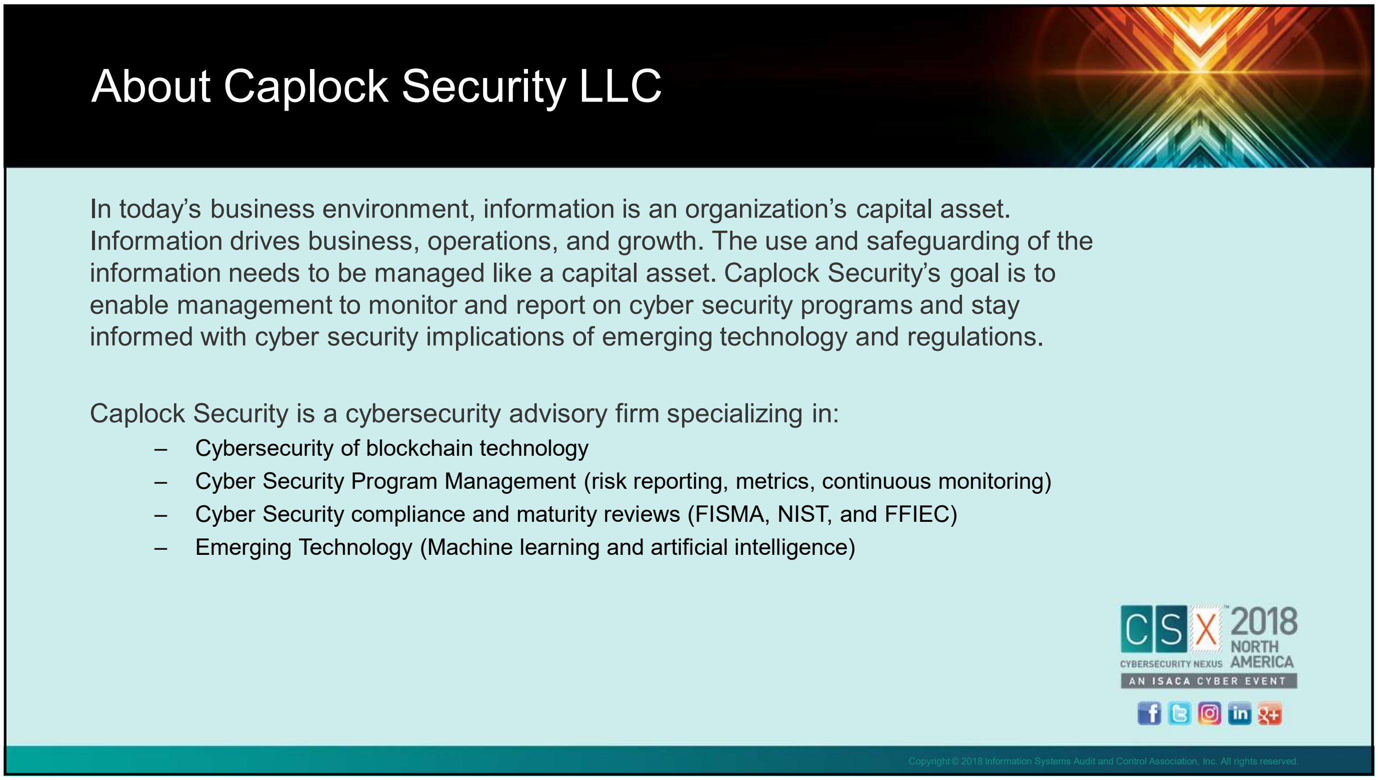
CSX 2018 NORTH AMERICA CYBERSECURITY NEXUS AN ISACA CYBER EVENT

Blockchain Technology: Beyond the Hype

Tuan Phan, CISSP, PMP, Security+, SSBB
Partner, Caplock Security LLC
tphan@caplocksecurity.com
Caplocksecurity.com
202-780-5455



About Caplock Security LLC

In today's business environment, information is an organization's capital asset. Information drives business, operations, and growth. The use and safeguarding of the information needs to be managed like a capital asset. Caplock Security's goal is to enable management to monitor and report on cyber security programs and stay informed with cyber security implications of emerging technology and regulations.

Caplock Security is a cybersecurity advisory firm specializing in:

- Cybersecurity of blockchain technology
- Cyber Security Program Management (risk reporting, metrics, continuous monitoring)
- Cyber Security compliance and maturity reviews (FISMA, NIST, and FFIEC)
- Emerging Technology (Machine learning and artificial intelligence)

CSX 2018 NORTH AMERICA CYBERSECURITY NEXUS AN ISACA CYBER EVENT

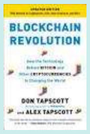
Agenda

- What is Blockchain?
- Use Cases
- The Flavors
- Key Elements
- Implications
- Pain & Gain
- Key Takeaways

- Hyperledger Fabric - Asset Exchange Demo

What is Blockchain?

Is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network.



BLOCKCHAIN REVOLUTION

DON TAPSCOTT and ALEX TAPSCOTT

Is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.

Is a distributed database that is continuously reconciled by participants.

