Blockchain & Money

Class 9

October 4, 2018

Class 9 Overview

- Readings and Study Questions
- Blockchain Technical and Commercial Challenges
- Permissioned Blockchain Systems
- Blockchain Systems vs. Traditional Databases
- Conclusions

Class 9 (10/4): Study Questions

- What is permissioned or private distributed ledger technology? How does it differ from permissionless or open blockchain applications?

- What are the key blockchain inspired features of Corda and Hyperledger Fabric? What is Digital Asset Holdings?

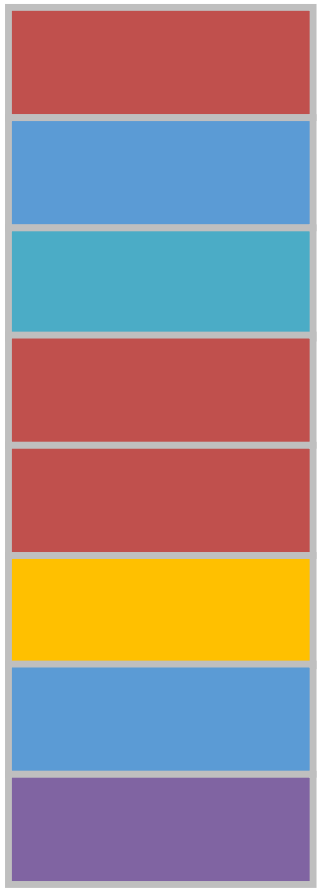
- What are the business tradeoffs of utilizing a permissioned vs. a permissionless application? What are the tradeoffs for consumers?

Class 9 (10/4): Readings

- '*Enterprises building Blockchain Confront Early Tech Limitations'* CoinDesk
- '*Technical difference between Ethereum, Hyperledger fabric and R3 Corda'* Nandi
- '*What is Corda?'* Newton
- *'A Blockchain Platform for the Enterprise, Introduction'* Hyperledger Fabric
- *'What is Digital Asset? / Distributed Ledgers for Financial Institutions'* Coin Central

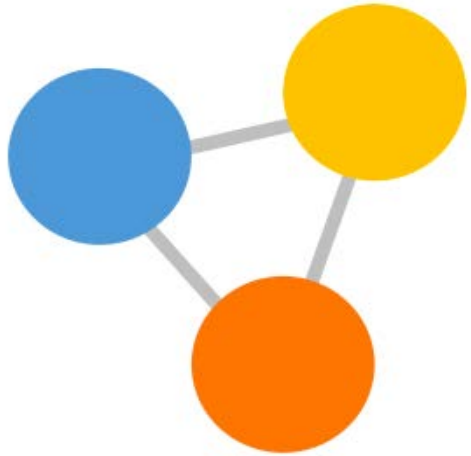
What is a blockchain?

