Blockchain & Money

Class 7

September 27, 2018

Class 7 Overview

- Readings and Study Questions
- Blockchain Technical Features
- Framework for Comparing Costs and Trade-offs of Decentralization
- Challenges with Blockchain Technology
- Buterin Trilemma
- Possible Solutions for Scalability, Efficiency, Privacy & Interoperability
- Governance Most Challenging
- Conclusion

Class 7 (9/27): Readings

Required

- *’Geneva Report’* Chapter 2 (pages 9 – 16); Casey, Crane, Gensler, Johnson, and Narula
- *‘On the Scalability of Blockchains’* The Control
- *‘Transaction Speeds: How do Cryptocurrencies Speeds Stack up to Visa or PayPal?,’* How Much.net
- ‘*Layer 2 / the Lightening Network’* Digital Currency Initiative
- *‘Top 8 Privacy Coins’* Invest in Blockchain

Optional

- *‘On Sharding Blockchains’* Ethereum Wiki
- *‘zkLedger: Privacy-Preserving Auditing for Distributed Ledgers’* Narula, Vasquez & Virza

Class 7 (9/27): Study Questions

- How critical are the technical and commercial challenges – scalability, efficiency, privacy, security, interoperability – of current blockchain technology?

- What are the possible tradeoffs of decentralization, scalability and security? What are tradeoffs of consensus software updates, governance and so-called ‘hard forks’?

- What might current work – Layer 2 applications, zero-knowledge proofs, alternative consensus algorithms – do to address current commercial challenges?

Blockchain – Technical Features

- <u>Cryptography & Timestamped Logs</u>
  - Cryptographic Hash Functions
  - Timestamped Append-only Logs (Blocks)
  - Block Headers & Merkle Trees
  - Asymmetric Cryptography & Digital Signatures
  - Addresses
- <u>Decentralized Network Consensus</u>
  - Proof of Work
  - Native Currency
  - Network
- <u>Transaction Code & Ledgers</u>
  - Transaction Inputs & Outputs or State Transitions
  - Unspent Transaction Output (UTXO) set or Account Based
  - Script, Solidity or Other Programing languages

Bitcoin and Ethereum Design

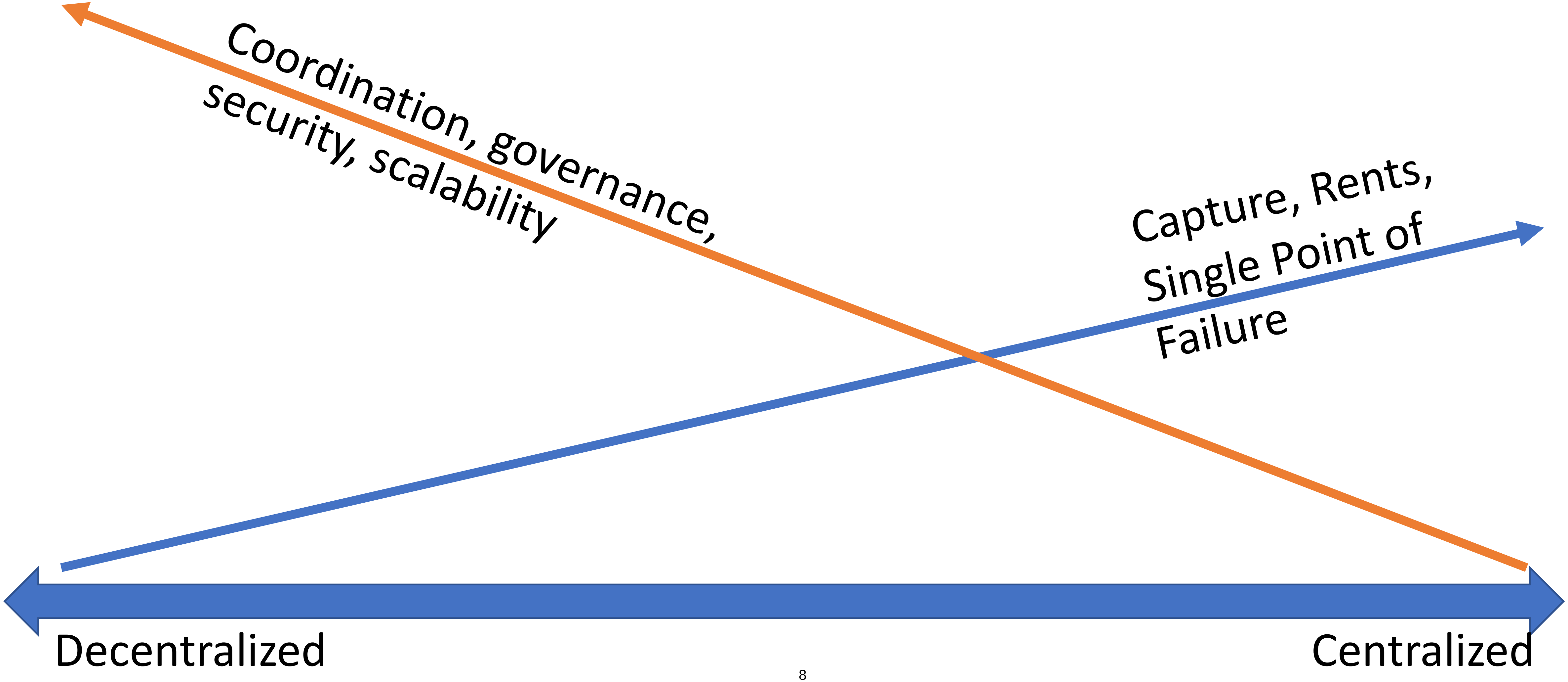
• Founder: Satoshi Nakamoto	↔	Vatalik Buterin
• Genesis: January 2009	↔	July 2015
• Code: Non Turing (Script)	↔	Turing Complete (Solidity, Serpent, LLL or Mutan)
• Ledger: UTXO – Transaction	↔	State - Account Based
• Merkle Trees: Transactions	↔	Transactions, State, Storage, Receipts (w/nonces)
• Block Time: 10 minutes	↔	14 seconds
• Consensus: Proof of Work	↔	Proof of Work
• Hash Function: SHA 256	↔	Ethash