Use Cases

Public Sector

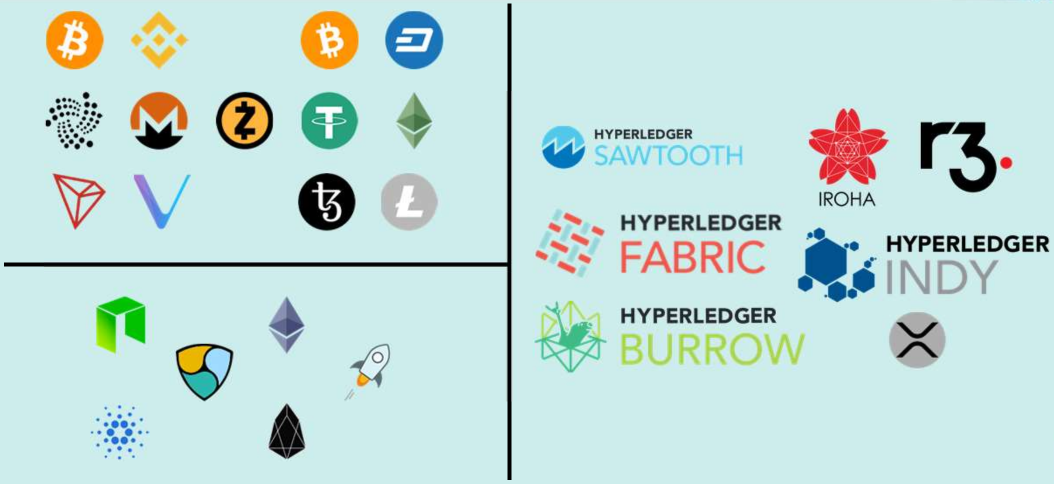
- Reduction of paperwork burdens and prevention of data errors
- Financial management and procurement
- IT asset and supply chain management and smart contracts
- Patents, Trademarks Copyrights, Royalties
- Government-issued credentials like visas, passports, SSN and birth certificates
- Federal personnel workforce data and appropriated funds
- Federal assistance and foreign aid delivery

Private Sector

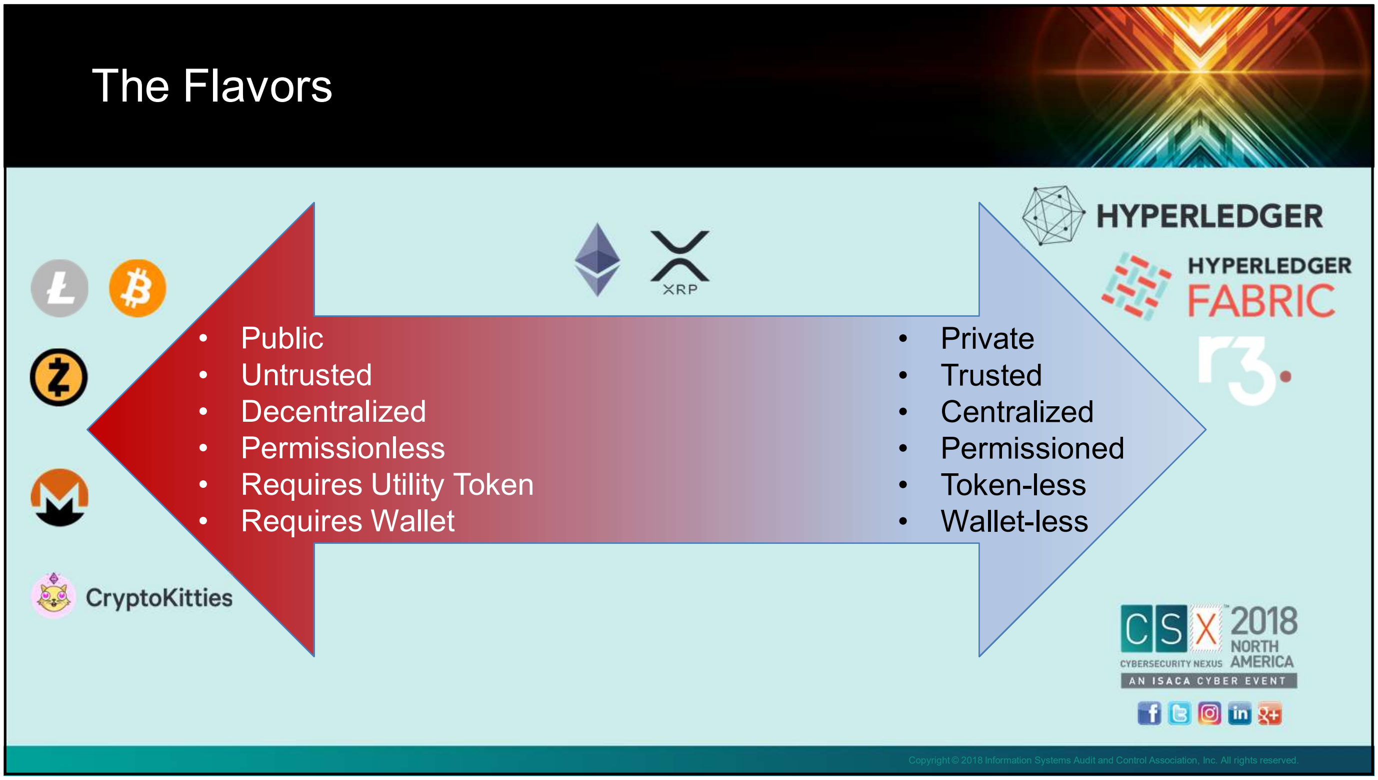
- Virtual currencies
- Digital identity
- Tokenization
- Accounting and auditing
- Smart contracting
- Inter-organizational data management
- Infrastructure for cross-border transactions
- Digital assets as a class
- Governance and markets
- Regulatory reporting and compliance
- Clearing and settlement

