Blockchain Technology: Ground Truths from Finance

MIT Research & Development Conference

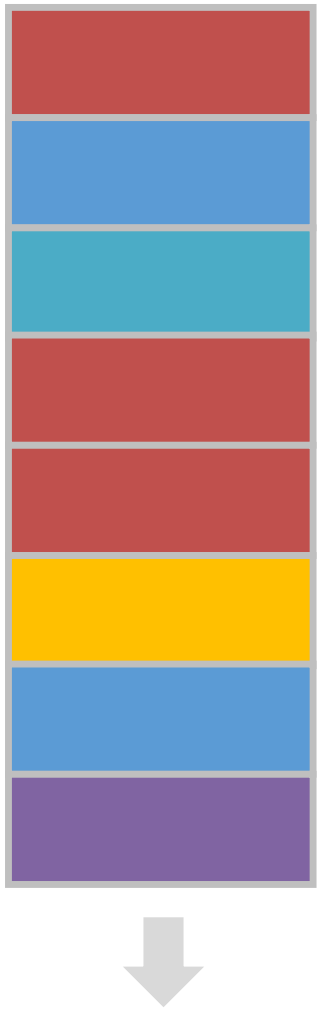
Gary Gensler
November 14

Satoshi Nakamoto: Bitcoin P2P e-cash paper October 31, 2008

“I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.”

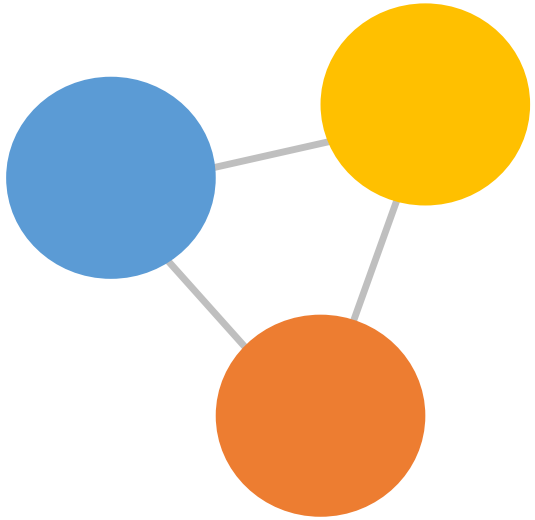
What is Blockchain Technology?

timestamped
append-only log



auditable database

consensus protocol



Secured via cryptography

- Hash functions for **tamper resistance** and **integrity**
- Digital signatures for **consent**
- Consensus for **agreement**

Addresses '**cost of trust**' (Byzantine Generals problem)

- Permissioned
- Permissionless

Use Cases: Assessing Costs & Benefits

- **Strategic questions?**
  - What is the value creation proposition?
  - What problem or ‘pain point’ is being solved?
  - What are competitors doing to address similar ‘pain points’?
  - Why is blockchain technology the best solution?
- **Specifics of the blockchain technology use case?**
  - Which costs of verification or networking can be reduced?
  - Which transactions need recording?
  - Which stakeholders need write and read access to ledgers?
  - What is the customer interface and how is it better than current interface?

Use Cases: Assessing Costs & Benefits

- **Costs of technical challenges and transition?**
  - What tradeoffs are necessary?:
  - Can Permissioned blockchain adequately address use case?
  - Can Traditional Data Base address use case?
  - How can broad adoption be realized?
- **Are *net* benefits sufficient?**

Financial Sector Issues with Blockchain Technology

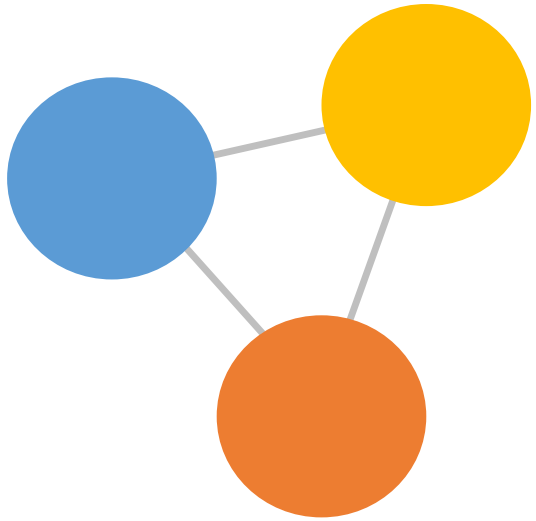
- Performance, Scalability, & Efficiency
- Privacy & Security
- Interoperability
- Governance
- Commercial Use Cases
- Public Policy & Legal Frameworks