Bitcoin and Ethereum Design

- Currency: Bitcoin ↔ ETH
- Mining: ASIC ↔ GPU
- Hashrate: 54 Exahash/S ↔ 260 Terahash/S

- Pre-sale: None ↔ ICO & prerelease of 72 m ETH
- Rewards: 12.5 BTC/block ↔ 3 ETH/block
- Monetary Policy: 1/2s every 210,000 blocks (4 yrs) ↔ Fixed, but changes by updates (was 5/block; proposal to 2)
- Fees: Voluntary ↔ Needed & market based

Framework for Comparing Costs & Trade-offs (Coase)


Coordination, governance, security, scalability
Capture, Rents, Single Point of Failure
Decentralized
Centralized

Challenges with Blockchain Technology

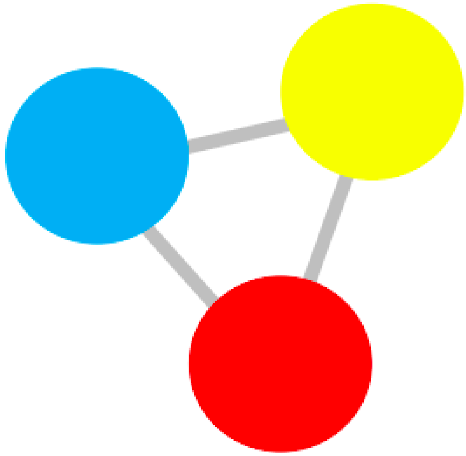
- Performance, Scalability, & Efficiency
- Privacy & Security