CSX 2018 NORTH AMERICA CYBERSECURITY NEXUS AN ISACA CYBER EVENT

Well-known Blockchain Platforms & Applications



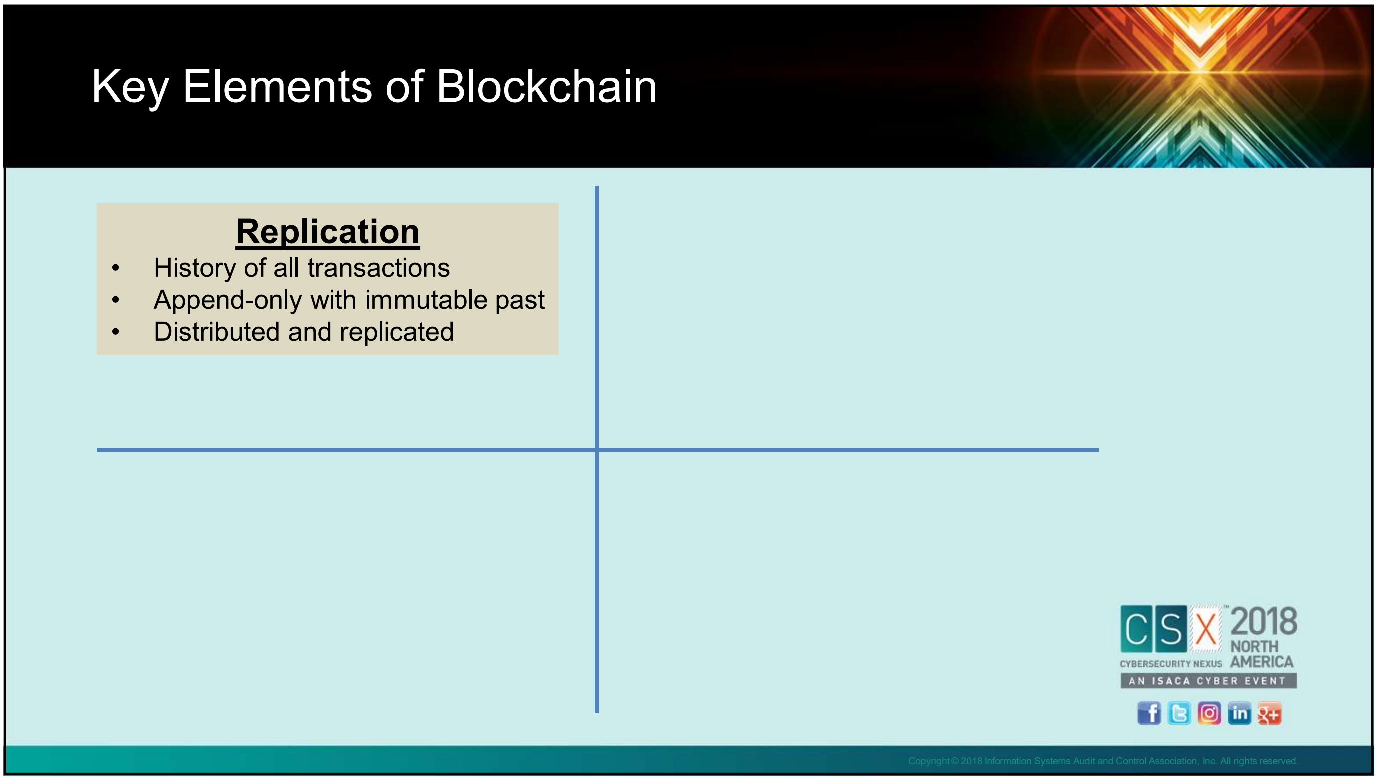
CSX 2018 NORTH AMERICA CYBERSECURITY NEXUS AN ISACA CYBER EVENT



The Flavors

- Public
- Untrusted
- Decentralized
- Permissionless
- Requires Utility Token
- Requires Wallet

- Private
- Trusted
- Centralized
- Permissioned
- Token-less
- Wallet-less



Key Elements of Blockchain

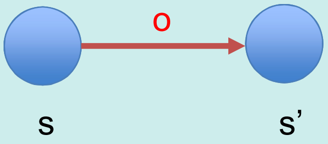
Replication

- History of all transactions
- Append-only with immutable past
- Distributed and replicated

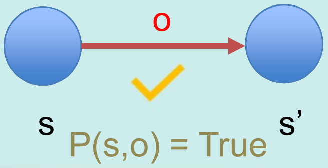
CSX 2018 NORTH AMERICA
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

State Machine

- Functionality F
  - Operation o transforms a state from s to s’

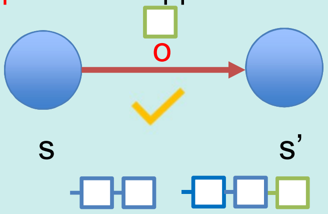


- Validation condition
  - Operation needs to be valid according to a predicate P()



Blockchain State Machine

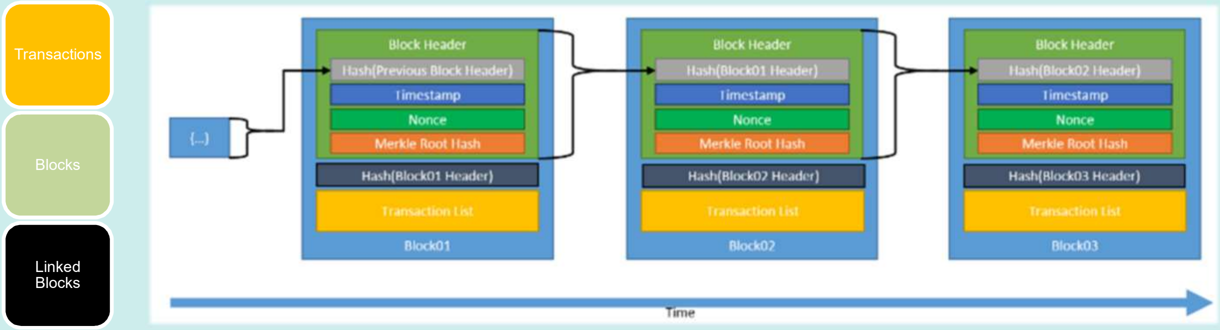
- Append-only log
  - Every operation o appends a block of valid transactions (tx) to the log



- Log content is verifiable from the most recent element

Blockchain State Machine (cont.)

