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?

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
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 Programming languages
Challenges with Blockchain Technology

• Performance, Scalability, & Efficiency
• Privacy & Security
• Interoperability
• Governance & Collective Action
• Commercial Use Cases
• Public Policy & Legal Frameworks
Vitalik Buterin Trilemma

Scalability

Decentralization

Security
Public Policy Framework

• Guarding Against Illicit Activity

• Financial Stability

• Protecting the Investing Public
Framework for Comparing Costs & Trade-offs (Coase)

Coordination, governance, security, scalability

Capture, Rents, Single Point of Failure

Decentralized

Centralized
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
## Blockchain – Technical Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Permissioned?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cryptography &amp; Timestamped Logs</strong></td>
<td>Yes</td>
</tr>
<tr>
<td>• Cryptographic Hash Functions</td>
<td>✓</td>
</tr>
<tr>
<td>• Timestamped Append-only Logs (Blocks)</td>
<td>✓</td>
</tr>
<tr>
<td>• Block Headers &amp; Merkle Trees</td>
<td>✓</td>
</tr>
<tr>
<td>• Asymmetric Cryptography &amp; Digital Signatures</td>
<td>✓</td>
</tr>
<tr>
<td>• Addresses</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Decentralized Network Consensus</strong></td>
<td>No</td>
</tr>
<tr>
<td>• Proof of Work</td>
<td>✓</td>
</tr>
<tr>
<td>• Native Currency</td>
<td>X</td>
</tr>
<tr>
<td>• Network</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Transaction Script &amp; UTXO</strong></td>
<td>Yes</td>
</tr>
<tr>
<td>• Transaction Inputs &amp; Outputs or State Transitions</td>
<td>✓</td>
</tr>
<tr>
<td>• Unspent Transaction Output (UTXO) or Account Base</td>
<td>✓</td>
</tr>
<tr>
<td>• Script, Solidarity or Other Programming Code</td>
<td>✓</td>
</tr>
</tbody>
</table>
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

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

Decentralized
Coordination, governance, security, scalability

Centralized
Capture, Rents, Single Point of Failure
Blockchains and Traditional Databases

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

**/non-cryptocurrency**
- Bitcoin
- Ethereum
- other cryptocurrencies
- permissioned blockchains
- ICOs
- databases

**/cryptocurrency**
- decentralized
- centralized
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