- Interoperability
- Governance & Collective Action

- Commercial Use Cases

- Public Policy & Legal Frameworks

Vitalik Buterin Trilemma



Decentralization

Scalability

Security

Performance, Scalability, & Efficiency

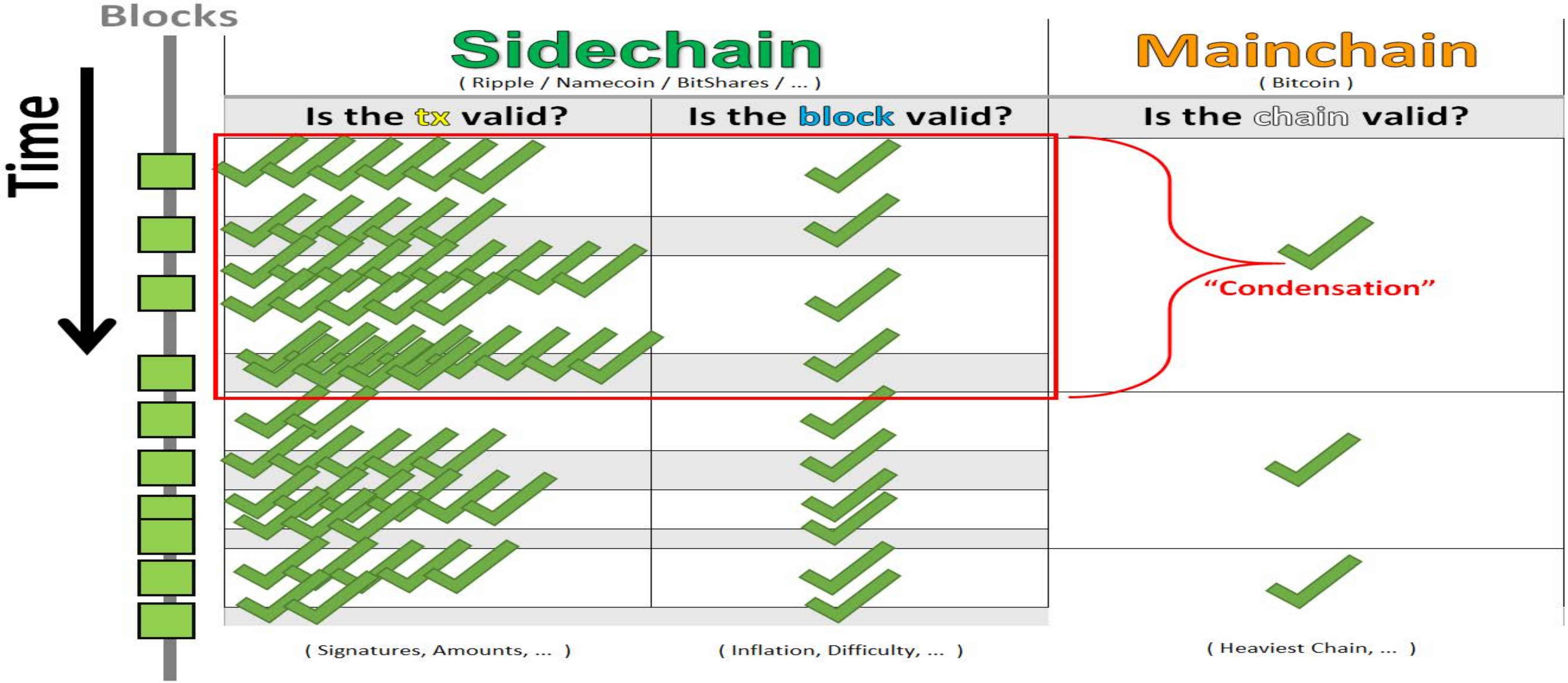
Throughput

- Bitcoin: 7 – 10 transactions / sec
- Ethereum: 20 transactions / sec
- Visa: 24,000 / sec
- DTCC: up to 100,000 / sec

Proof of Work Energy Consumption

- Bitcoin: estimates range.
- Digiconomist estimates 200 million Kwh/day - Equivalent to Electricity Consumption of:
    - 6.8 million U.S. homes,
    - 0.33% of the World, or
    - Austria