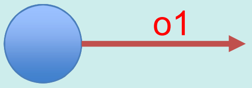
- Log entries form a hash chain over time



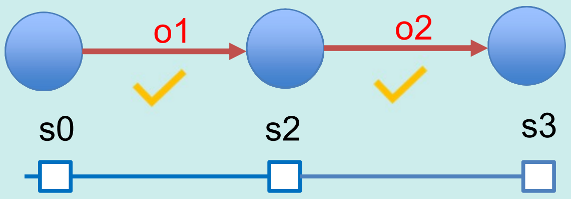
From NIST NISTIR 8202, Blockchain Technology Overview

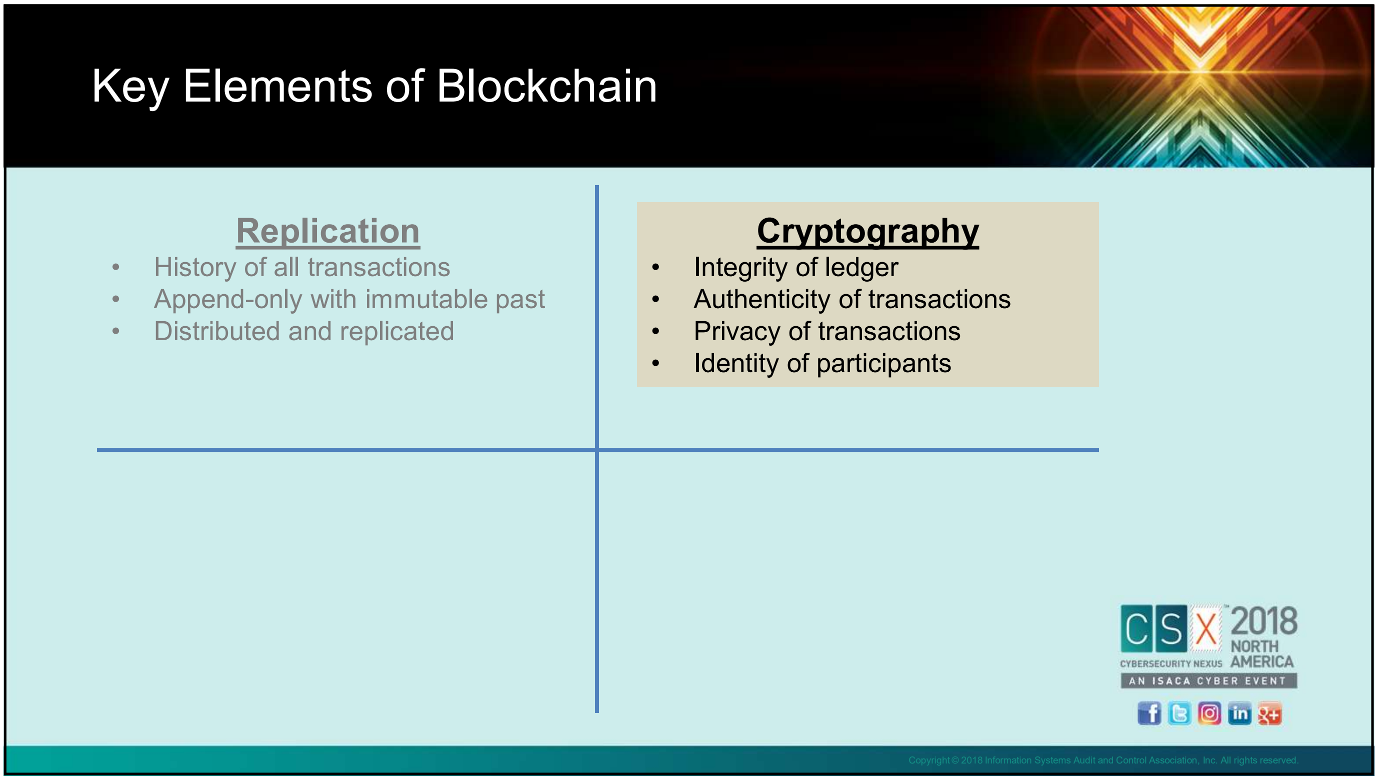
Distributed Blockchain Network

- Peer-to-peer distributed network
  - Nodes produce transactions



  - Nodes run a protocol to construct the ledger





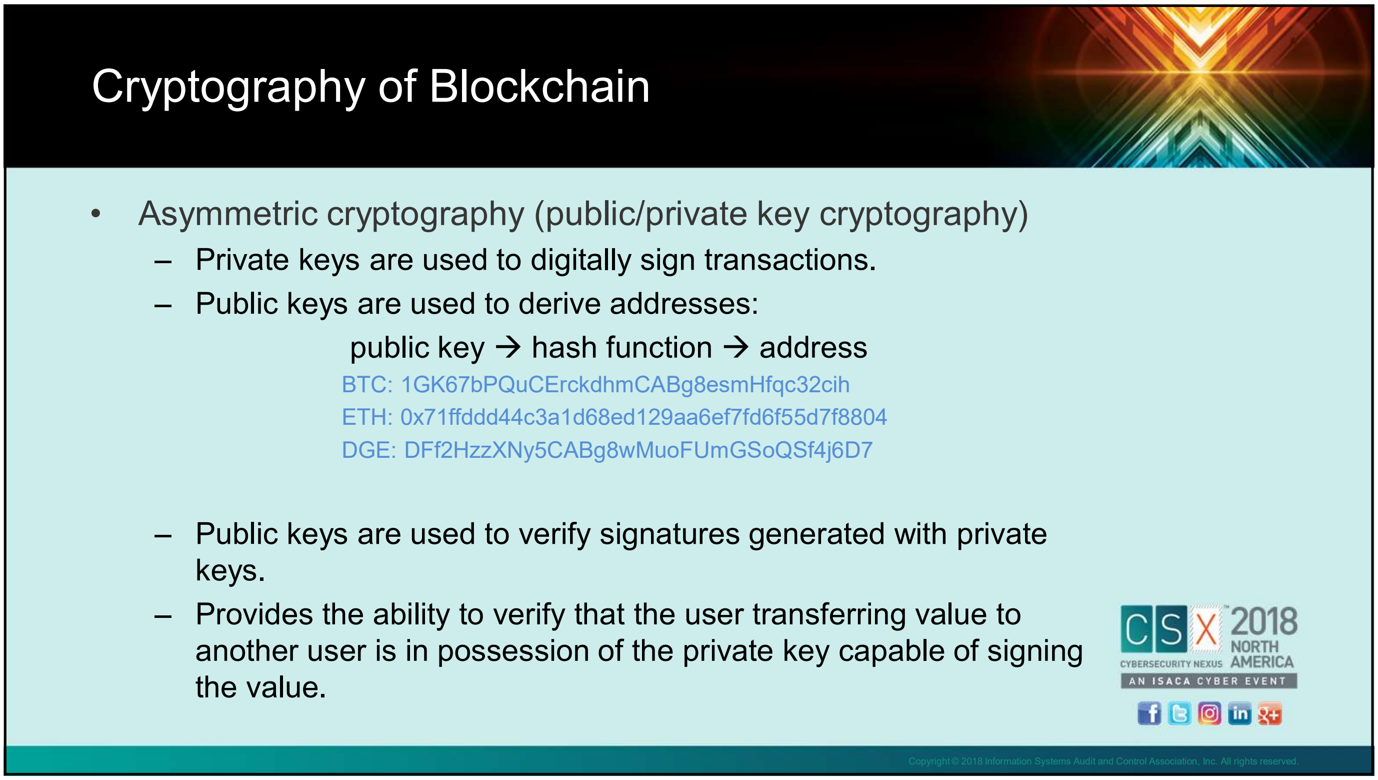
Key Elements of Blockchain

Replication

- History of all transactions
- Append-only with immutable past
- Distributed and replicated

Cryptography

- Integrity of ledger
- Authenticity of transactions
- Privacy of transactions
- Identity of participants



