Why *BlockChain*: The disruptive disintermediation of infrastructure with *blockchain* technology.

Samuel M. Smith Ph.D.
Founder
ProSapien
sam@prosapien.com

What is BlockChain Technology?

Euphemism for a host of related technologies and concepts of which blockchains are not the most important

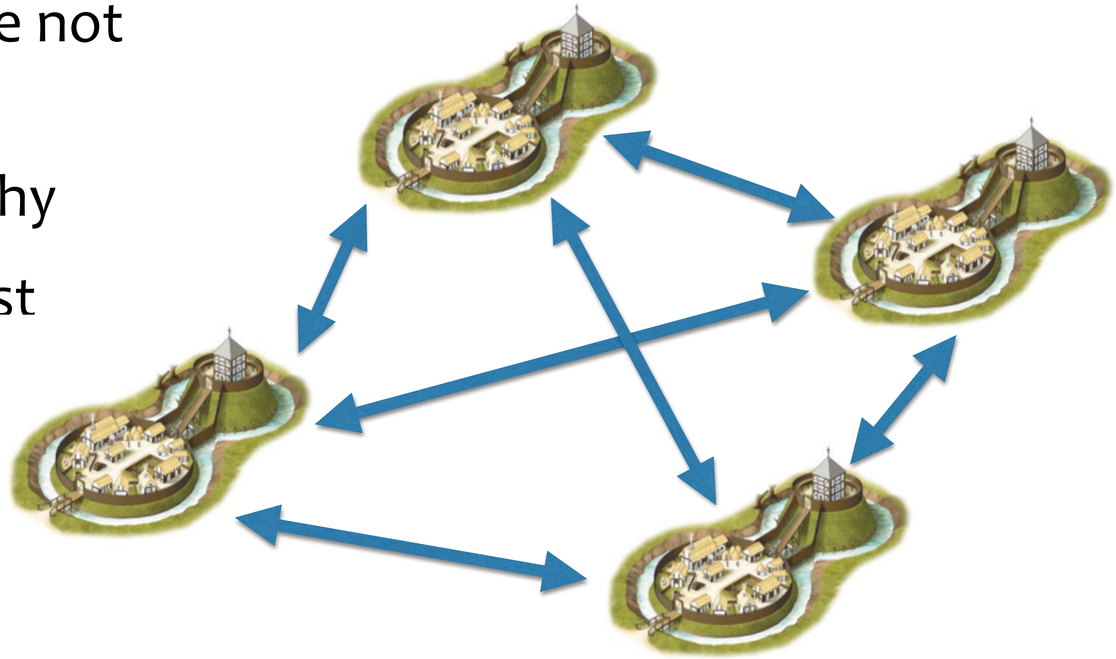
Diffuse Trust

- Cellular distributed topology.

  "Think clandestine spy ring or resistance organization"

- Defeating each node (cell, element) requires an independent exploit.
  - No single point of failure. *"Universal root privileges"*
  - No common mode failures. *"Exploit to attain root privileges"*
- As long as the majority or super majority of nodes are not exploited the system is trustworthy.
- Cooperation between peers vs. authoritarian hierarchy
- Distributed consensus is a way to achieve diffuse trust

VS



Why Distributed Consensus

- Enables diffuse trust systems using de-centralized computing infrastructure
- Allows secure infrastructure outside a firewall by distributing the attack surface.
- Enables the replacement of strongly controlled computing infrastructure with weakly controlled computing infrastructure that may be more secure.
- Enables computation in the "*fog*" vs computation in the "*cloud*".
- Enables new disruptive business models

Distributed Consensus Applications

- Settlement, and other FinTech
- Exchanges
- IoT
- Neighborhood computing
- Open Platforms
- Smart Contracts
- Distributed AI

Platform Business Models

A platform is a business based on enabling value-creating interactions between external producers and consumers.

A platform provides an open, participative infrastructure and sets governance conditions for these interactions.

A platform consummates matches among users that facilitate the exchange of goods, services, or social currency, thereby enabling value creation or co-creation for all participants.

A platform is the antithesis of a pipeline.

(See Platform Revolution 2016, Platform Scale 2015)

Platforms vs Pipelines

A pipeline is a business that directly creates and moves value from …

producers at one end to consumers at the other end.

Platforms eat pipelines because platforms unlock new sources of value creation and supply

not-even-mine *replaces* *just-in-time*

Primary activity shifts from …

internal mechanisms of control of the value chain

to …

external orchestration/coordination of interactions between third parties

Platform Network Effects

Supply economies of scale (production efficiency)

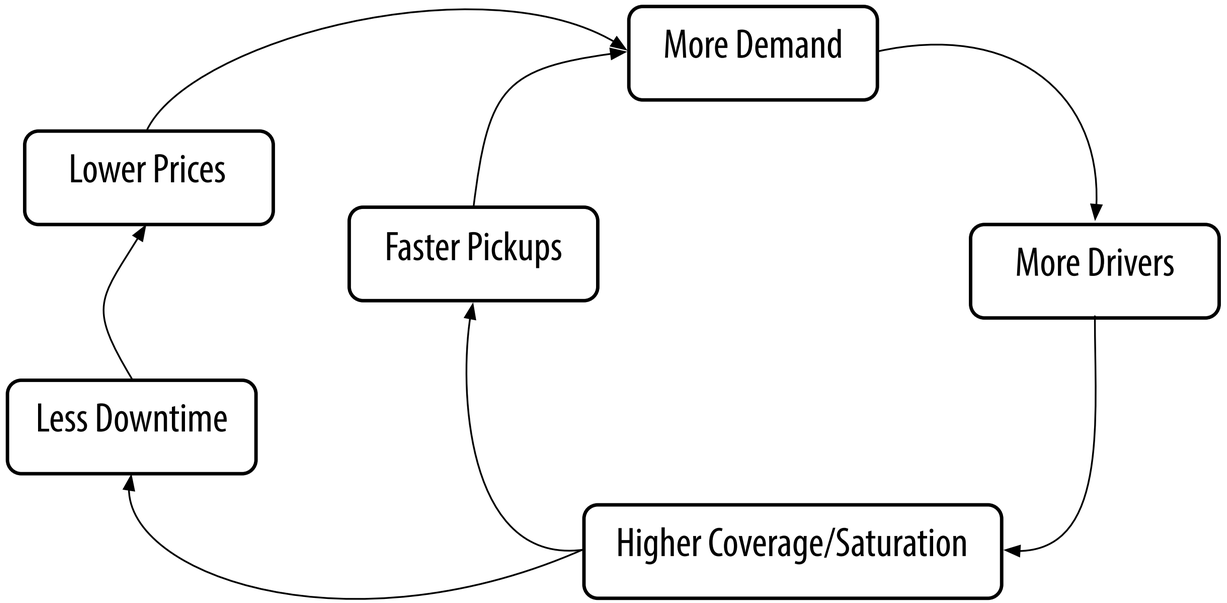
replaced with

Demand economies of scale (network effect multipliers of value)

Two-sided network effects

Core Interaction = *Participants + Value unit + Filter*

Platform = *pull + match + facilitate*



Platform Manifesto

External eco-system is the new warehouse and supply chain
Network effect is the new driver for scale
Data is the new dollar
Community management is the new human resource management
Liquidity management is the new inventory control
Curation and reputation are the new quality control
User journeys are the new sales funnels
Distribution is the new destination
Behavior design is the new loyalty program
Data science is the new business process optimization
Social feedback is the new sales commission
Algorithms are the new decision-makers
Real-time customization is the new market research
Plug-n-play (APIs) is the new business development
Invisible hand is the new iron fist

Enablement

Platforms disintermediate pipelines

Distributed network computation enables platforms

Distributed consensus enables trustworthy platforms

Governance matters

Super-efficient re-intermediation with distributed AI platforms

Disintermediation Theory

Selectorate: Those in power to make decisions for others as intermediaries/agents.

