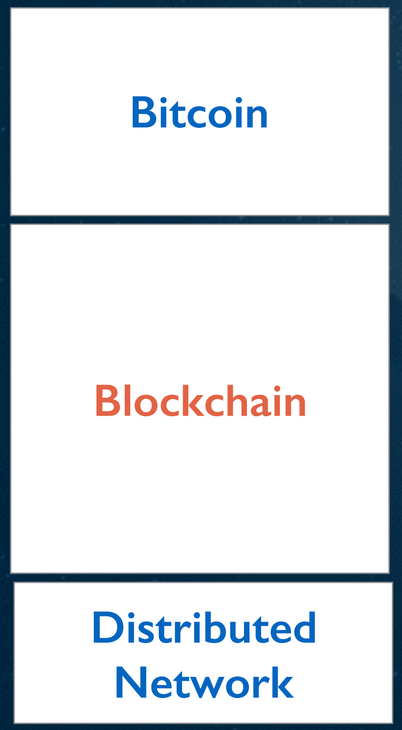
LEVEL

Leveraging Blockchain To Solve Banking Challenges

Blockchain Overview

Bitcoin was invented as a solution to the double-spend and centralized management problems inherent with most digital currencies.



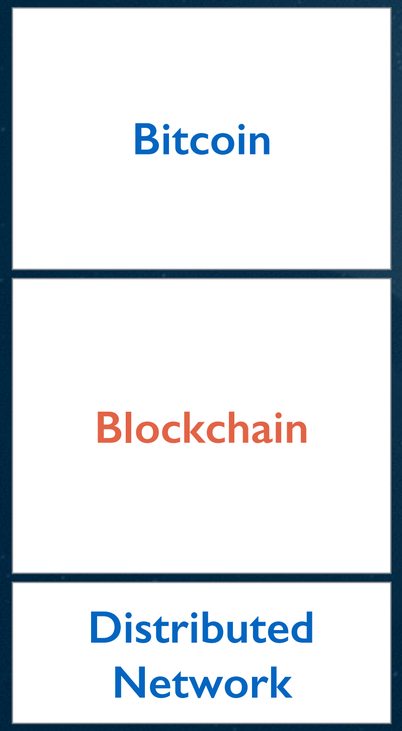
- Cryptographically secured distributed currency
- Bitcoins (the currency) must be controlled by the protocol - no central bank

- Decentralized ledger of all transactions
- Solves the Byzantine Generals Problem
- Protocol for achieving distributed consensus on a distributed network

- Currency operates over a distributed network (the public internet)
- Must be resilient to communication failures and malicious actors

Blockchain Overview

There is nothing inherent in blockchain conceptually or technically that requires the use of Bitcoin. Instead, Bitcoin is one application built on blockchain capabilities.



- Applications built on distributed networks using a common messaging protocol
- Think of Netflix, Amazon, or a web-based expense reporting system

- Messaging protocol
- Think WWW, FTP, TCP/IP

- Internet
- Private networks (intra- or inter-organization)

Blockchain and Banking: A Story of Fast Adoption

In six years, blockchain has evolved from anonymous invention to commercial use!

… but when *should* banks use blockchain to solve problems?

Is Blockchain Right for *X*?

<u>Five Key Characteristics:</u>

Database (Ledger)