Cryptography of Blockchain

- Asymmetric cryptography (public/private key cryptography)
  - Private keys are used to digitally sign transactions.
  - Public keys are used to derive addresses:

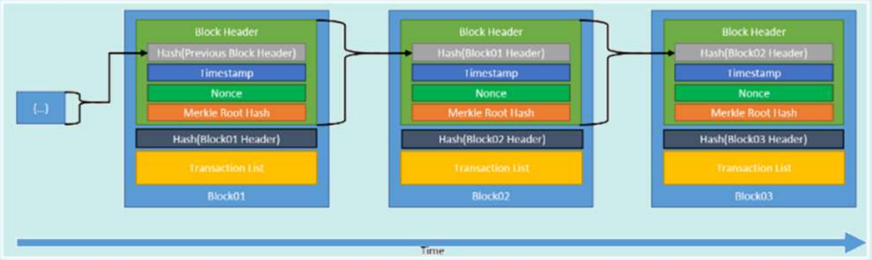
    public key → hash function → address

    BTC: 1GK67bPQuCErckdhmCABg8esmHfqc32cih
    ETH: 0x71ffddd44c3a1d68ed129aa6ef7fd6f55d7f8804
    DGE: DFf2HzzXNy5CABg8wMuoFUmGSoQSf4j6D7

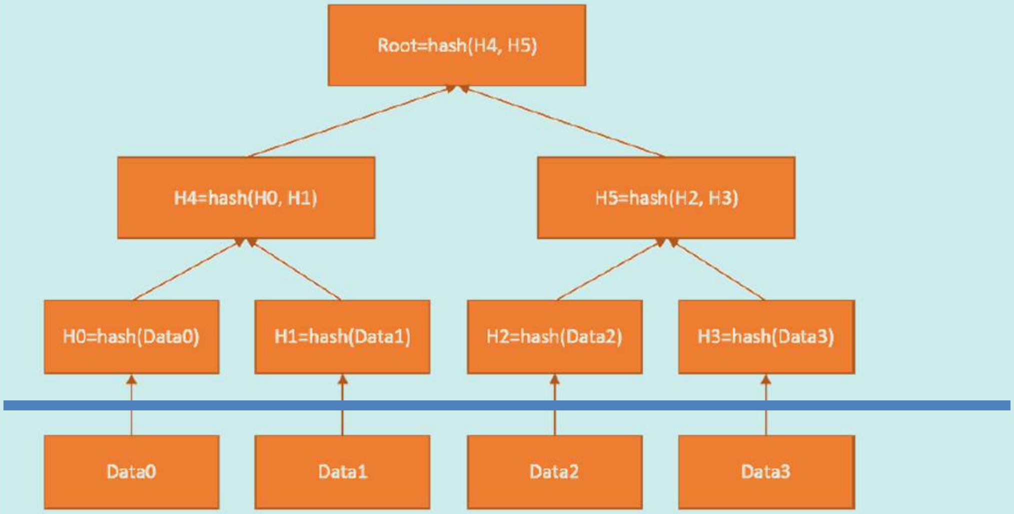
  - Public keys are used to verify signatures generated with private keys.
  - Provides the ability to verify that the user transferring value to another user is in possession of the private key capable of signing the value.