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

5

Blockchain – Technical Features

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

Challenges with Blockchain Technology

- Performance, Scalability, & Efficiency
- Privacy & Security

- Interoperability
- Governance & Collective Action

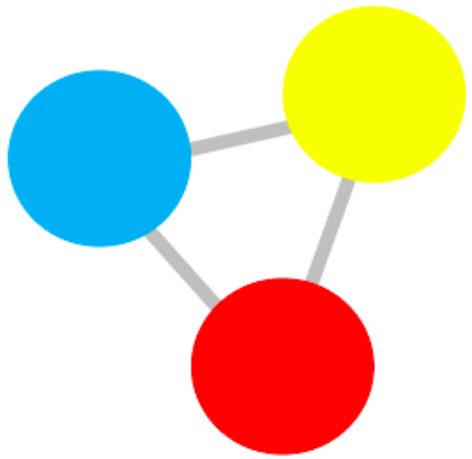
- Commercial Use Cases

- Public Policy & Legal Frameworks

7

Vitalik Buterin Trilemma

Scalability



Decentralization

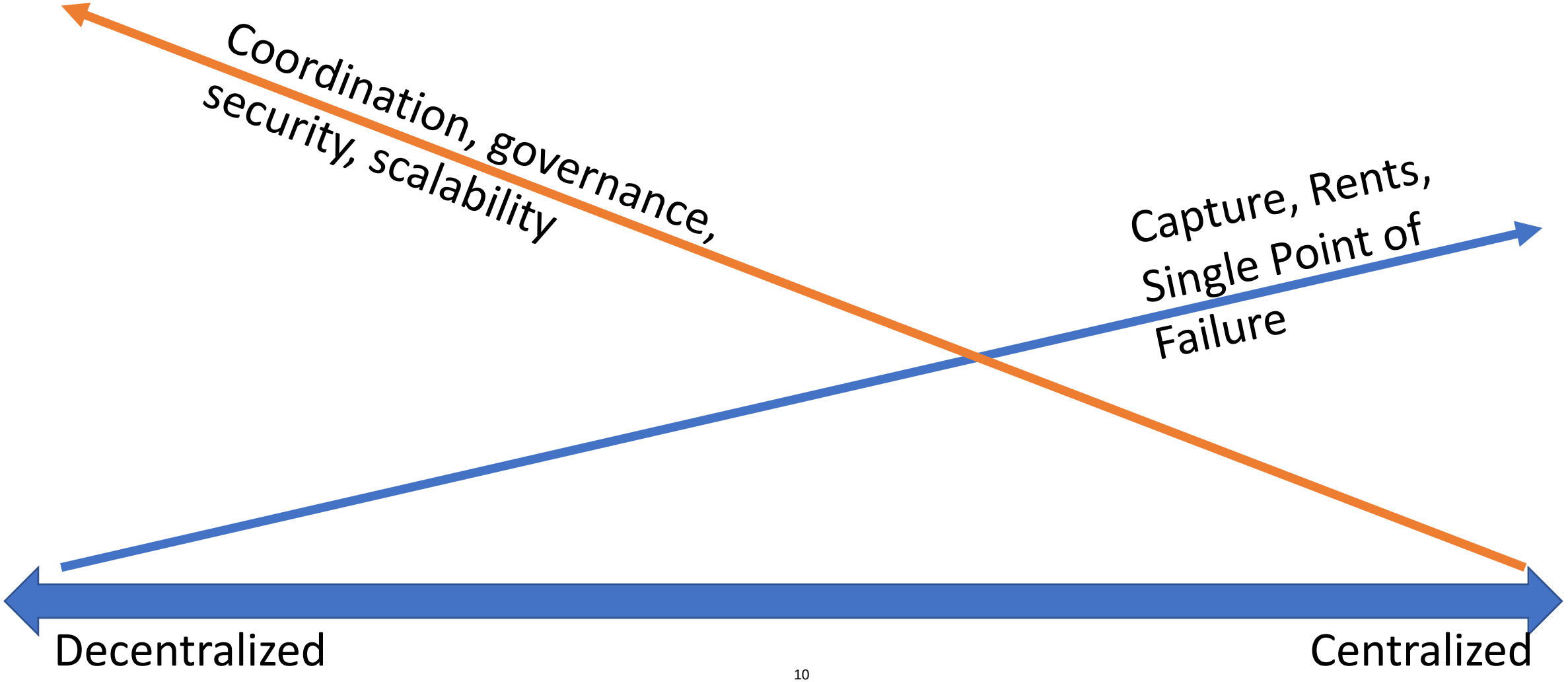
Security

Public Policy Framework

- Guarding Against Illicit Activity
- Financial Stability
- Protecting the Investing Public