Nominal, influential, essential.

How distributed/centralized is the agency? (democratic——despotic)

Distribution of agency increases the ratio of selectorate to total population

Typically better outcomes arise overall when agency is more distributed

Increased agency results in increased autonomy (happiness) and meritocracy (performance)

The mechanism for distributing agency (increasing the selectorate) is disintermediation.

To change outcomes, don't ask those in power to be nicer, fairer, or more responsive, just disintermediate them.

Seek disintermediation, not justice.

Disintermediation Opportunities

Whenever producers and consumers of value interact through intermediaries.

Example:

Social media on Facebook/Google is intermediated by Facebook/Google.

Facebook/Google is the sole intermediary.

Facebook/Google owns all content and controls all interactions in order to extract value.

What if users could interact without the value tax of Facebook/Google?

Radical Disruptive Disintermediation

Make the governance of the interaction more distributed.

Allow users (producers and consumers) to interact without despotic control.

Allow user ownership of their content and control of their interactions.

Enable users to extract more value from their content and interactions.

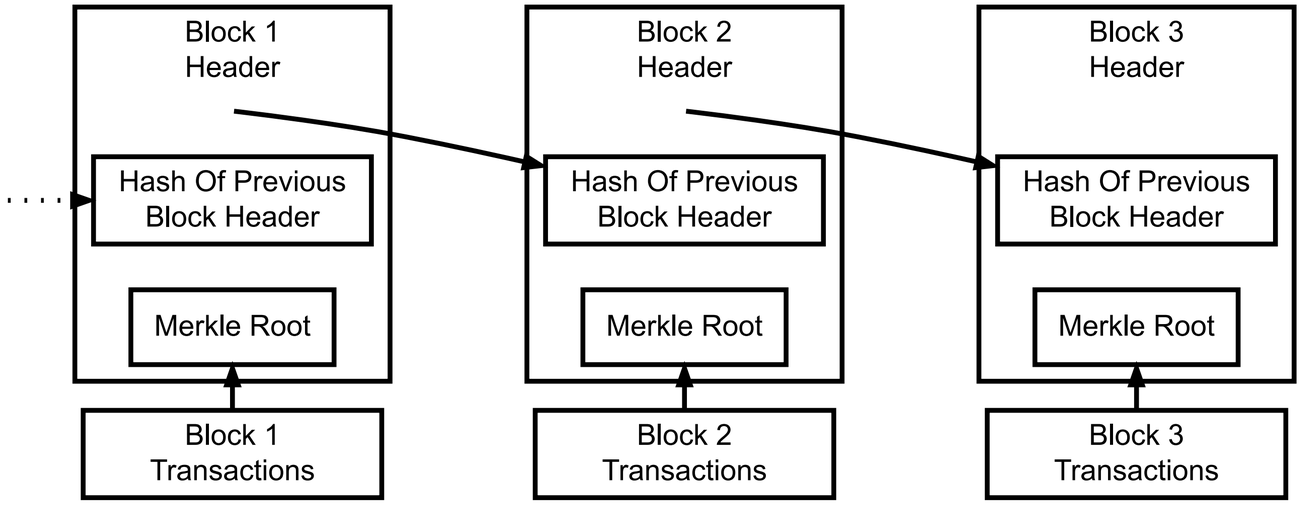
Closed pipelines/platforms are opportune for disruptive disintermediation via blockchain technology.

Distributed Consensus Types

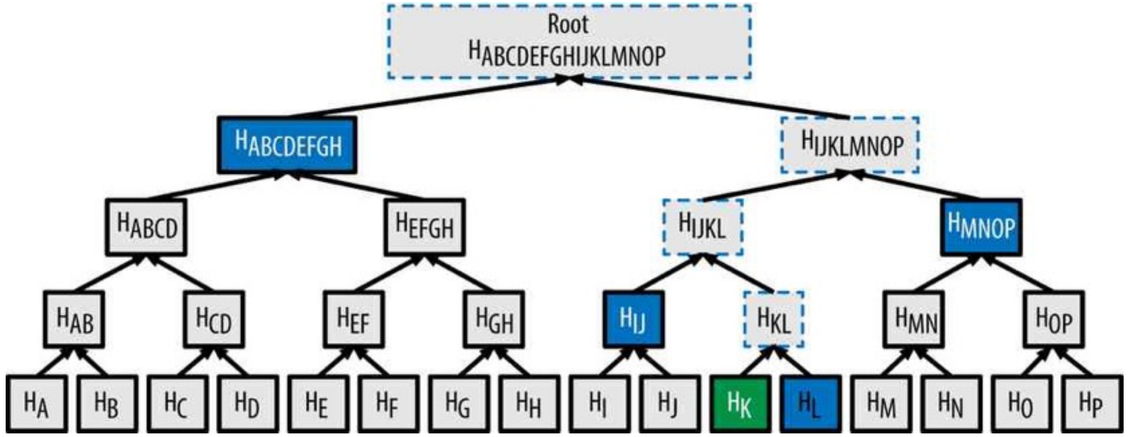
- Proof of Work: Simple, highly inefficient, high latency, low throughput
- Proof of Stake: More complex, more efficient, lower latency, higher throughput (Asymmetric Proof of Work)
- Byzantine Agreement: Most complex, most efficient, lowest latency, highest throughput. (Byzantine Fault Tolerant)
- Hybrid: Side chains, anchoring,

BLOCKCHAIN CRYPTOCURRENCY

- BitCoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf
- Solved in a logically simple but computationally inefficient way the double-spend problem on a distributed ledger with uncensored hosts
- Proof of Work: Do the work up front. Fastest worker (miner) wins. Solve cryptographic hash proof.
- Validation: All the workers (miners) validate. Majority rules.