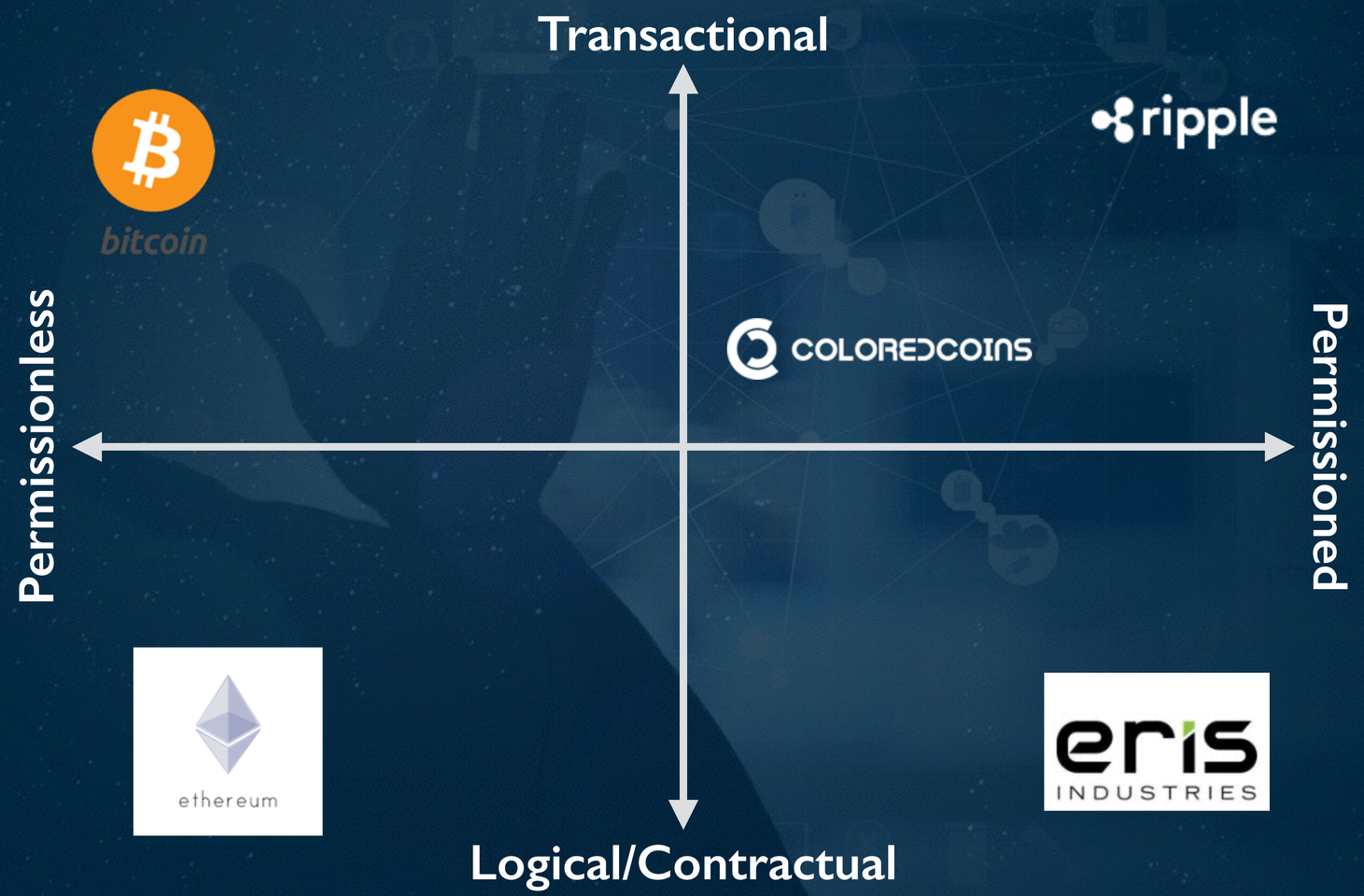
Many Writers (Authorities)

No Single Owner

No Logical Intermediary

Framework for Consensus

Which Blockchain Technology Is Best for *X*?



Consensus and Security

Most blockchain solutions attempt to solve the Byzantine Generals problem and preventing three types of failures and attacks.

- Errors of commission: forging a transaction, often through the coordination between malicious participants in the system
- Errors of omission: censoring a transaction that occurred from the ledger
- Errors of deletion: reversing a transaction that was thought to be final

The characteristics of each blockchain use case determines the relative importance of preventing these errors and the effort applied to do so.

Consensus and Security Implications

Two commonly used approaches to achieving security and consensus are based on proving that a party has performed an activity legitimately: proof of work and proof of stake.