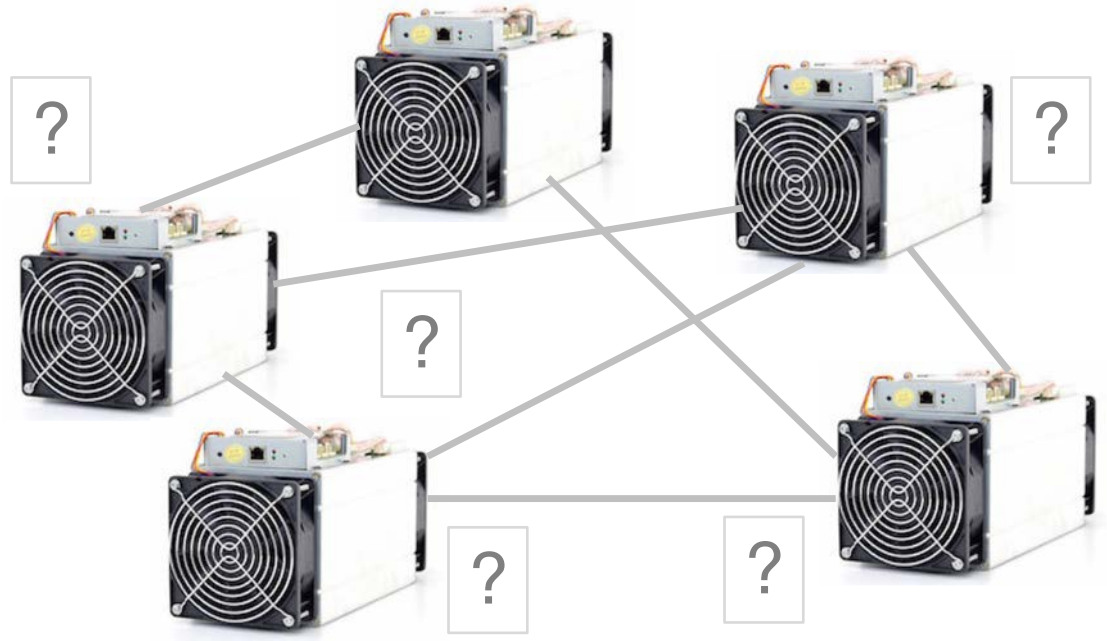
Financial Sector Potential Use Cases

- **Venture Capital -** Crowdfunding through Initial Coin Offerings
- **Payment Systems -** Cross border, Large interbank, & Retail
- **Loan Issuance & Trade Finance -** Digitizing paper-based processes
- **Clearing, Settlement and Processing –** Securities & Derivatives
- **Data Reporting**
- **Central Bank Digital Currency & Private Stable Value Tokens**

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

Why use a Blockchain vs. Traditional Database?

Traditional Databases

Trusted Party Hosts Data

Trusted Party can Create, Read, Update, & Delete (CRUD)

