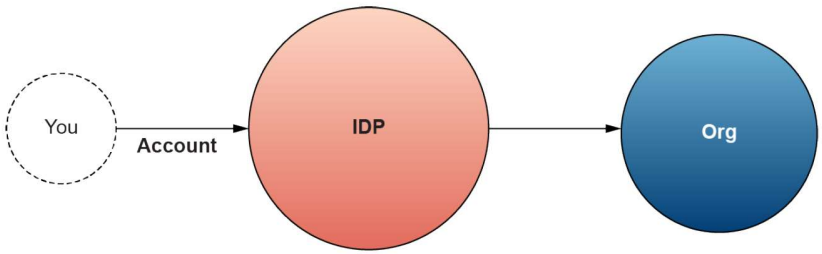
Blockchain in Digital Identity

- Centralized Identity
  - Not secure, poor user experience
- Federated identity
  - Lack of universality, being surveilled
- Self-Sovereign identity
  - Decentralized, new model of data ownership

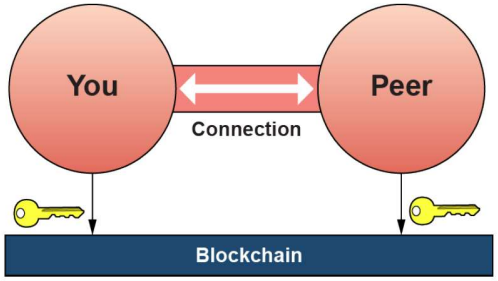
Centralized Identity



Federated Identity



Self-Sovereign Identity



Blockchain in Digital Currencies & Payments

- Four (4) classes of digital currencies
  - Cryptocurrencies: Bitcoin, Ethereum, etc
  - Stablecoins: USDT, USDC, DAI, BUSD, etc
  - Platform-based digital currencies (PBDC)
  - Central Bank Digital Currencies (CBDC)

- P2P transactions, reduce intermediaries
  - Faster, cheaper
  - Transparency & tractability
  - Better security and privacy

Blockchain in Asset Management

- Represents all the links involved in manufacturing (or creating of digital assets), deployment, and disposal

- Issues: lack of transparency and costly
  - No reliable way among parties to verify and validate the true value of the products and services

- Benefits through blockchain
  - Prove ownership, provenance
  - Enhance record transparency, completeness & accuracy
  - Alleviation of reconciliation need
  - Enhance security and privacy
  - Cost saving
- Some existing systems
  - IBM blockchain for enterprise asset management: applied to food industry, cargo tracking, truck tracking
  - Alibaba: engaged with PwC to build a “food safety framework
  - Everledger: tracking high value assets like diamonds

Supply Chain News

World's Largest Mining Company to Use Blockchain for Supply Chain Management

The world's largest mining firm by market value intends to begin using the ethereum blockchain to improve its supply chain processes.

October 2, 2016 · By Pete Rizzo

BHP Billiton to use Blockchain

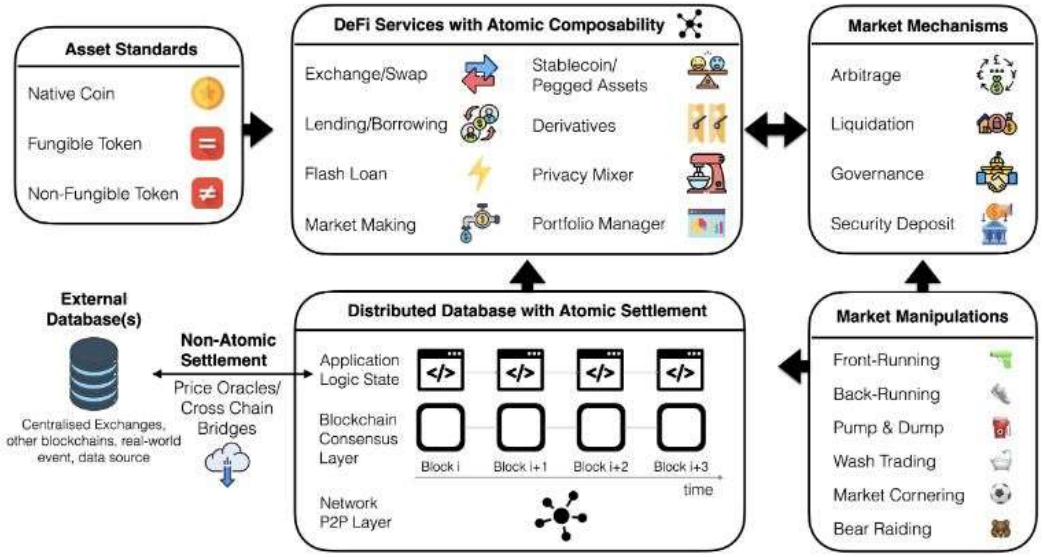
BHP Billiton revealed at the second annual Global Blockchain Summit that it will use blockchain to record movements of wellbore rock and fluid samples and better secure the real-time data that is generated during delivery.