Proof of Work

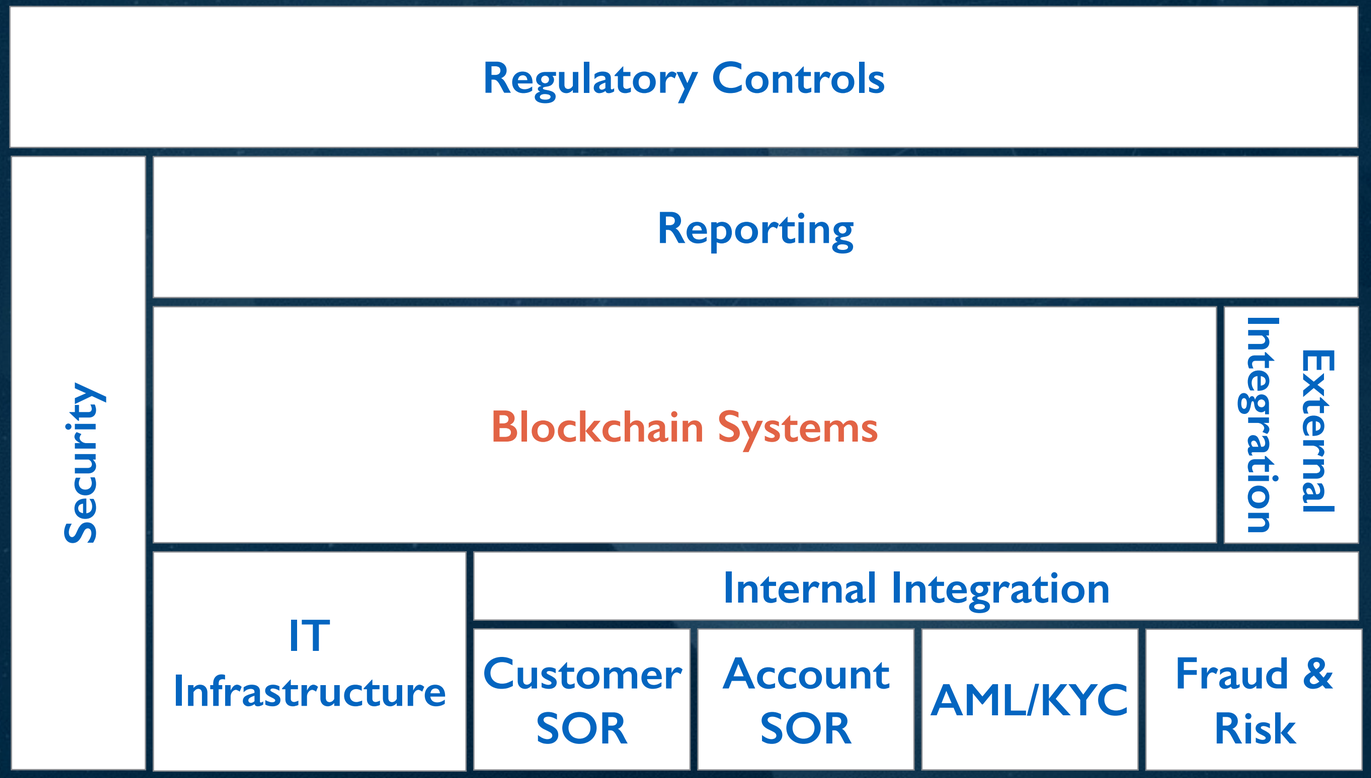
- Requires nodes that assemble blocks to solve mathematical problems of known difficulty
- Consuming CPU cycles (a proxy for spending money on electricity) reduces risk of fraud and abuse
- Difficulty of problems solved can be adjusted as processing power on the network changes