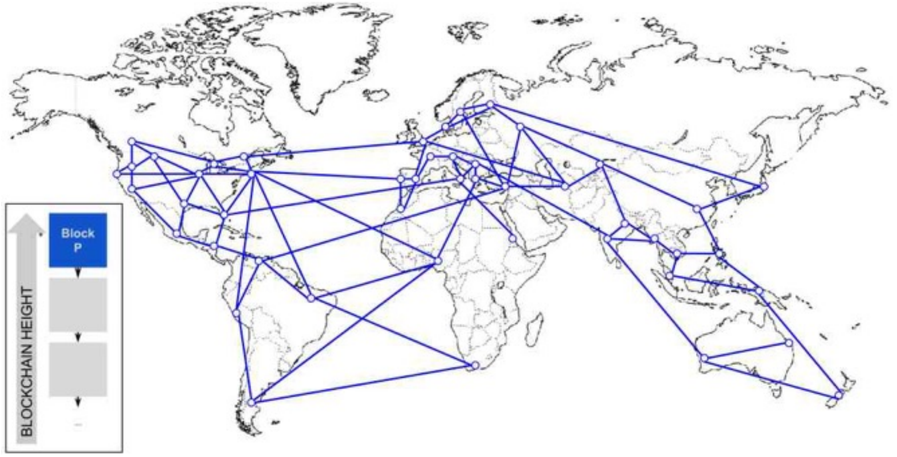
Simplified Bitcoin Block Chain

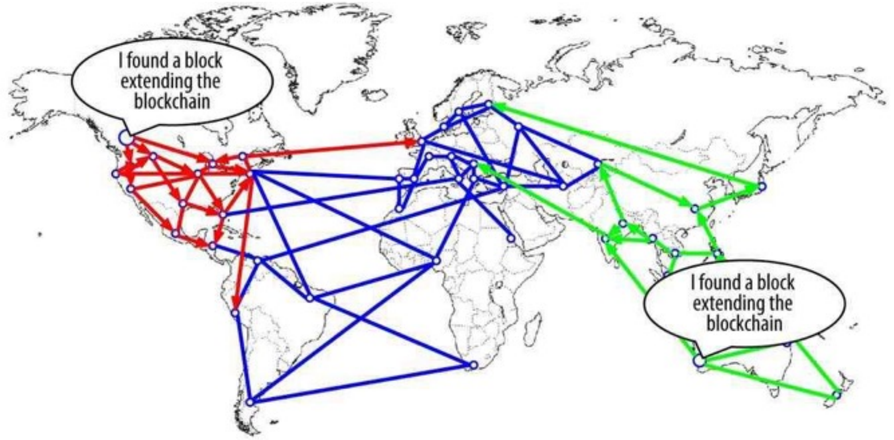


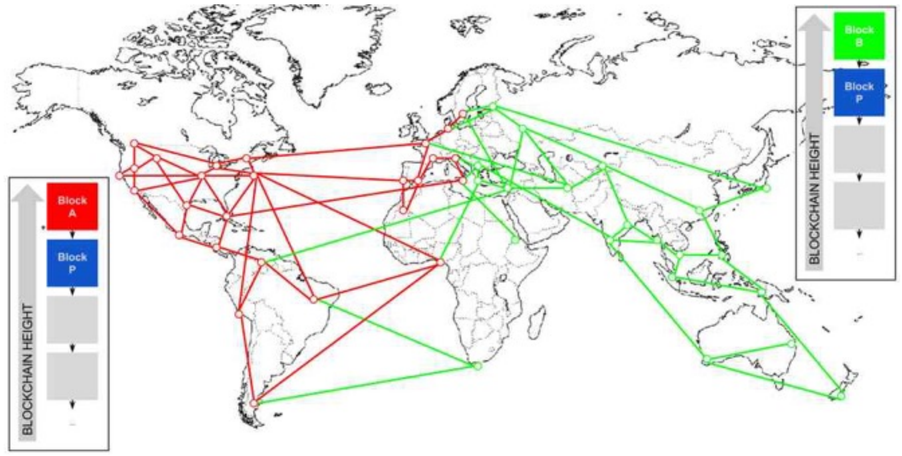
Proof of Work

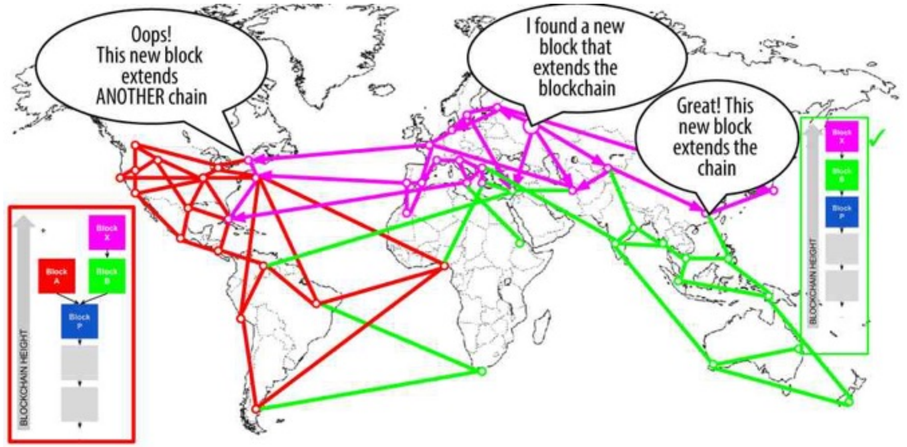
- Every new block requires proof of work.
- To change a block down in the chain requires reworking all the blocks above it.
- Deep enough blocks become exponentially difficult to change.
- In order to double spend, one must control a majority of the compute power to create a forked chain and then collude with spenders to reverse and then respond prior spends.
- Transactions made by other spenders cannot be double spent.

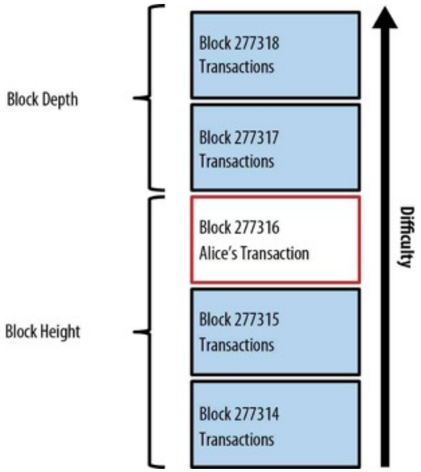
- Multi Billions of currency outside of any firewall. Safe from attack











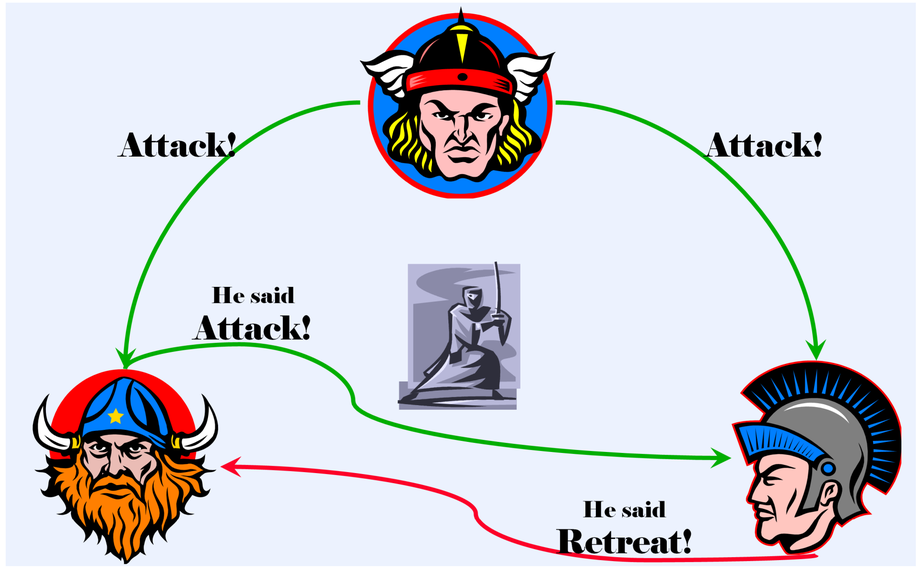
Byzantine Generals

- Analogy to war in the Byzantine era where generals were prone to duplicitous acts
- The Byzantine Generals Problem:

  http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf

  Separated generals agree to attack a city. If they unite they win. If not the attacker(s) lose.