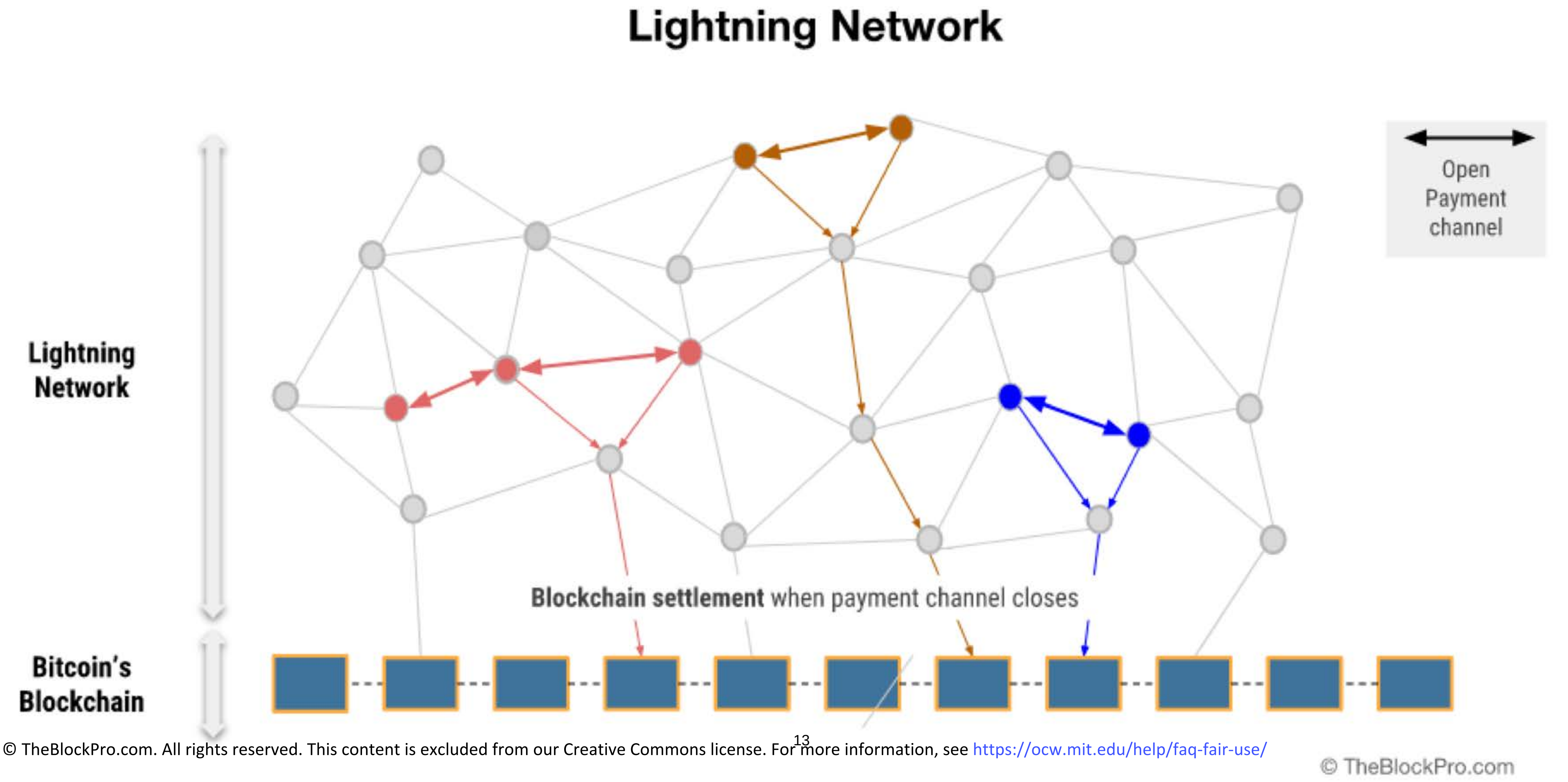
Side Chains, Sharding, Layer 2, & Payment Channels



Source: Truthcoin (11/24/15)

Image by Truthcoin. Used with permission.

Lightning Network



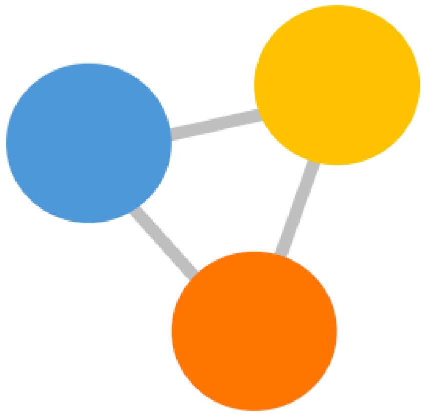
Alternative Consensus Protocols

Generally Randomized or Delegated Selection of Nodes to Validate next Block

- May have added mechanism to confirm Block Validators’ Work

Randomized Selection May be Based upon:

- Proof of Stake – Stake in Native Currency
- Proof of Activity - Hybrid of POW and POS
- Proof of Burn – Validation comes with Burning of Coins
- Proof of Capacity (Storage or Space) – Based upon Hardware Space



