Blockchain Concensus with Proof of Stake

Sean Au
talkcrypto.org

Agenda

- What is Proof of Stake?
- How it works?
- It's importance to Ethereum

What is a Consensus Algorithm?

- In a distributed, trustless computing network...
- ... allows a collection of machines...
- ...to reach an agreement of facts.

What is its purpose?

- Allow the secure updating of a state according specific state rules

Concensus Algorithms

- Proof of Work
- Proof of Stake
- Proof of Activity
- Proof of Capacity

Consensus Mechanisms

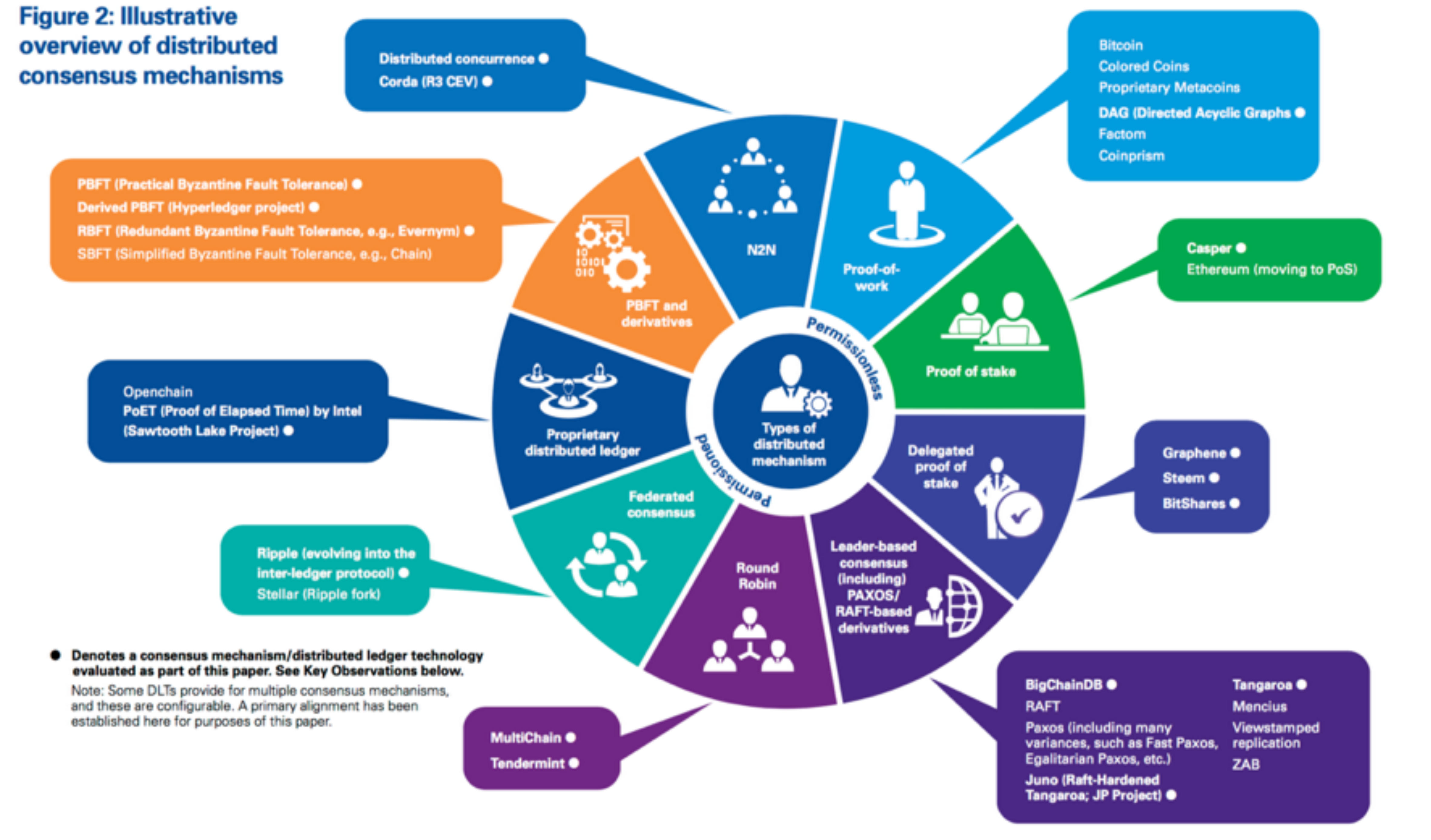


Figure 2: Illustrative overview of distributed consensus mechanisms

Distributed concurrence ●
Corda (R3 CEV) ●

Bitcoin
Colored Coins
Proprietary Metacoins
DAG (Directed Acyclic Graphs ●
Factom
Coinprism