  The communication of intent to attack and confirmation of intent to attack is subject to delay and error.



- Byzantine agreement:

  A valid consensus is guaranteed despite a fraction of the participants behaving in a malicious and/or erroneous manner.

- Consensus despite “Byzantine” faults:

  Dropped, erroneous, or malicious Packets. Partitioning. Sybil attacks.

  A consensus algorithm that achieves agreement despite the presence of Byzantine faults is called Byzantine fault tolerant (BFT).

BA Enables High Performance, Application Specific, Distributed Consensus Which Can Manage

- Transactions
- Settlement
- Smart Contracts
- Databases, DHTs, Open Storage
- Identity
- Reputation

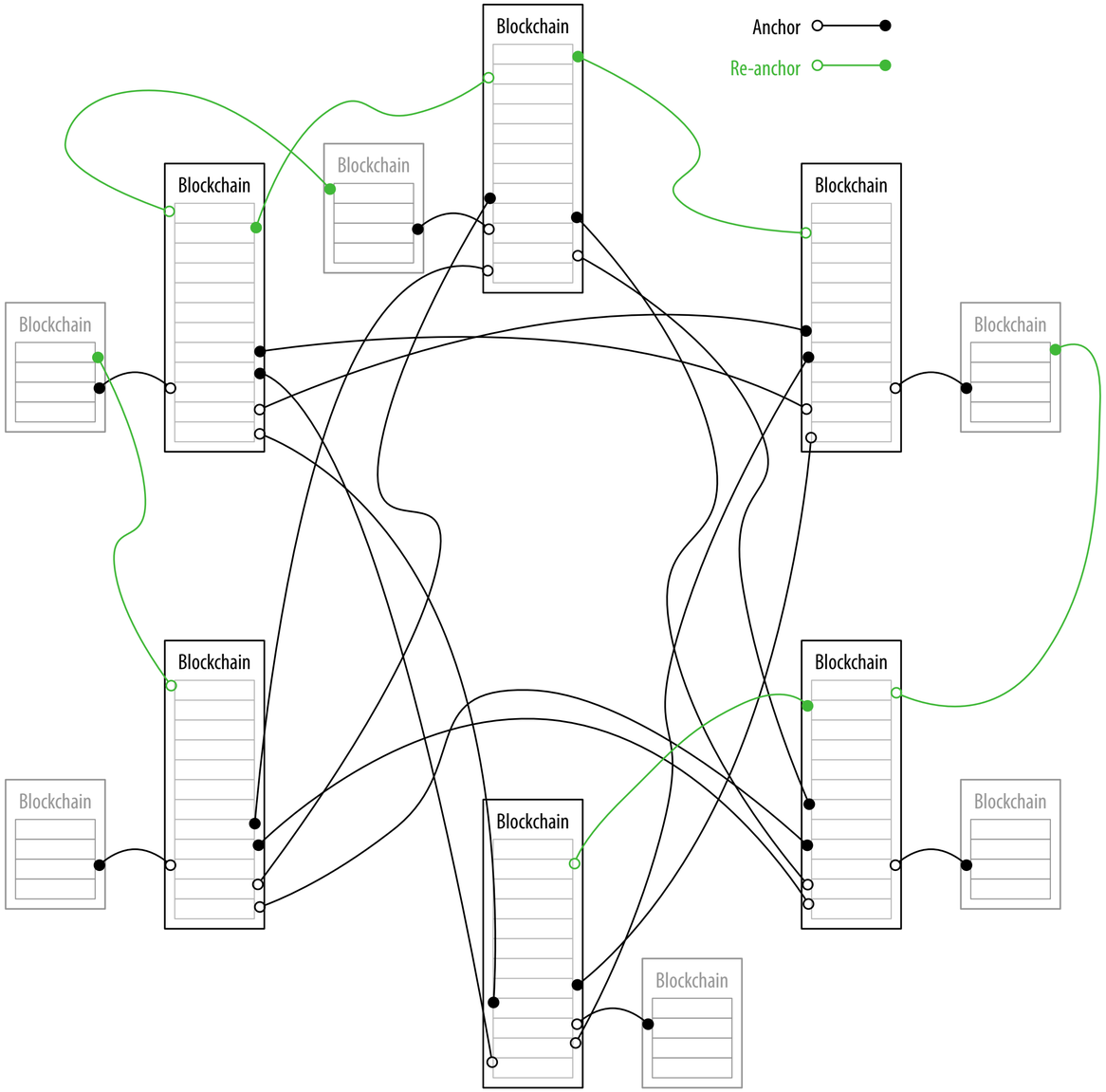
Permissioned Distributed Consensus
AKA *XBFT* or Byzantine Agreement (BA)

- Permissioned Distributed Ledgers Swanson 2105

  http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf

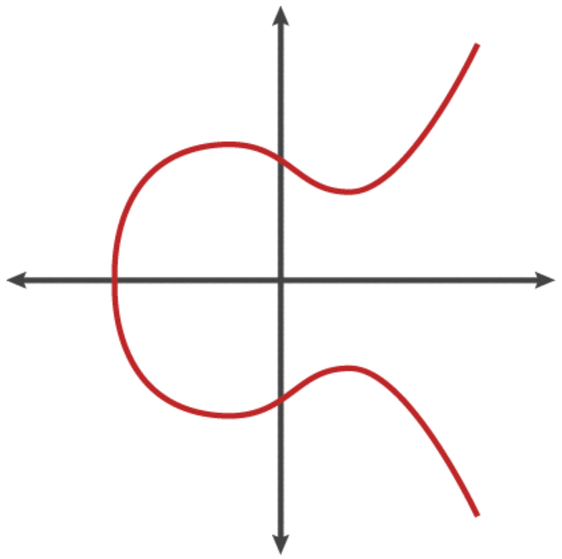
- Permissioned governance to address Sybil attack. Censorship.