Cryptography of Blockchain (cont.)

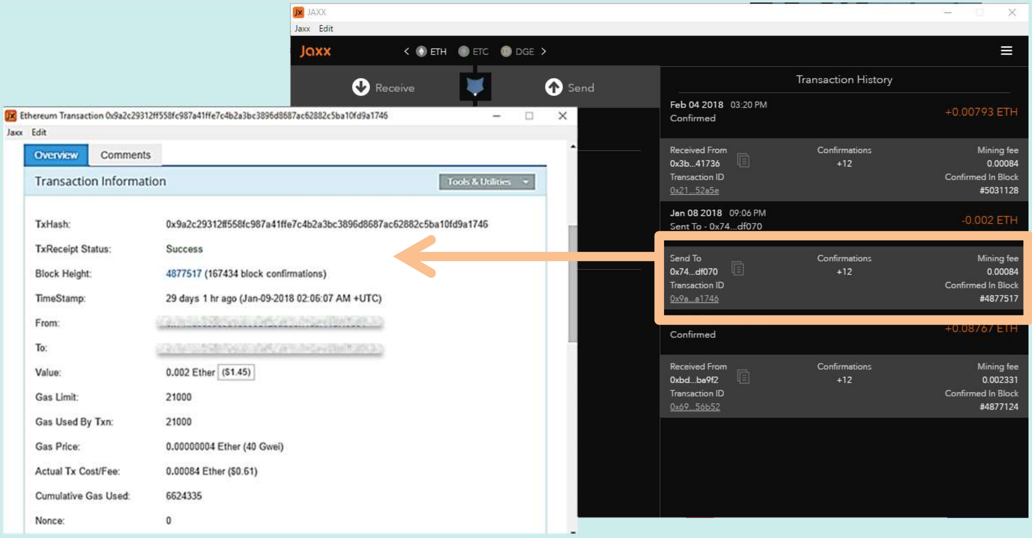
- Chaining blocks
  - Hash algorithms utilized vary with blockchain platforms:
    - SHA-256 (Bitcoin), Keccak-256 (Ethereum), Scrypt (Litecoin)
  - Are chained together where each block containing the hash of the previous block's header and is then broadcast to all nodes in the network.



Merkel Tree



Sample Transactions



Transaction History

Feb 04 2018 03:20 PM
Confirmed
+0.00793 ETH

Received From 0x3b...41736 | Confirmations +12 | Mining fee 0.00084
Transaction ID 0x21...52a5e | Confirmed In Block #5031128

Jan 08 2018 09:06 PM
Sent To - 0x74...df070
-0.002 ETH

Send To 0x74...df070 | Confirmations +12 | Mining fee 0.00084
Transaction ID 0x9a...a1746 | Confirmed In Block #4877517

Confirmed
+0.08767 ETH

Received From 0xbd...ba9f2 | Confirmations +12 | Mining fee 0.002331
Transaction ID 0x69...56b52 | Confirmed In Block #4877124

Ethereum Transaction 0x9a2c29312ff558fc987a41ffe7c4b2a3bc3896d8687ac62882c5ba10fd9a1746

Transaction Information

TxHash:	0x9a2c29312ff558fc987a41ffe7c4b2a3bc3896d8687ac62882c5ba10fd9a1746
TxReceipt Status:	Success
Block Height:	4877517 (167434 block confirmations)
TimeStamp:	29 days 1 hr ago (Jan-09-2018 02:06:07 AM +UTC)
From:	[redacted]
To:	[redacted]
Value:	0.002 Ether ($1.45)
Gas Limit:	21000
Gas Used By Txn:	21000
Gas Price:	0.00000004 Ether (40 Gwei)
Actual Tx Cost/Fee:	0.00084 Ether ($0.61)
Cumulative Gas Used:	6624335
Nonce:	0