PBFT (Practical Byzantine Fault Tolerance) ●
Derived PBFT (Hyperledger project) ●
RBFT (Redundant Byzantine Fault Tolerance, e.g., Evernym) ●
SBFT (Simplified Byzantine Fault Tolerance, e.g., Chain)

Casper ●
Ethereum (moving to PoS)

Openchain
PoET (Proof of Elapsed Time) by Intel (Sawtooth Lake Project) ●

Graphene ●
Steem ●
BitShares ●

Ripple (evolving into the inter-ledger protocol) ●
Stellar (Ripple fork)

MultiChain ●
Tendermint ●

BigChainDB ●
RAFT
Paxos (including many variances, such as Fast Paxos, Egalitarian Paxos, etc.)
Juno (Raft-Hardened Tangaroa; JP Project) ●

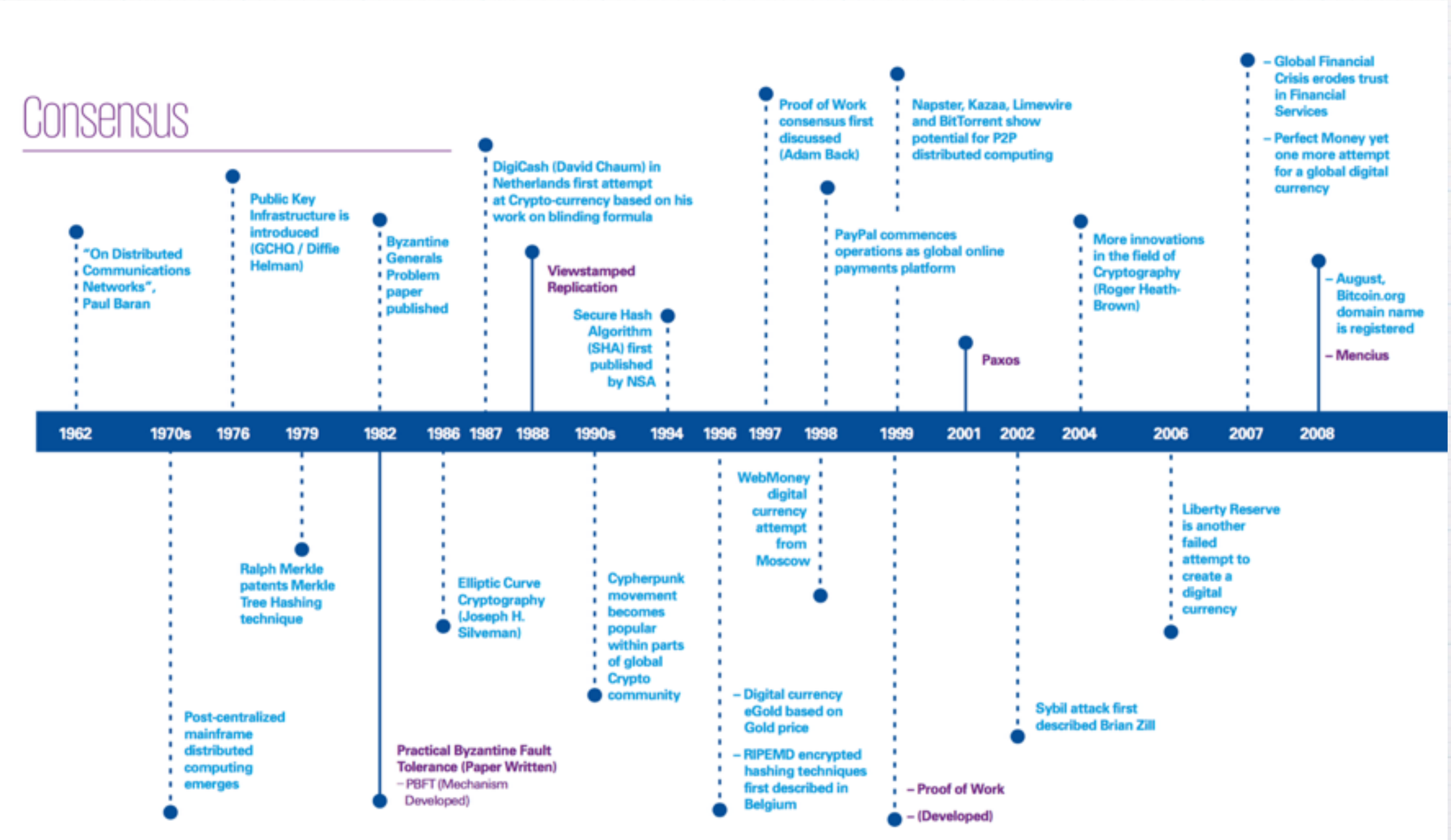
Tangaroa ●
Mencius
Viewstamped replication
ZAB

● **Denotes a consensus mechanism/distributed ledger technology evaluated as part of this paper. See Key Observations below.**

Note: Some DLTs provide for multiple consensus mechanisms, and these are configurable. A primary alignment has been established here for purposes of this paper.