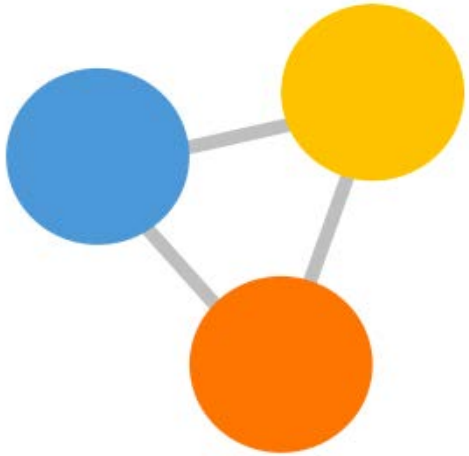
9

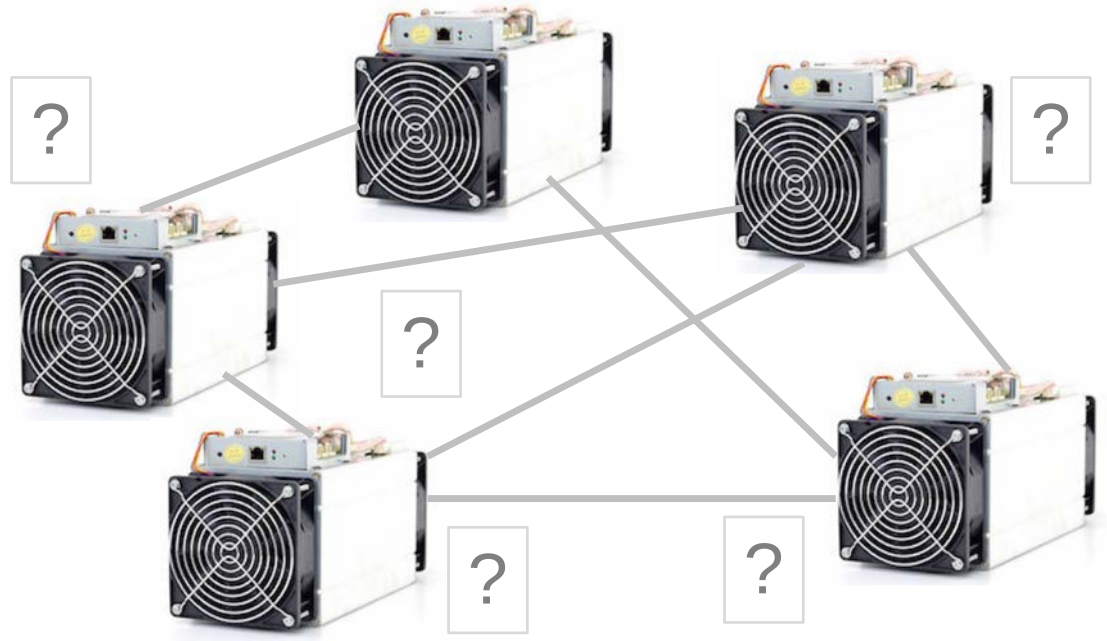
Framework for Comparing Costs & Trade-offs (Coase)



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

11

Blockchain – Technical Features

Permissioned?

- Cryptography & Timestamped Logs — Yes
  - Cryptographic Hash Functions ✓
  - Timestamped Append-only Logs (Blocks) ✓
  - Block Headers & Merkle Trees ✓ ✓
  - Asymmetric Cryptography & Digital Signatures ✓
  - Addresses ✓
- Decentralized Network Consensus — No
  - Proof of Work — **PBFT, Notary Nodes, etc.**
  - Native Currency — **X**
  - Network ✓
- Transaction Script & UTXO — Yes
  - Transaction Inputs & Outputs or State Transitions ✓
  - Unspent Transaction Output (UTXO) or Account Base ✓
  - Script, Solidarity or Other Programing Code ✓