Key Elements of Blockchain

Replication

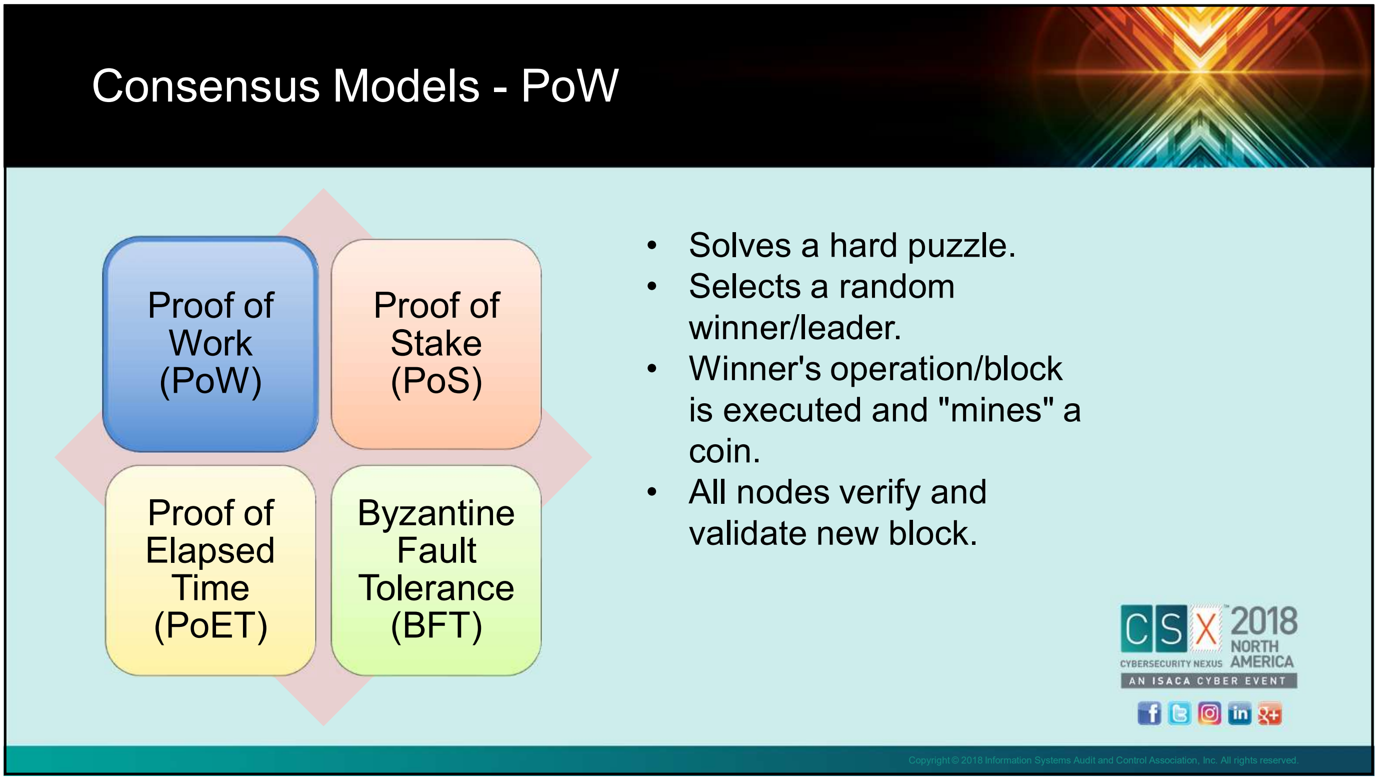
- History of all transactions
- Append-only with immutable past
- Distributed and replicated

Cryptography

- Integrity of ledger
- Authenticity of transactions
- Privacy of transactions
- Identity of participants

Consensus

- Consensus protocol
- Shared control tolerating disruption
- Transactions validated



Consensus Models - PoW

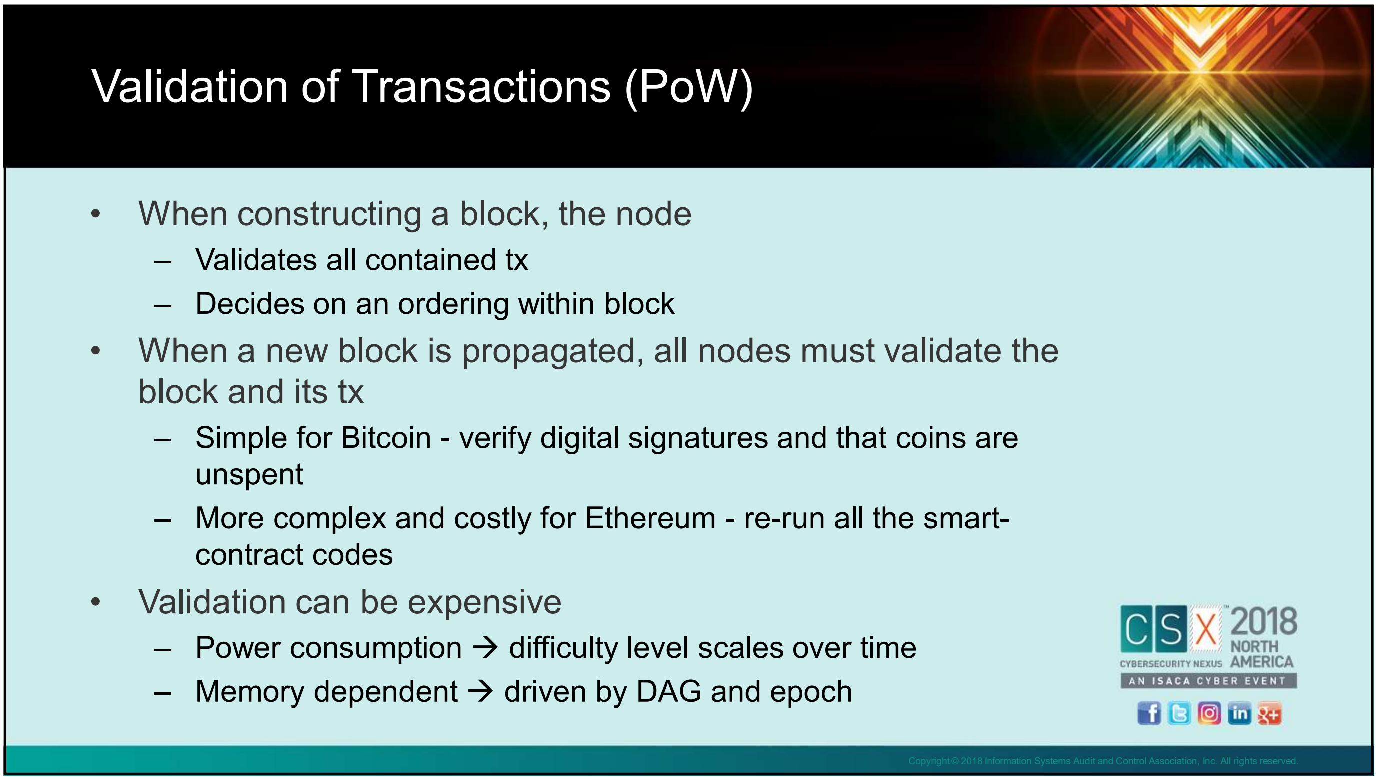
Proof of Work (PoW)