Delegated Selection May be Based upon Tiered System of Nodes

Major Permissionless Blockchain Applications still use Proof of Work – though:

- DASH is a hybrid of POW with a tiered system of ‘Masternodes’
- NEO uses a Delegated protocol of ‘Professional Nodes’

Privacy & Security

- Contradictory Tensions of Pseudonymous Addresses
  - Law Enforcement & Regulators want more Transparency
  - Financial Institutions, Regulators & Some Users want less Public Transparency

- Concerns about Privacy Coins & Mechanisms Fostering Illicit Activities
  - Coins: Dash, Monero, Zcash
  - Mechanisms: Mixers or Tumblers

- Cybersecurity Challenges of Private Key Custody, Generation & Storage
  - Significant Losses due to Hacks, Mismanagement and Thefts

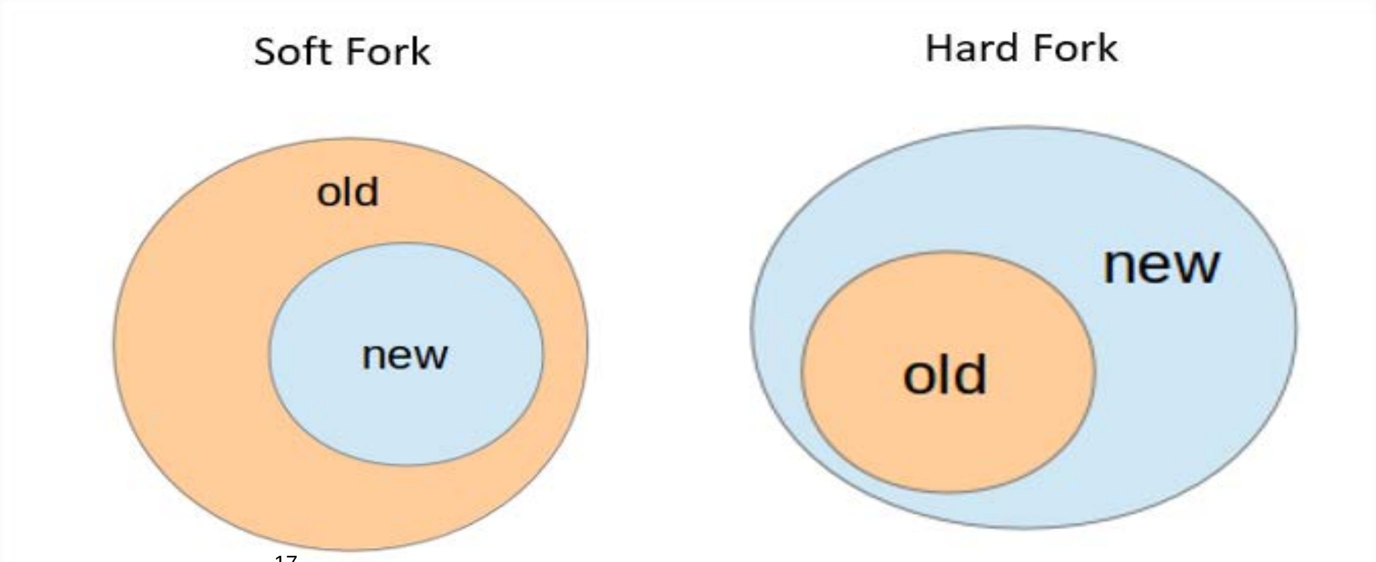
- Possible Solutions involve a) Zero Knowledge Proofs & b) Pedersen Commitments
  - Cryptographic Primitives that: a) lets Someone Prove a Statement is True without Revealing the Details of Exactly why that Statement is True & b) commit to data (like hash) but can also combine commitments

Interoperability

- Linking Blockchain Application to Legacy databases, infrastructures, and technologies
- Raises ‘Costs of Trust’ in Coordinating the Transfer of Assets and Information into the Blockchain or Across Chains
- A Solution may be to enable Decentralized Mechanisms, (including Side Chains or a ‘Layer 0’) for data transfers Across Chains
- Far more Work is Needed to Achieve Seamless Movement between and amongst new Blockchain Technology and existing Technology