Permissioned Private Blockchains
Key Design Features

- Membership Limited to Authorized Nodes
- Transactions can also be Limited to Authorized Known Participants
- Data & Ledgers can be Partitioned to Keep amongst Subgroups of Nodes
- Consensus built on Permissioned, Private Protocols – Globally or Modular between Transacting Parties.
  - Practical Byzantine Fault Tolerance
  - Delegated Notary Nodes
  - Diverse Protocols – from Protocols for Multi Party Consensus to Crash Fault Tolerant for 1 Party
- Uses Cryptography and Registration Authorities to Mask User Data
- Facilitates Smart Contracts using Chaincode or other Programming Language
- No Native Currency – Possible, though, with Smart Contracts
- Code Generally Open Source

Hyperledger Fabric and Corda vs. Ethereum

Characteristics	Ethereum	Hyperledger Fabric	R3 Corda
Programming Language	Solidity	Go, Java	Kotlin
Governance	Distributed among all participants	Linux foundation and organisation in the Chain	R3 and organisations involved.
Smart Contract	Not legally bounded	Not legally bounded	Legally bounded
Consensus Algorithm	PoW. Casper implementation PoS.	PBFT	Notary nodes can run several consensus algorithm
Scalability	Existing scalability issue	Not prevalent	Not prevalent
Privacy	Existing privacy issue	Not prevalent	Not prevalent
Currency	Ether	None Can be made using chaincode	None

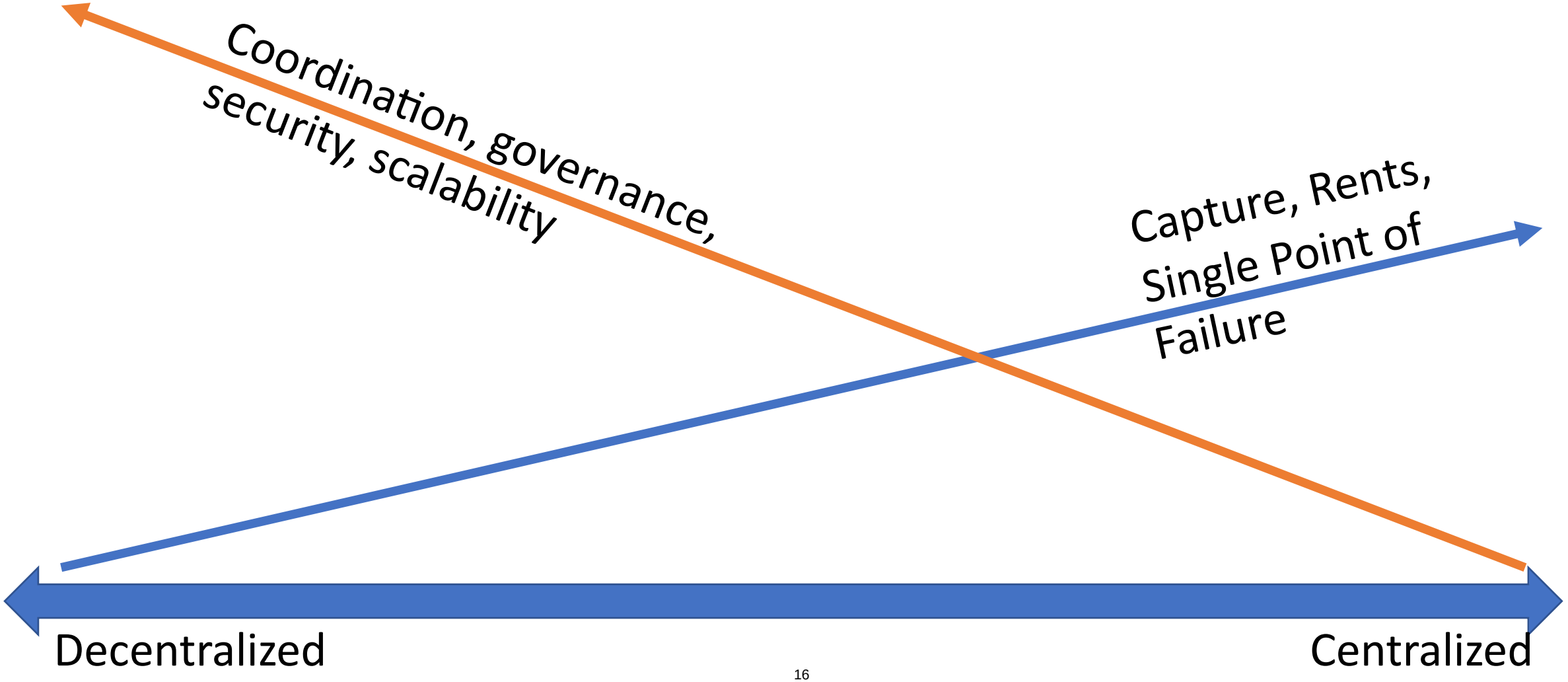
Permissioned Private Blockchains vs. Traditional Databases