Chainmail or Mesh Anchoring

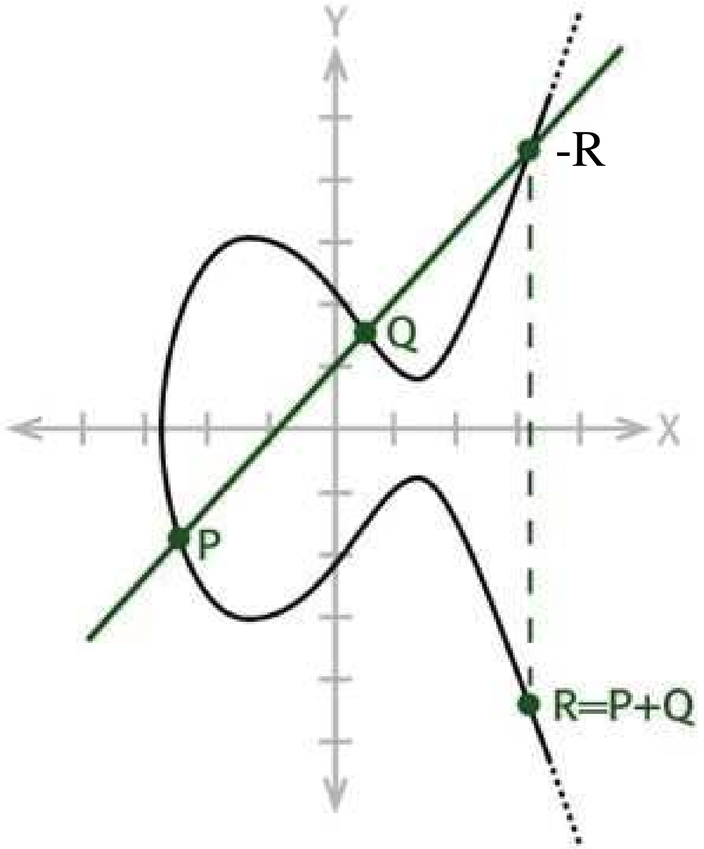


Modern Crypto: Elliptic Curves

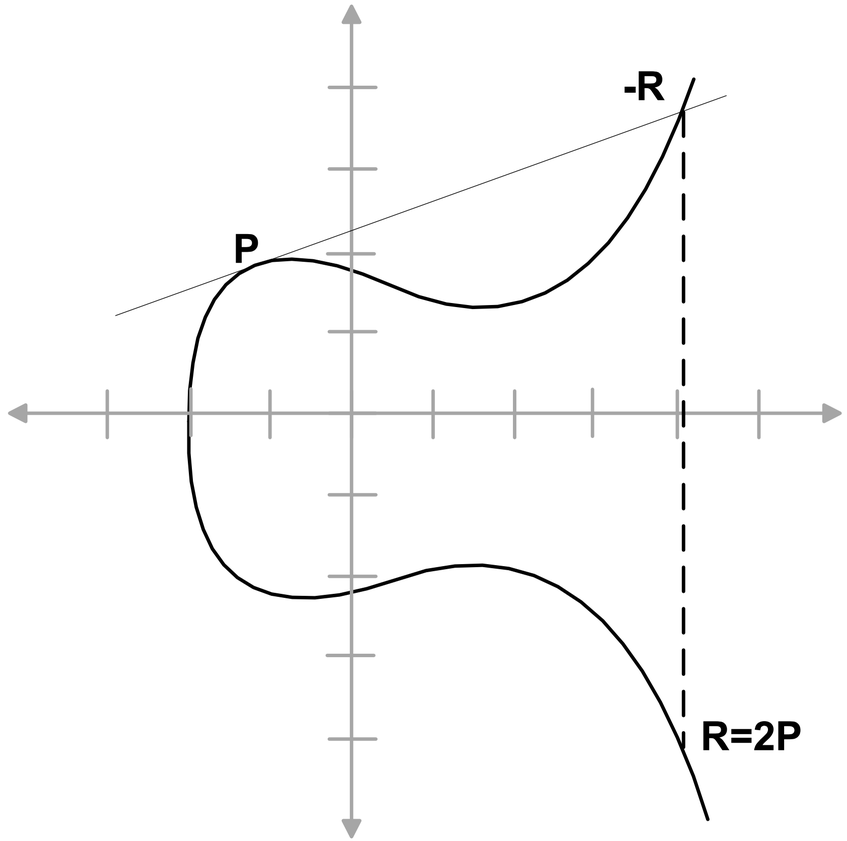
$y^2 = x^3 + ax + b \mod p$



$R = P + Q$



$R = P + P = 2P$



Modern Crypto: ECC Diffie-Hellman Key Exchange

Given elliptic curve polynomial coefficients *a*, *b*, mod prime *p* and, Generator point *G* on curve.

(*Public, private*) key pair *(K, k)* where *K =k*G*,
k is random number,
* means ECC scalar multiplication by adding *G*, *k* times
scalar multiplication is commutative
K is another point on the curve

Alice picks private key *a*, random number, and generates public key *A*, point on curve. A = a*G

Bob pick private key *b*, random number, and generates public key *B*, point on curve. B = b*G

Alice and Bob exchange public keys *A* and *B.*

Alice generates shared secret key *S*, point on curve, from Alice's private key *a* and Bob's public key *B.*

S = a * B = a * b * G

Bob generates shared secret key *S*, point on curve, from Bob's private key *b* and Alice's public key *A.*