Client Server Architecture

Private Blockchain

Known Participants

Private Write Capability

Append Only Timestamped Log

Publicly Verifiable

No Native Currency

Public Blockchain

Unknown Participants

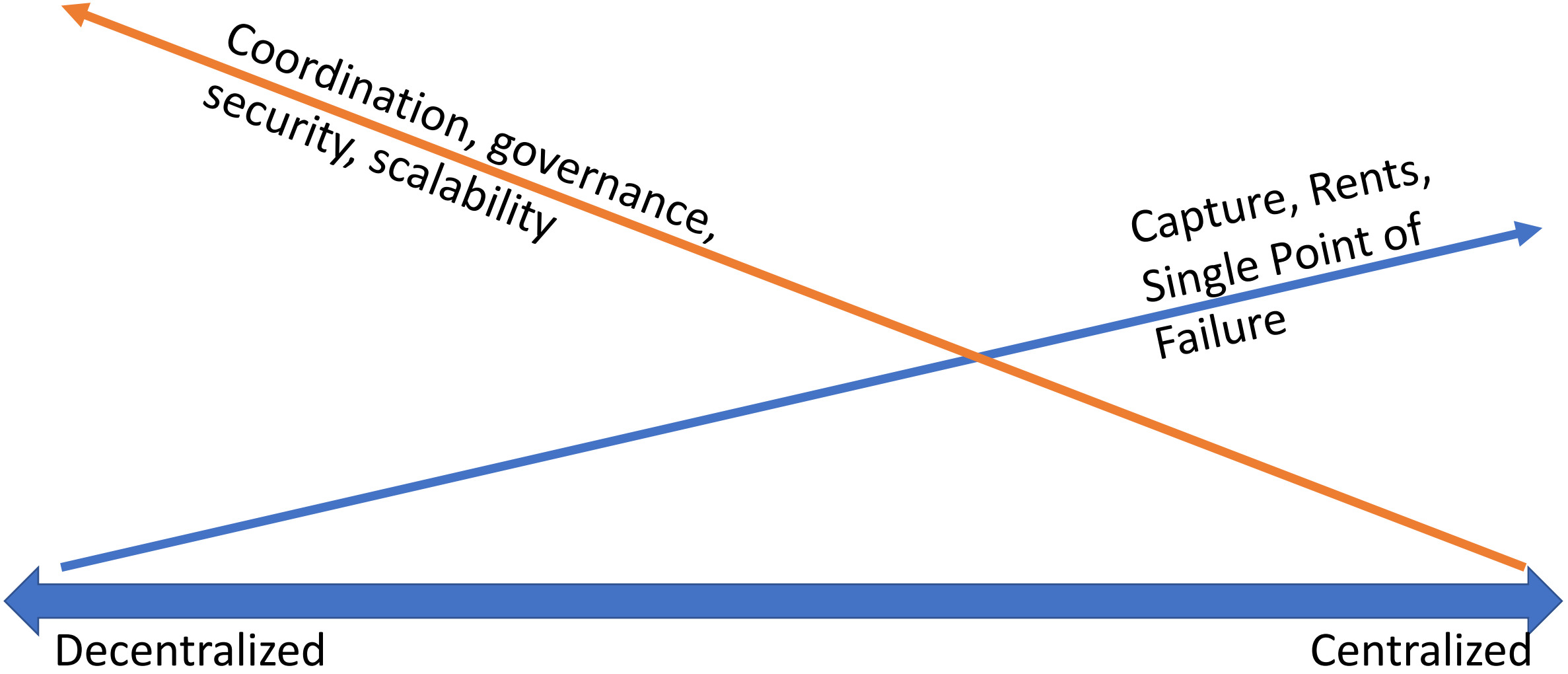
No Central Intermediaries

Public Write Capability

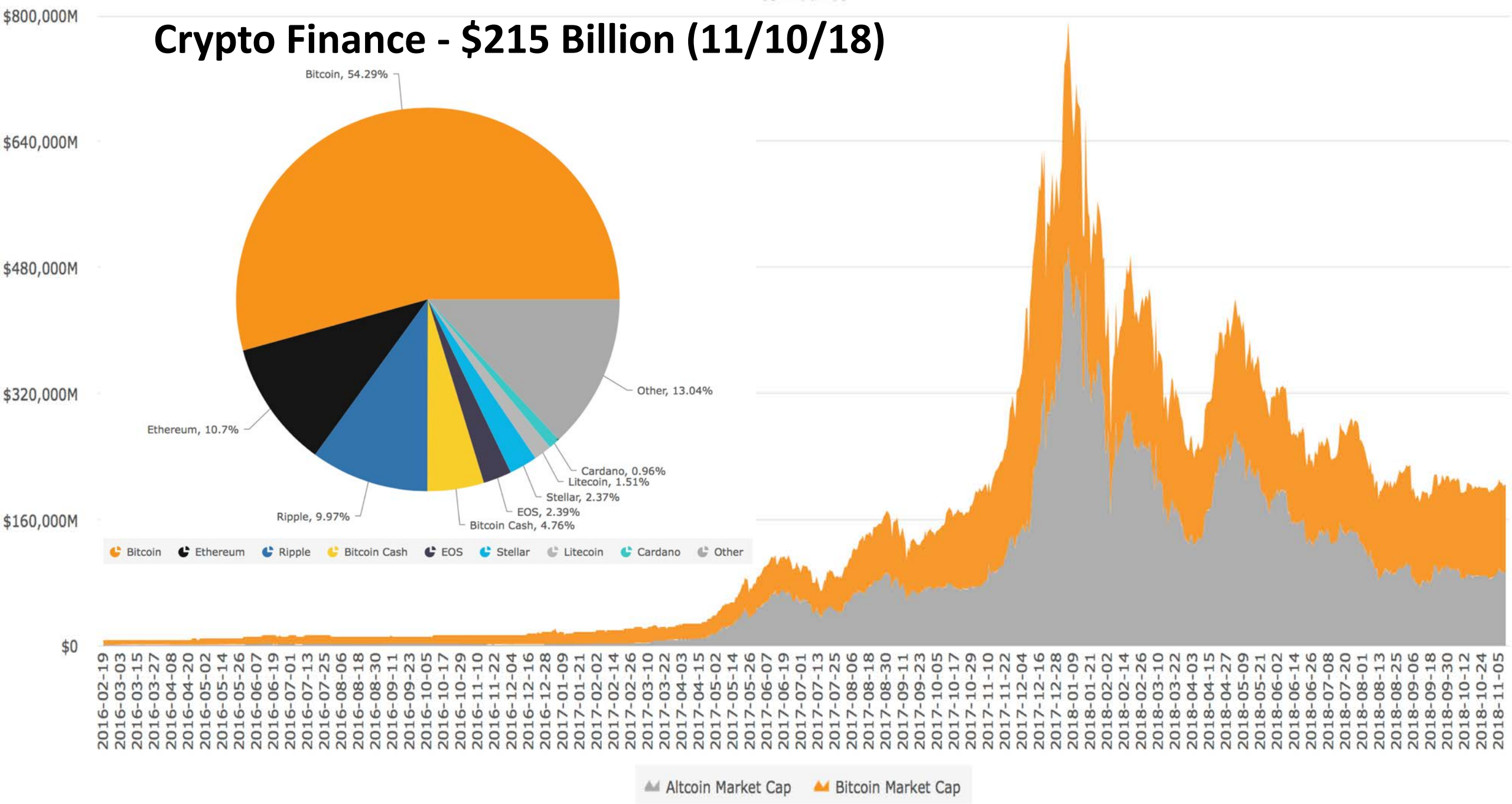
Peer to Peer Transactions

Token Economics

Framework for Comparing Costs & Trade-offs



Crypto Finance - $215 Billion (11/10/18)



Crypto Finance Investor Challenges

- Assessing Viability of Token Use Cases
- Custody of Private Keys
- Markets Readily subject to Fraud, Scams, & Manipulation
- Crypto Lending and Borrow
- Tax Compliance and Reporting
- Evolving Regulatory Guidance