- Append-only Timestamped Logs vs.
  Create, Read, Update, and Delete (‘CRUD’)

- Cryptographic Data Commitment Schemes for Data
- Distributed Ledgers & Application Platforms

- Provides Finality of Settlement
- Can provide Real Time Ledger Updates
- Lowers Reconciliation Costs (and Need for) Distributed Data Bases

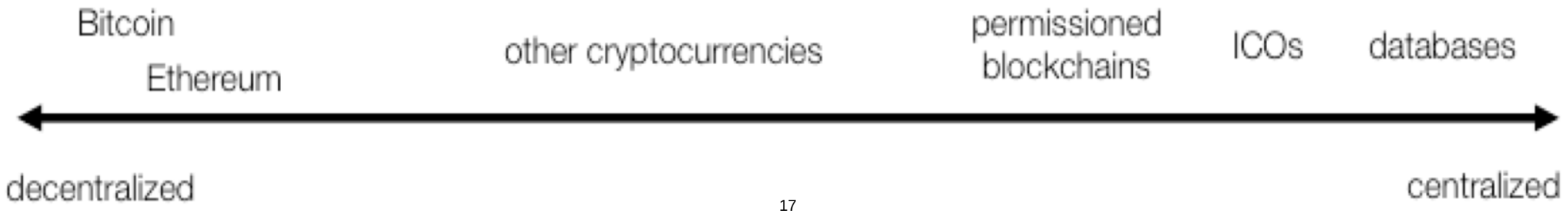
Framework for Comparing Costs & Trade-offs



Blockchains and Traditional Databases

Access Control Protocol

Open Permissionless	Multiple Permissioned	Client Server
Public Blockchain	**Private Blockchain**	**Traditional Databases**
Public Write Capability	Private Write Capability	Trusted Party Hosts Data
Peer to Peer Transactions	Finality of Data in Append Only Log	Trusted Party can 'CRUD'
No Central Intermediaries	Public Verifiability	Client Server Architecture
Token Economics		



Class 10 (10/11): Study Questions

- What are the tradeoffs of centralized institutions and markets in the financial sector?

- Which challenges of the financial sector – periodic crises, concentrated risks, economic rents, legacy systems, processing risks, financial inclusion – might present opportunities for blockchain applications?

- How does blockchain technology fit within other trends – particularly with regard to technology - facing the financial sector in 2018?

Class 10 (10/11): Readings

- '*Top financial services issues of 2018*' PwC Financial Services Institute
- 'Sheila Bair on What Hasn't Changed since the Great Recession' New York Magazine
- '*The Rise of Market Concentration and Rent Seeking in Financial Sector*' Zhang

Optional

- *'Ten Years after the Crash, We are Living in a World it Brutally Remade'* New York Magazine

Conclusions

- Public 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 – though Promising work exists on Possible Solutions – Financial Sector Currently Favors Permissioned Systems
- Blockchains – Private and Public – can Provide Real Time Final Settlement Features and Lessen Reconciliation Costs compared with Traditional Databases
- Permissioned Systems may Currently Provide better Performance and Privacy than Public Blockchains but Innovation may Well Narrow the Gap

15.S12 Blockchain and Money
Fall 2018