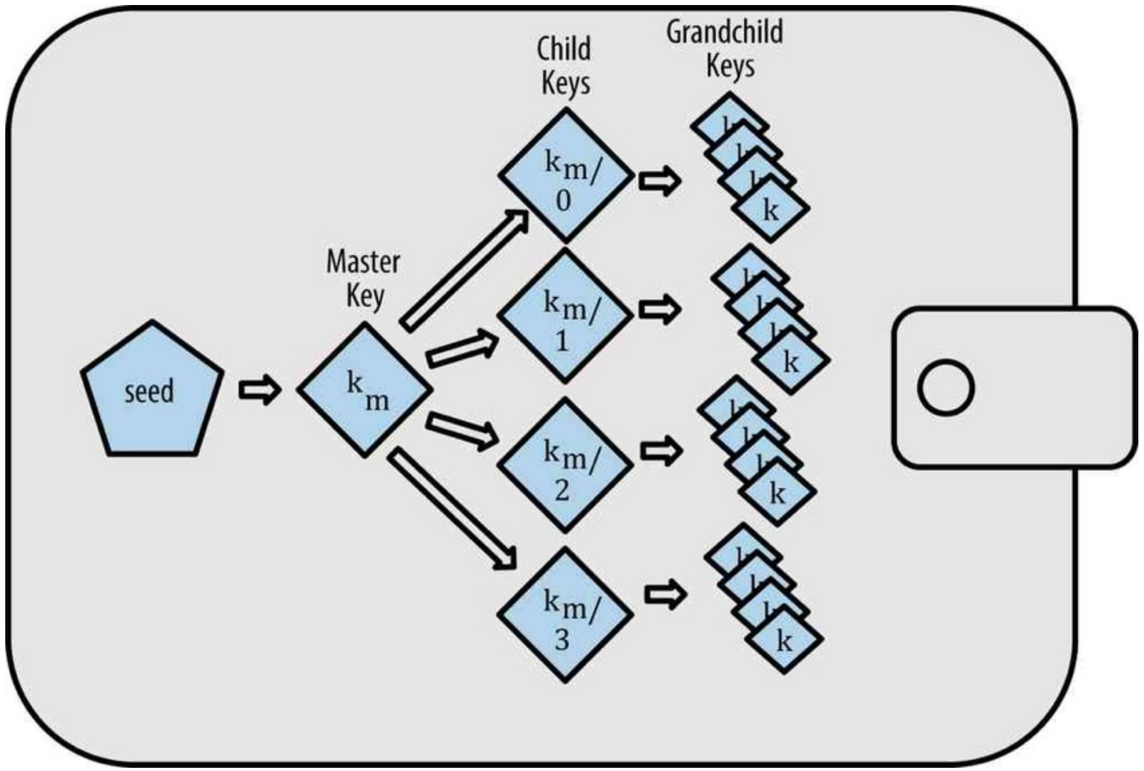
*S = b * A = b * a * G*

*S = b*a*G =a*b*G*

Now S can be used as source of shared secret to encrypt/ decrypt messages between Alice and Bob.

Key Management

- Hierarchical Deterministic Keys
- Multi-Signature
- Key Recovery
- Secret Sharing
- Revocation
- Group Key Anonymity
- EPID Enhanced Privacy ID + SoftwareGuardExtension, Sawtooth



Secret Sharing

Split secret into pieces and distributed them.

N of M pieces needed to reconstruct secret.

Analogy = Voldemort Horcrux.

Key Recovery.

Data Storage.

Modern Crypto: Zero Knowledge

Trusted first party Prover, proves to second party, Verifier that a statement is true in such a way that secret information upon which the proof of the statement is based is not conveyed to the Verifier. The Verifier cannot then prove to a third party that the statement is true.

Modern Crypto: Blinded Signature

Party A writes message.
Party B verifies A's identity.
A writes message on paper but does not disclose message to B.
A puts message in carbon paper envelope.
B signs outside of envelope and transmits envelope to party C.
Party C opens envelope and knows message came from a verified identity by the carboned signature.
C cannot be trace the contents of the message back to A.

DJB NaCL Cipher Suite

Best of breed Crypto Library is NaCl. Designed by Daniel J. Bernstein, http://nacl.cr.yp.to

Most popular implementation is LibSodium: https://www.gitbook.com/book/jedisct1/libsodium/details

LibNacl: Python

Ed25519 Signatures

Curve25519 (X25519) Diffie-Hellman Key Exchange

XSalsa20/20 Stream Cipher Encryption

poly1305 Message Authentication Code

CurveCP Protocol

NaCL: One True Cipher Suite

Ian Grigg: "*In the past, things like TLS, PGP, IPSec and others encouraged you to slice and dice the various algorithms as a sort of alphabet soup mix. Disaster. What we got for that favour was code bloat, insecurity at the edges, continual arguments as to what is good & bad, focus on numbers & acronyms, distraction from user security, entire projects that rate your skills in cryptoscrabble, committeeitus, upgrade nightmares, pontification ... Cryptoplumbing shouldn't be like eating spagetti soup with a toothpick. There should be One Cipher Suite and that should do for everyone, everytime. There should be no way for users to stuff things up by tweaking a dial they read about in some slashdot tweakabit article while on the train to work... Picking curve25519 xsalsa20 poly1305 is good enough for that One True CipherSuite motive alone... It's an innovation! Adopt it.*"

Matthew Green: "*Any potential 'up my sleeve' number should be looked at with derision and thoroughly examined (Schneier thinks that the suggested NIST ECC curves are probably compromised by NSA using 'up my sleeve' constants). This is why I think we all should embrace DJB's curve25519.*"

wolfSSL: "*Curve25519 so far is destroying the key agreement and generation benchmarks of previous curves, putting up numbers for both key agreement and generation that are on average 86 percent faster than those of NIST curves."*

Adam Langley: "*Of the concrete implementations of Diffie-Hellman, curve25519 is the fastest, common one.*"

Dan Bernstein: "*An attacker who spends a billion dollars on special-purpose chips to attack Curve25519, using the best attacks available today, has about 1 chance in 1,000,000,000,000,000,000,000,000,000 (27 0s) of breaking Curve25519 after a year of computation.*"

RAET Reliable Asynchronous Event Transport

https://github.com/RaetProtocol/raet

End-to-End Encryption and Signing with NaCL, X22519, CurveCP Handshake, Curve22519, Salsa20/20 Poly1305

Python with LibNacl, Ioflo

Asynchronous architecture with non-blocking I/O

UDP for Interhost communication

Unix domain sockets for interprocess communications

Presence Support

Plenum RBFT Python Implementation

PLenum RBFT https://github.com/evernym/plenum

https://github.com/evernym/plenum/wiki

Digital Signatures (no Macs) so don't need digests.

Uses RAET (Reliable Asynchronous Event Transport) protocol

https://github.com/RaetProtocol/raet

Smart Contracts

Distributed consensus server acts as an autonomous notary

Provides contract creation, validation, and enforcement

Ricardian contracts = user readable but digitally executable (JSON)