Consensus Required for Certain Software Updates

- Open Source Software Updates which are not Backward Compatible
  - Older Versions won’t Validate all new Blocks
  - Similar to if Excel or Word update and New Files are not Compatible
- Leads to ‘Hard Forks’



Blockchain – Consensus supports Longest Chain

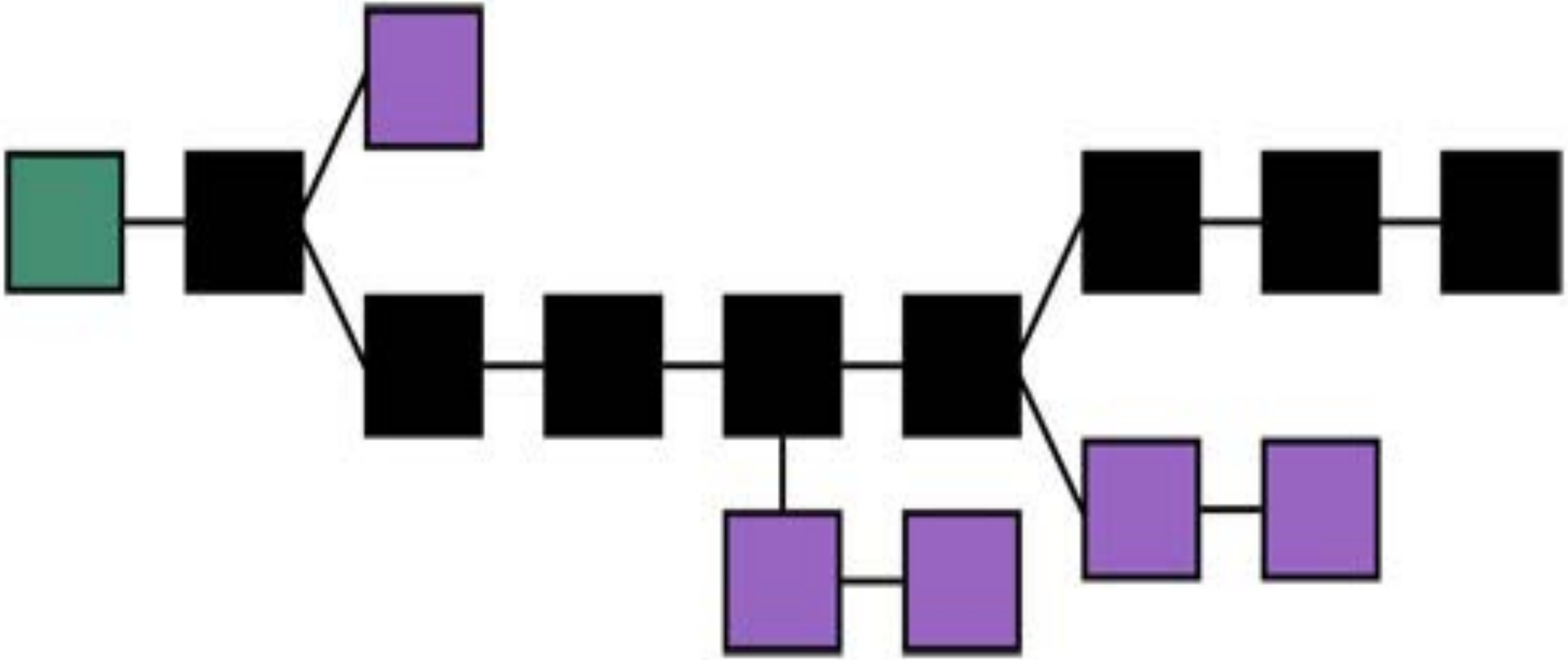


Image by Meek Mark on Wikipedia. CC BY.