Public Policy Framework

- Guarding Against Illicit Activity

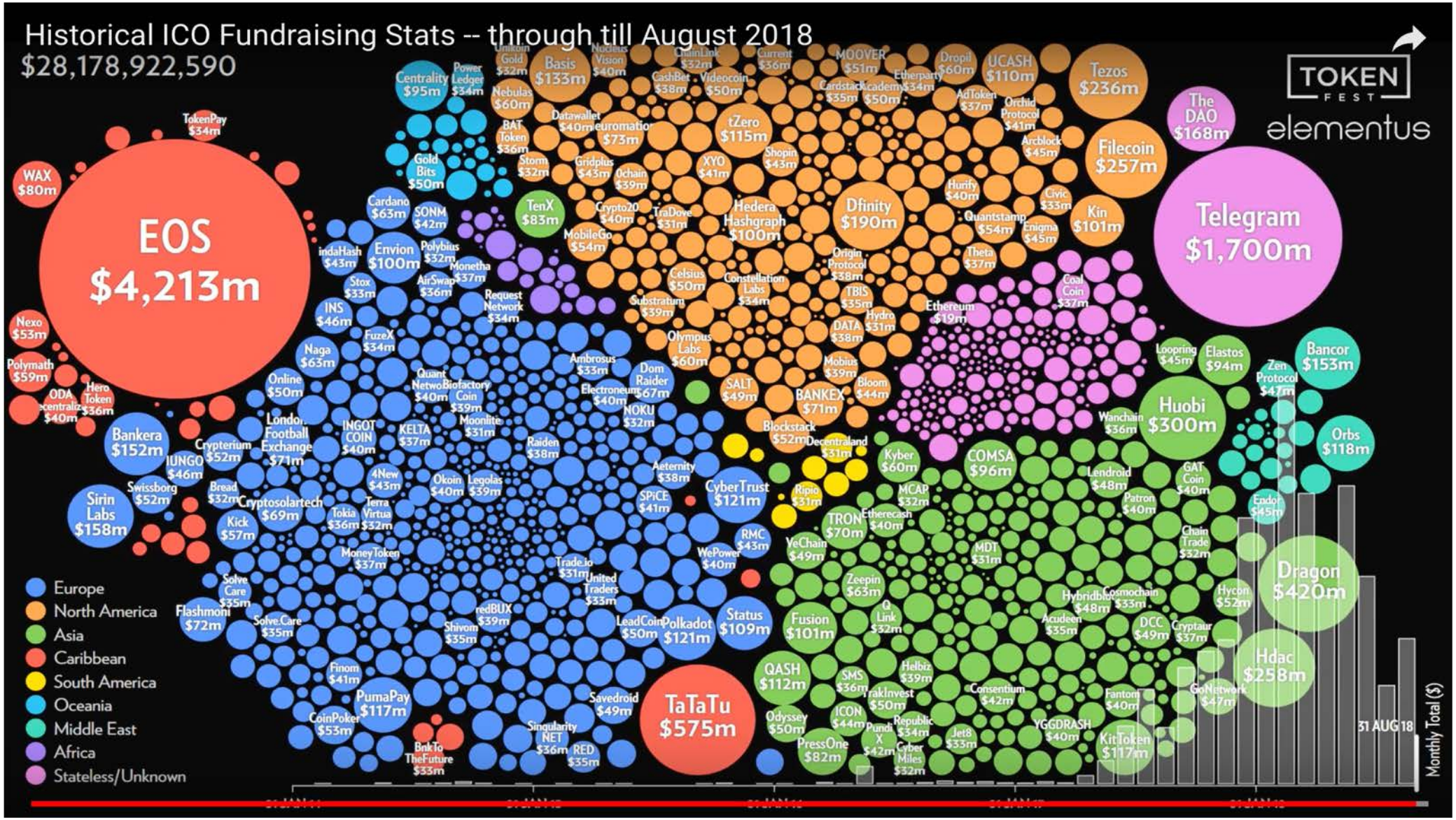
- Financial Stability

- Protecting the Investing Public

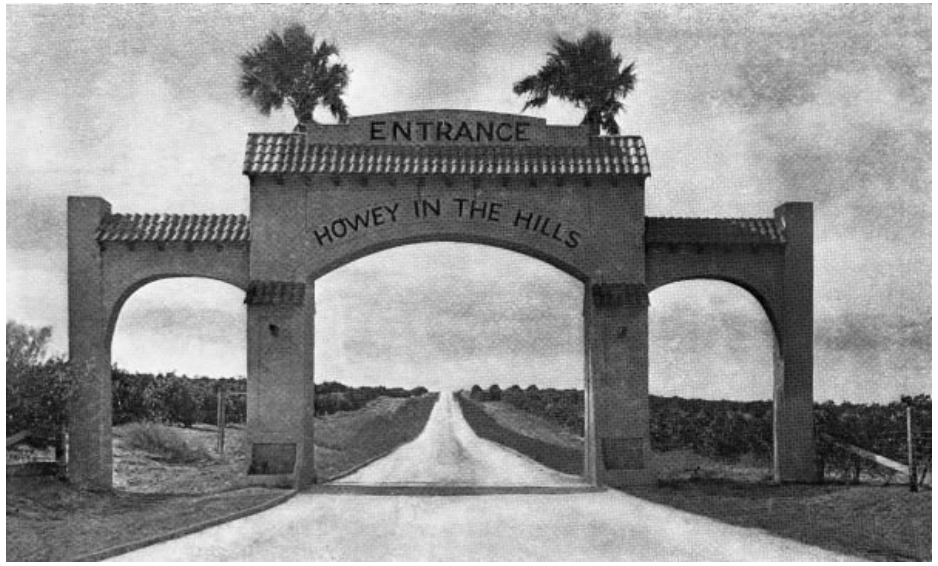
Crypto Exchanges

- Responsible for vast majority of crypto secondary market
- Critical gateways to instill confidence and implement public policy
- Greater than 30 million direct members
- Lack brokered access or meaningful market integrity rules
- Custodial wallets are honey pots for hacks
- Decentralized exchanges present new opportunities and risks

Initial Coin Offerings – Crowdfunding for Investment & Consumption



U.S. Securities Law



- The Howey Test (1946):
  - Is it an investment of money or assets?
  - Is the investment in a common enterprise?
  - Is there a reasonable expectation of profits?
  - Is it reliant on the efforts of a promoter or others?

The Duck Test

“When I see a bird that walks like a duck and swims like a duck and quacks like a duck, I call that bird a duck.”

James Whitcomb Riley, poet

Central Banks, Cryptocurrencies, and Blockchain Technology

- Monitor and Study
- Restrict Use
- Payment System Experimentation
- Central Bank Digital Currency Initiatives

Conclusions – Blockchain Technology

- Provides Peer to Peer Alternative
- Addresses Verification and Networking Costs
- Use Cases Must Address why vs. Traditional Data Base?

- Financial Sector's Characteristics, Challenges and Scale Present Opportunities
- Broad Adoption rests on addressing Technical and Commercial Challenges
- Public Confidence is Built upon coming within Public Policy Norms

- Development will Swing with Hype Masquerading as Fact
- Disrupters, Financial Incumbents and Big Tech will all Play a Role
- The Potential, though, to be a Catalyst for Change is Real