According to BHP geophysicist R Tyler Smith, the new system will enable benefits for its internal efficiency while allowing it to work more effectively with partners.

Smith explained that BHP relies on vendors at nearly every stage in the mining

Blockchain in Investing

- Decentralized Exchanges (DEX):
  - Three main types: Automated market makers (AMM), Order book DEXs, DEX aggregators
- Decentralized Finance (DeFi)
  - Asset exchanges, loans, leveraged trading, decentralized governance, stablecoins, etc



Bloomberg

Sign In | Subscribe

Live Now | Markets | Industries | Technology | Politics | Wealth | Pursuits | Opinion | Businessweek | Equality | Green | CityLab | Crypto | More

Technology

Australia Stock Exchange's Blockchain Project Hits Another Snag

By David Earl Jolly
August 4, 2022 at 2:52 PM EDT

Listen to this article
1:37

Share this article

The Australian Stock Exchange's plan to replace its main trading applications with a blockchain-based system has hit another snag, and the market operator's new CEO is bringing in consulting giant Accenture to study the project.

- Must lower cost
- Quicker speed of trading and settlement
- More accurate record-keeping
- Transparency of ownership
- Autonomous "smart contracts" for debt and contingent securities

More use-cases

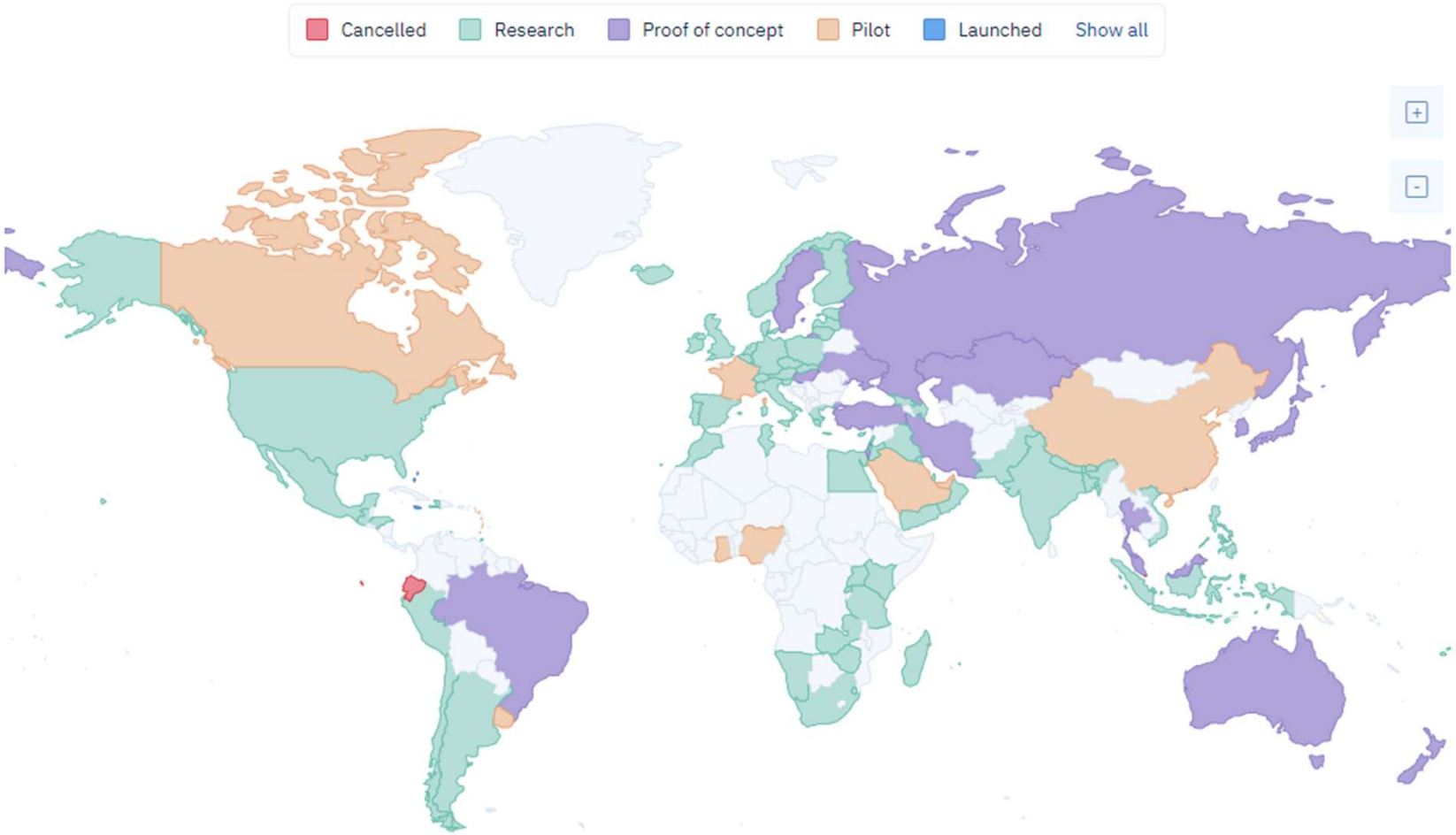
- Infrastructure/Value-Add Services
  - Decentralized storage like Filecoin, Storj, etc
  - Node-as a-Service
- Online Marketplaces and Supply Chains
  - Introduce decentralization and privacy to traditional marketplace
  - Supply Chain Finance (SCF):
    - Eliminate information asymmetry
    - Enable traceable and tamper-proof systems to detect irregularities and anti-counterfeit challenges
    - Typical companies: Contour (R3 Corda), Skuchain (HLF), komgo (Quorum), etc
- Crowdfunding
- Corporate Governance
  - DAO, ICO, etc