- https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf

Consensus



Consensus

1962 – "On Distributed Communications Networks", Paul Baran

1970s – Post-centralized mainframe distributed computing emerges

1976 – Public Key Infrastructure is introduced (GCHQ / Diffie Helman)

1979 – Ralph Merkle patents Merkle Tree Hashing technique

1982 – Byzantine Generals Problem paper published

1982 – Practical Byzantine Fault Tolerance (Paper Written) – PBFT (Mechanism Developed)

1986 – Elliptic Curve Cryptography (Joseph H. Silveman)

1987 – DigiCash (David Chaum) in Netherlands first attempt at Crypto-currency based on his work on blinding formula

1988 – Viewstamped Replication

1990s – Cypherpunk movement becomes popular within parts of global Crypto community

1994 – Secure Hash Algorithm (SHA) first published by NSA

1996 – Digital currency eGold based on Gold price – RIPEMD encrypted hashing techniques first described in Belgium

1997 – Proof of Work consensus first discussed (Adam Back)

1998 – PayPal commences operations as global online payments platform

1998 – WebMoney digital currency attempt from Moscow

1999 – Napster, Kazaa, Limewire and BitTorrent show potential for P2P distributed computing

1999 – Proof of Work – (Developed)

2001 – Paxos

2002 – Sybil attack first described Brian Zill

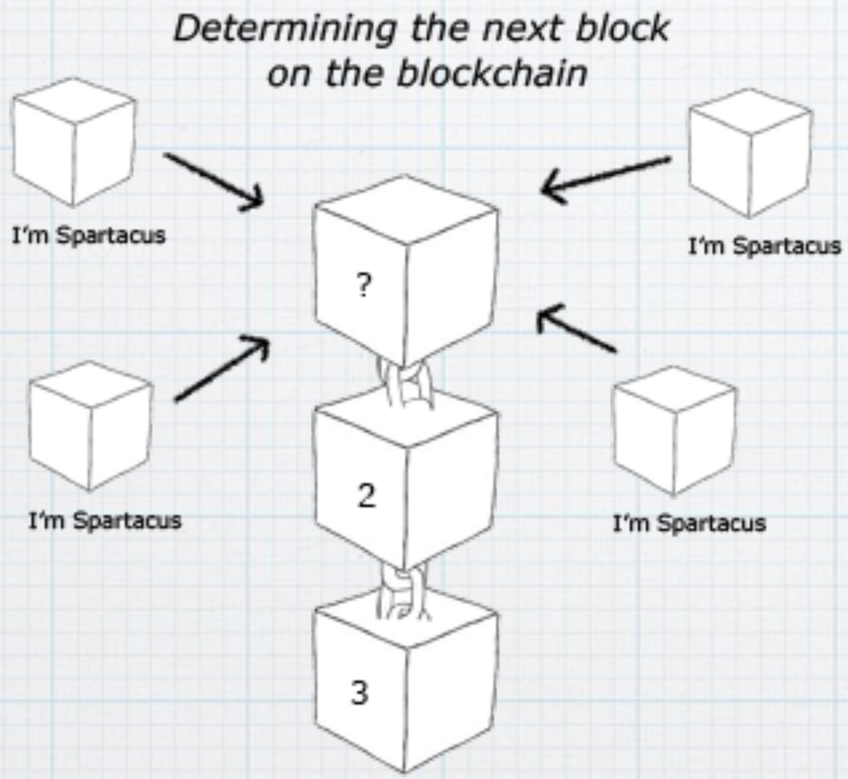
2004 – More innovations in the field of Cryptography (Roger Heath-Brown)

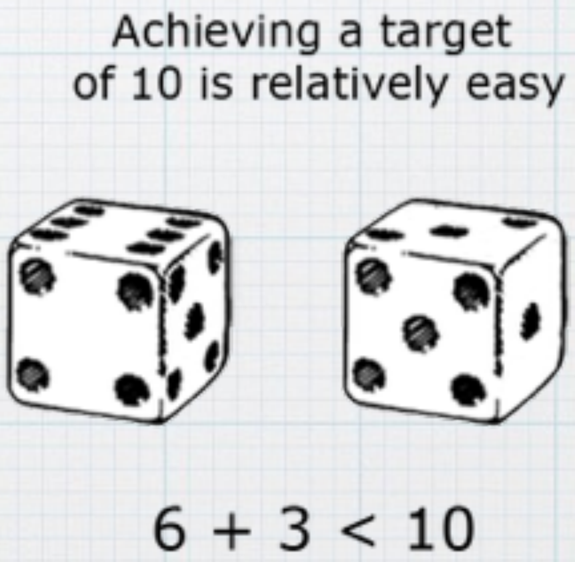
2006 – Liberty Reserve is another failed attempt to create a digital currency