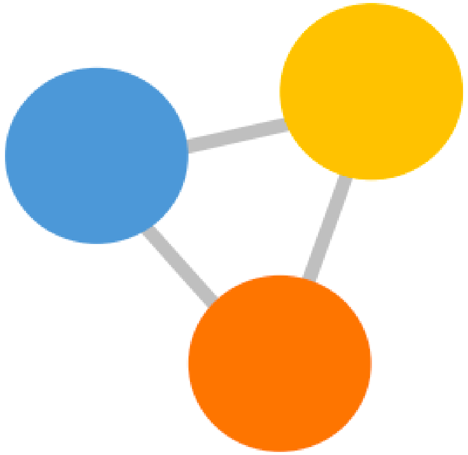
Collective Action

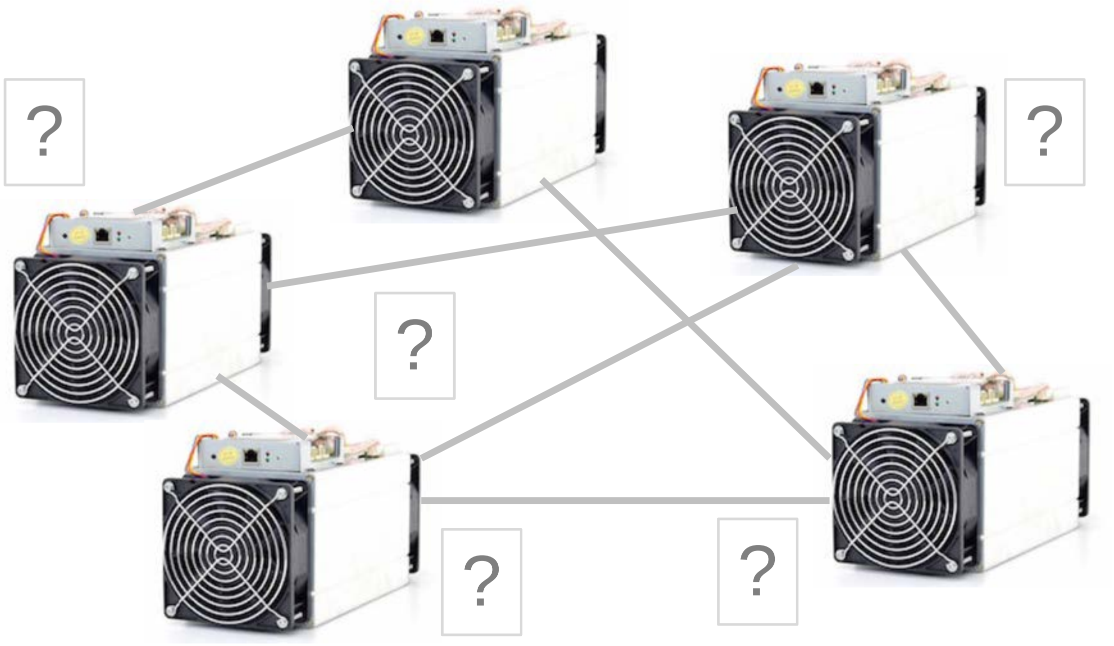
- Blockchain Applications derive their value from the participation of multiple parties in a network, adoption requires collective action

- Chicken and egg: need early adopters to start network effects, but path to incremental adoption is not often clear

Financial Sector Currently Favors

permissioned blockchains vs. permissionless blockchains





- Known set of participants
- No proof-of-work or mining
- No need for a native currency
- Distributed database technology

- Unknown participants
- Security based on incentives
- Native currency
- Crypto-economics

Class 8 (10/2): Study Questions

- How do key public policy frameworks – guarding against illicit activities, ensuring financial stability, and protecting investors – relate to blockchain technology and crypto finance?

- Under tax, bank secrecy, securities and commodities laws, what is the relevance if crypto tokens are deemed property? Currencies? Something of value? An investment contract? A commodity? What is the essence of the U.S. Supreme Court ‘Howey Test’?

- How might the ‘Duck Test’ guide thinking of blockchain technology and crypto finance?

Class 8 (10/2): Readings

- ‘*Cryptocurrencies: Oversight of New Assets in the Digital Age*’ Gensler

- ‘*The Future of Money’* Carney

- ‘*Nobel-Winning Economists: Authorities will bring down ‘hammer’ on bitcoin*’ CNBC

Conclusions

- Blockchain provides P2P Networking, but with Costs

- Decentralization Costs and Trade-offs of Permissionless Blockchain need be Compared to Centralized and Permissioned Systems

- For Scalability, Efficiency, & Privacy Challenges – it's Early Days but Promising work exists on Possible Solutions – Side Chains, Alternative Consensus Protocols & Zero Knowledge Proofs

- Challenges of Interoperability might Benefit from Decentralized Mechanisms across Chains

- Governance and Collective Action Issues inherent to the Design may end up being the Most Challenging to Solve