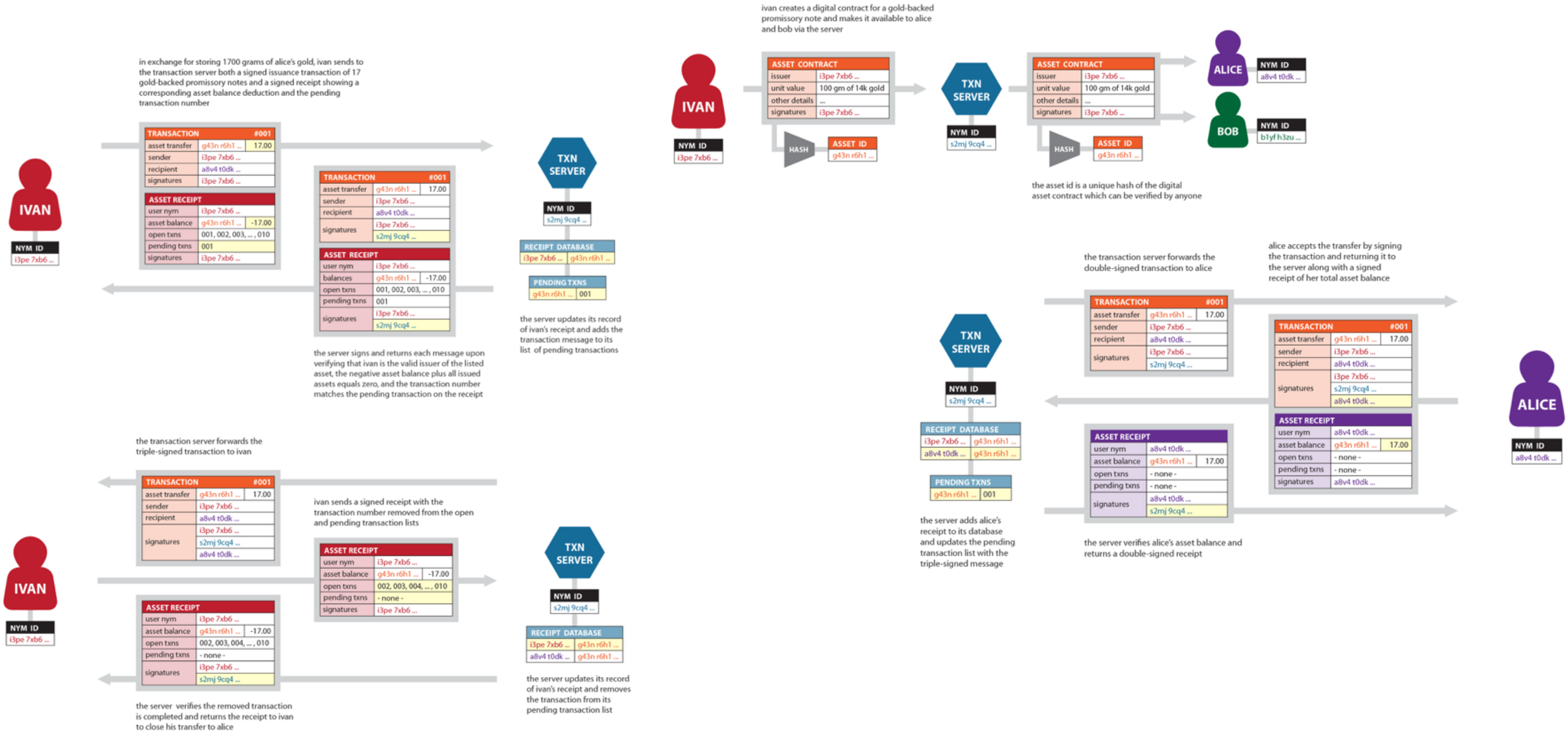
Triple Entry Bookkeeping

Ethereum, Open Transactions, HyperLedger etc

Triple Entry Bookkeeping

Distributed Consensus Notary is Automated Third Signer

Destruction of account history after completion because each party has legally enforceable triple signed receipt



Graph Based Identity

Identity = *Identifiers* + *Attributes*

Identifiers = *globally unique* *cryptonyms* + *aliases*

Attributes = *user data, proofs*

Facilitate attribute exchange between entities sufficient to enable transaction to proceed

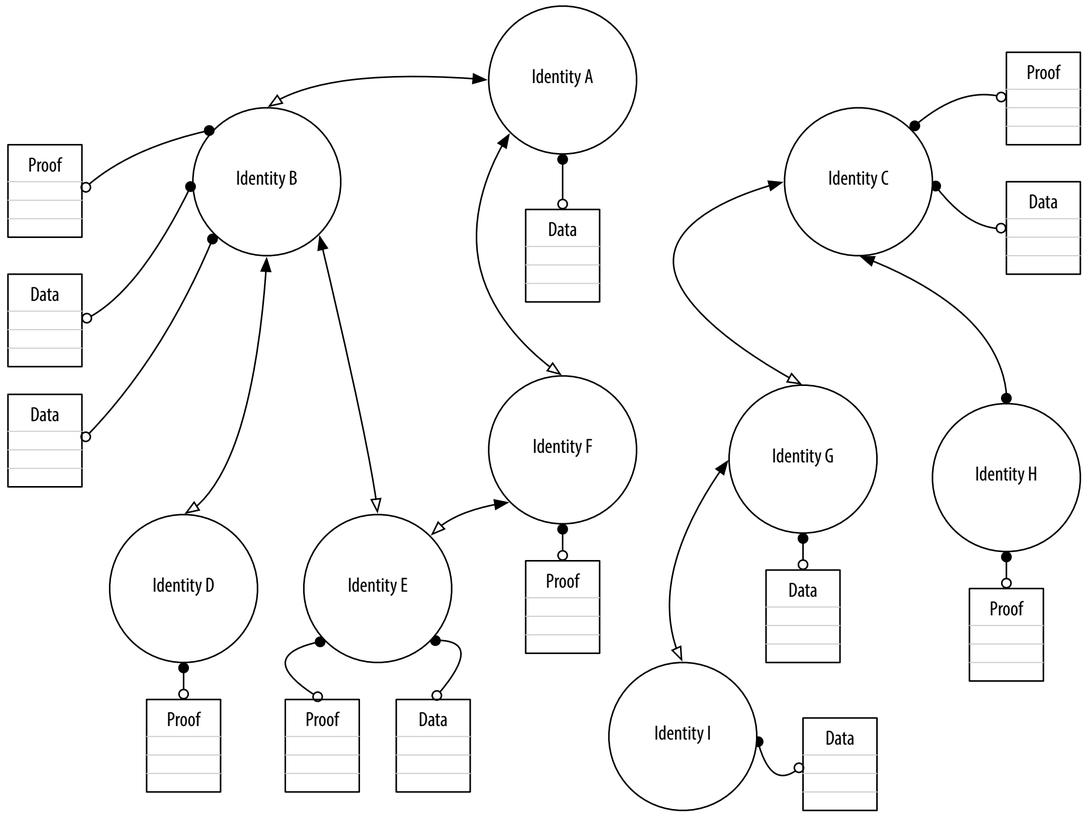
Identity System Features:

- Sovereignty (own your own identity)
- Security (impervious to fraud)
- Privacy (least disclosure)