2007 – Global Financial Crisis erodes trust in Financial Services – Perfect Money yet one more attempt for a global digital currency

2008 – August, Bitcoin.org domain name is registered – Mencius

Proof of Work (PoW)





http://www.talkcrypto.org/blog/2016/07/27/going-pow-on-the-blockchain/

Proof of Stake

- The probability to create a block and receive a reward is proportional to a user's stake in the system.
- A stakeholder who has p fraction of the coins in circulation creates a new block with p probability

Example

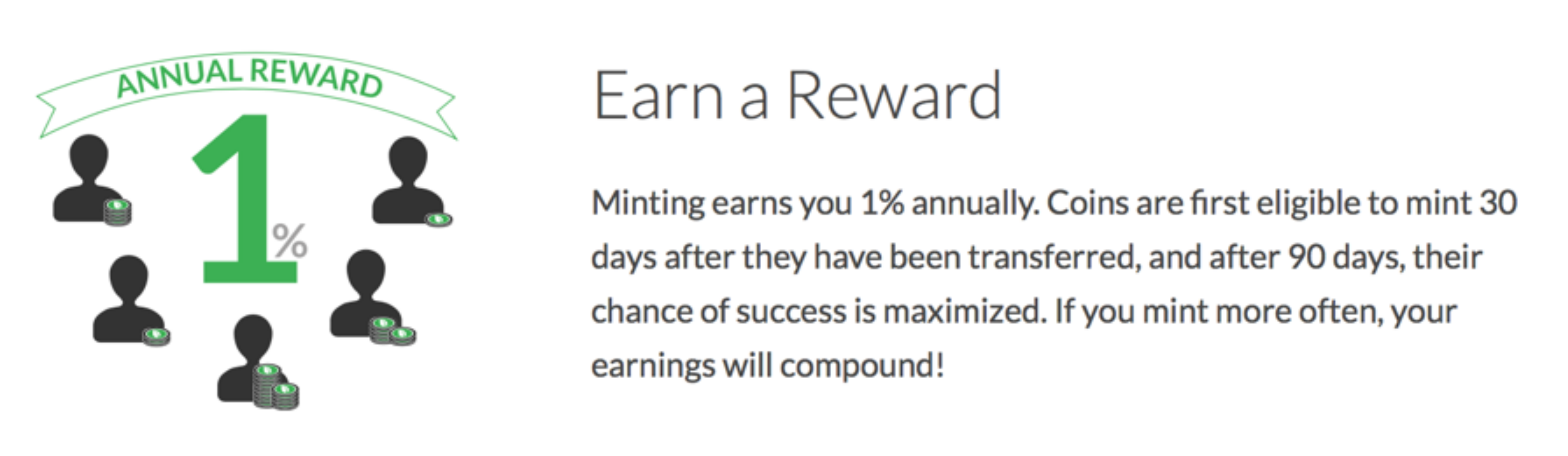
- John = 3 blue tokens
- Mary = 5 red tokens
- Sally = 8 green tokens

Don't the rich get richer?

- Coin age
  - stake x age
- Reset of coin age
  - min & min period

Peercoin

- https://peercoin.net



Earn a Reward

Minting earns you 1% annually. Coins are first eligible to mint 30 days after they have been transferred, and after 90 days, their chance of success is maximized. If you mint more often, your earnings will compound!

- Sign the coins

Benefits

- No large consumption of electricity
- Reduced incentives for attack.
- Reduced centralisation risk?
- Could provide faster block generation times

Implementation

- Peercoin or PPCoin (peercoin.org)
- Nxt (nxt.org)
- BlackCoin (blackcoin.co)
- Novacoin (novacoin.org)

Ethereum

- Does any one mine ETH?
- Frontier -> Homestead -> Metropolis -> Serenity
- Articles >1 yr ago. Casper

Ethereum

- https://souptacular.gitbooks.io/ethereum-tutorials-and-tips-by-hudson/content/proof-of-stake_resources.html

Proof of Stake

- https://www.youtube.com/watch?v=bSdwqa3YI0Q

References

- http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf
- https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf
- https://blog.ethereum.org/2015/12/28/understanding-serenity-part-2-casper/
- http://ethereum.stackexchange.com/questions/9/why-does-ethereum-plan-to-move-to-proof-of-stake

Summary

- PoS is a consensus algorithm
- Users put their stake in the system
- Ethereum's move to Casper in 2017