Blockchain and CBDC

Central Bank Digital Currency (CBDC)

- What is Central Bank Digital Currency (CBDC)
  - Digital form of cash
  - Issued and controlled by Central Banks
  - Must provide properties like privacy, universal access, resilience, and security
  - Can be online only or both online and offline

- Uses cases of CBDCs
  - Wholesale: used to facilitate interbank settlement
  - Retail: used for payments between individuals and businesses or other individuals



Source: CBDC Tracker (updated September 2022)

Blockchain Technology for CBDC

Why?

- System trust
- Programmability
- Data availability
- Innovation

Why not?

- Decentralized architecture and controls

PoC CBDC system based on Blockchain

- Project Jasper-Ubin
  - BoC and MAS developed a CBDC project that offer cross-border payment solutions
  - Clearing and settlement of payments and securities from two different blockchain platforms
  - Developed on Ethereum, Corda
- Project Aber
  - Between Arabian Monetary Authority and Central Bank of the UAE
  - Developed on Hyperledger Fabric (HLF), a permissioned blockchain
- Project Inthanon-LionRock
  - Initiated by Bank of Thailand and Hong Kong Monetary Authority
  - Project extended with People's Bank of China and CB of UAE: mCBDC Project
  - Ethereum, Corda

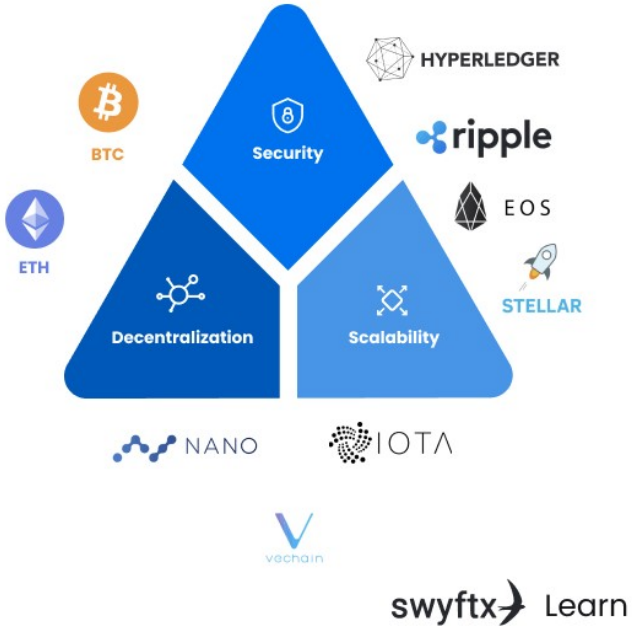
PoC CBDC system based on Blockchain

- Project Hamilton
  - Between MIT and FED Bank of Boston
  - Develop an open-source blockchain-based CBDC, called OpenCBDC
- SWIFT: global CBDC
  - Do experiments involving the central banks of France and Germany, HSBC, UBS, Standard Chartered
  - Transactions from different blockchain networks, using both CBDCs and fiat currencies

Challenges for using Blockchain in Fintech

Challenges of Blockchain-based Fintech

- Scalability
  - Bitcoin is able to process ~7Txs/s vs tens thousands Txs/s of VISA
- Security
  - Blockchain code is not mature, new technology can face new cyber threats
- Privacy:
  - Parties can be tracked, transaction info/smart contracts could be disclosed, etc
- Interoperability
  - issues of communication between different blockchain platforms
- Law and Regulation
  - Lack of laws and regulation for this new technology



Thank you!

Q&A