Sovereignty = portable identifiers + user controlled access

Security = distributed consensus + modern crypto

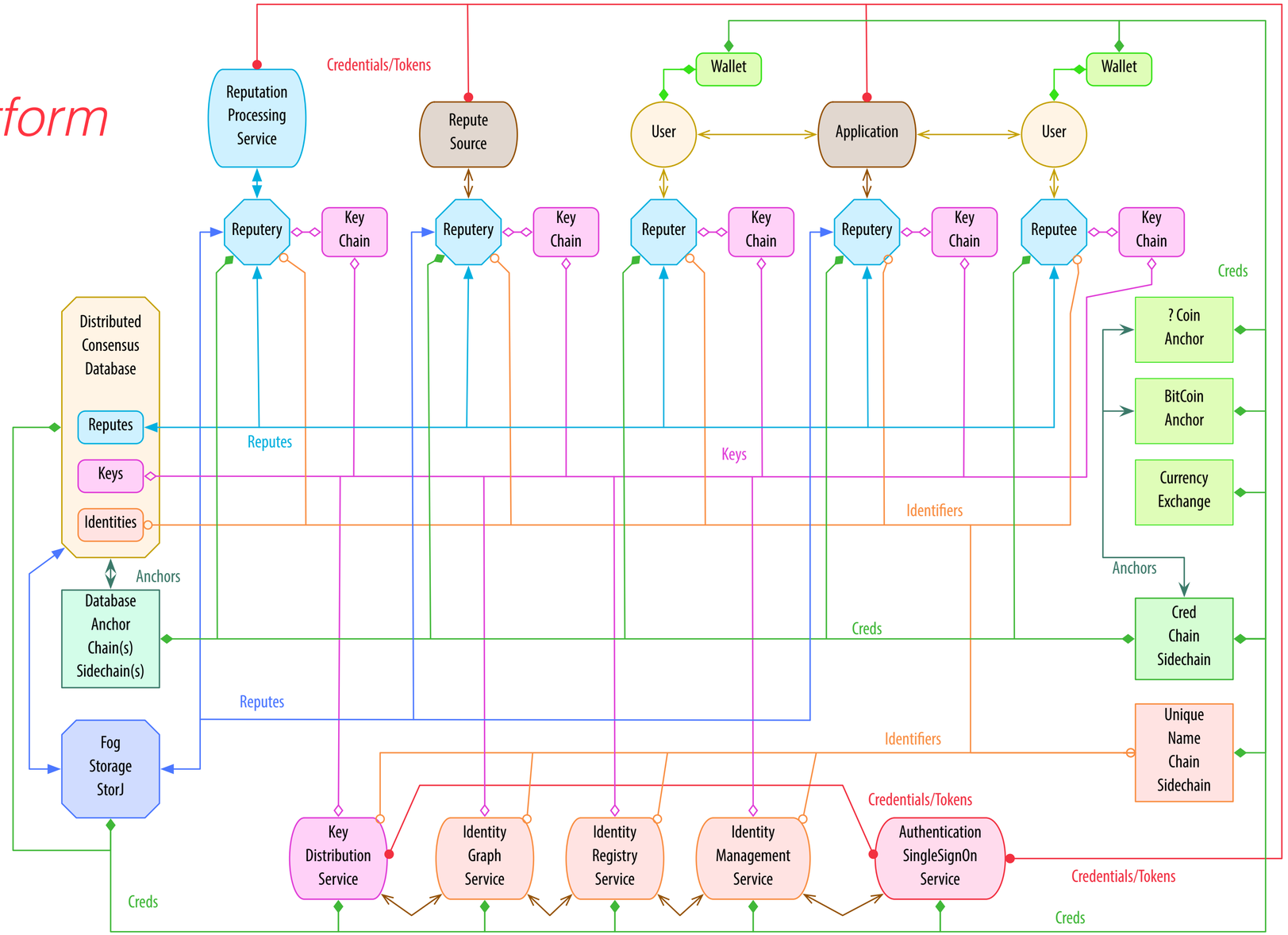
Privacy = granular graph based identities + layered disclosures + zero knowledge disclosures + group identities



https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/Identity-System-Essentials.pdf

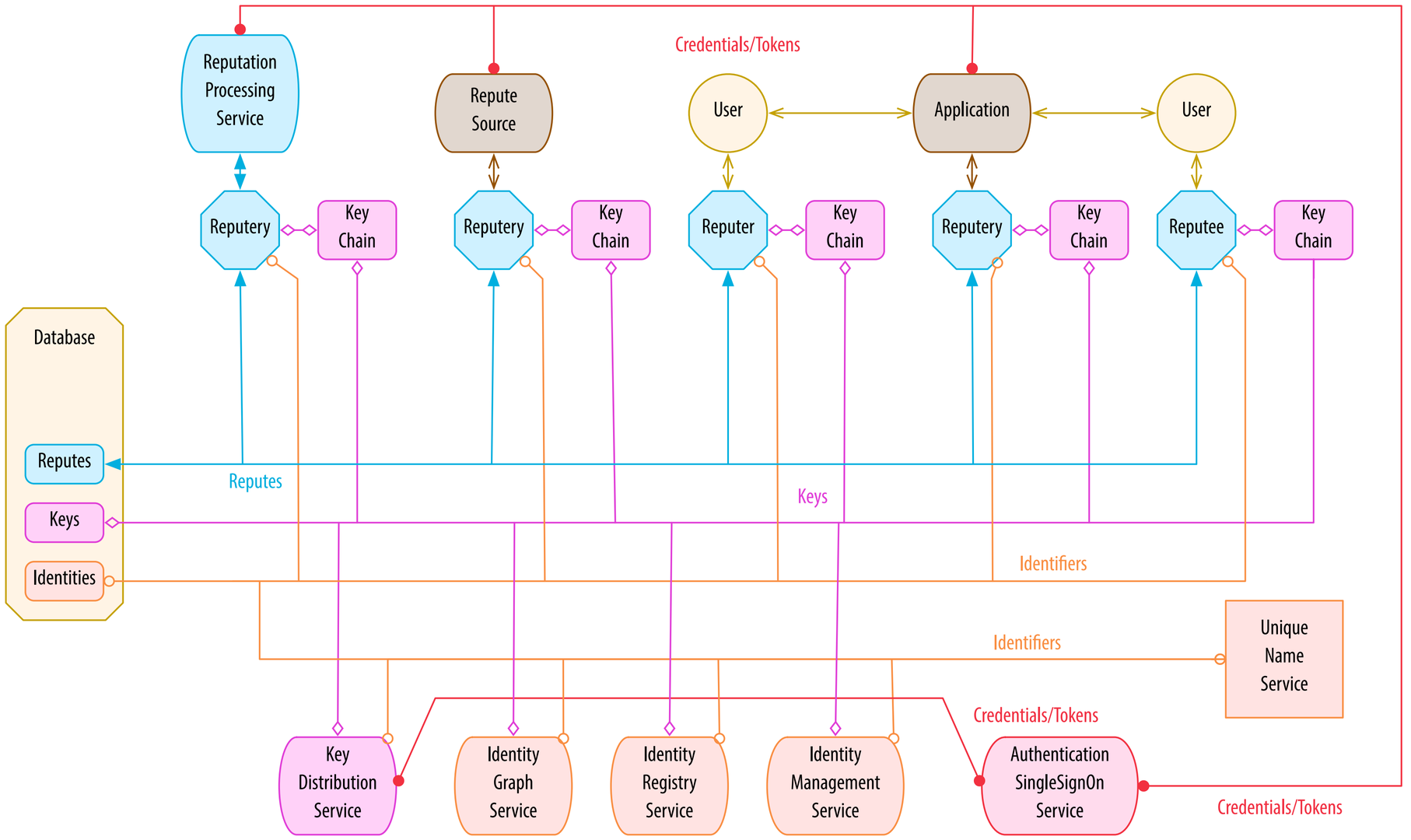
Reputation System

Key component of any *platform*



https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/open-reputation-low-level-whitepaper.pdf

Simple Reputation



Distributed Autonomic Service

DAS = service based on distributed consensus + autonomic computing algorithms on decentralized computing infrastructure = *distributed AI*

*Now b*uilding a *reputation as a service* (RAAS)

Eventually a RAAS on a DAS

Slides

https://github.com/SmithSamuelM/Papers/blob/master/presentations/BlockChain.pdf

sam@prosapien.com