Proof of Stake

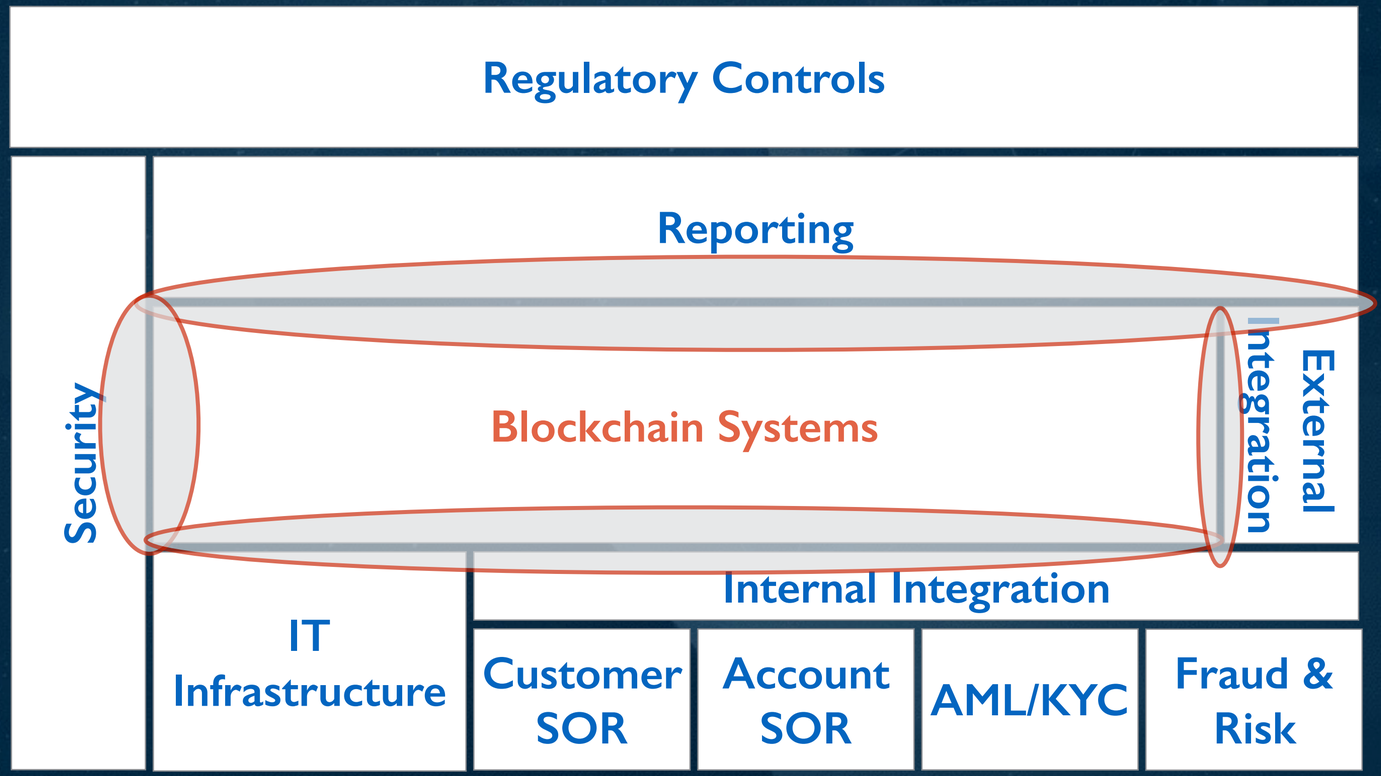
- Requires nodes that assemble blocks to post a bond
- Bond amount determines the value of transactions they can validate
- Bonded amount is returned only after some time from the last validation performed

Sufficiently secured blockchain networks operating between trusted parties may require less security than public, permissionless blockchain networks.

Blockchains Require Enterprise Integration



Integration Is Challenging



Key Questions When Evaluating Blockchain

1. Is blockchain the best technical solution or can this problem be solved more simply using traditional database technology?

2. Is the use case more transactional (e.g. money movement, securities settlement) or logical/contractual (e.g. trade finance, escrow)?

3. Is a permissioned or permissionless blockchain implementation better suited for the solution based on the security and consensus requirements?

4. With which systems must the blockchain integrate?

5. Based on the software selected, are there technical support and/or open source indemnification considerations?

7. If this is the first blockchain implementation in your institution, what strategies can be employed to limit risk?


THANK YOU