Proof of Stake (PoS)

Proof of Elapsed Time (PoET)

Byzantine Fault Tolerance (BFT)

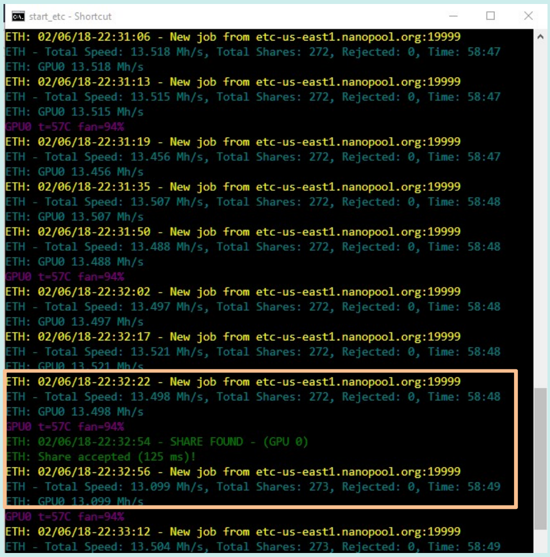
- Solves a hard puzzle.
- Selects a random winner/leader.
- Winner's operation/block is executed and "mines" a coin.
- All nodes verify and validate new block.



Validation of Transactions (PoW)

- When constructing a block, the node
  - Validates all contained tx
  - Decides on an ordering within block
- When a new block is propagated, all nodes must validate the block and its tx
  - Simple for Bitcoin - verify digital signatures and that coins are unspent
  - More complex and costly for Ethereum - re-run all the smart-contract codes
- Validation can be expensive
  - Power consumption → difficulty level scales over time
  - Memory dependent → driven by DAG and epoch

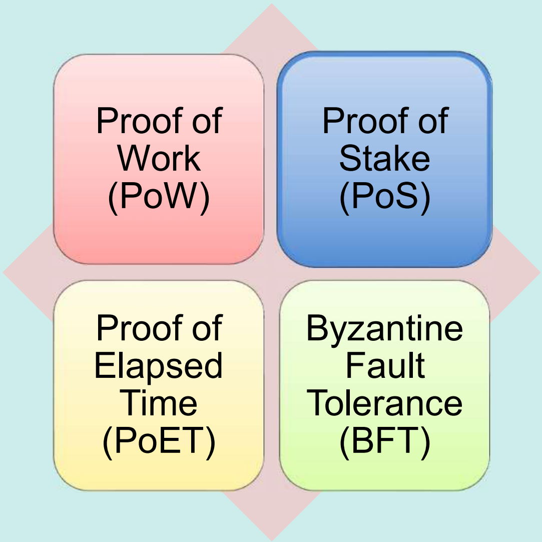
Mining Operation



```
ETH: 02/06/18-22:31:06 - New job from etc-us-east1.nanopool.org:19999
ETH - Total Speed: 13.518 Mh/s, Total Shares: 272, Rejected: 0, Time: 58:47
ETH: GPU0 13.518 Mh/s
ETH: 02/06/18-22:31:13 - New job from etc-us-east1.nanopool.org:19999
ETH - Total Speed: 13.515 Mh/s, Total Shares: 272, Rejected: 0, Time: 58:47
ETH: GPU0 13.515 Mh/s
GPU0 t=57C fan=94%
ETH: 02/06/18-22:31:19 - New job from etc-us-east1.nanopool.org:19999
ETH - Total Speed: 13.456 Mh/s, Total Shares: 272, Rejected: 0, Time: 58:47
ETH: GPU0 13.456 Mh/s
ETH: 02/06/18-22:31:35 - New job from etc-us-east1.nanopool.org:19999
ETH - Total Speed: 13.507 Mh/s, Total Shares: 272, Rejected: 0, Time: 58:48
ETH: GPU0 13.507 Mh/s
ETH: 02/06/18-22:31:50 - New job from etc-us-east1.nanopool.org:19999
ETH - Total Speed: 13.488 Mh/s, Total Shares: 272, Rejected: 0, Time: 58:48
ETH: GPU0 13.488 Mh/s
GPU0 t=57C fan=94%
ETH: 02/06/18-22:32:02 - New job from etc-us-east1.nanopool.org:19999
ETH - Total Speed: 13.497 Mh/s, Total Shares: 272, Rejected: 0, Time: 58:48
ETH: GPU0 13.497 Mh/s
ETH: 02/06/18-22:32:17 - New job from etc-us-east1.nanopool.org:19999
ETH - Total Speed: 13.521 Mh/s, Total Shares: 272, Rejected: 0, Time: 58:48
ETH: GPU0 13.521 Mh/s
ETH: 02/06/18-22:32:22 - New job from etc-us-east1.nanopool.org:19999
ETH - Total Speed: 13.498 Mh/s, Total Shares: 272, Rejected: 0, Time: 58:48
ETH: GPU0 13.498 Mh/s
GPU0 t=57C fan=94%
ETH: 02/06/18-22:32:54 - SHARE FOUND - (GPU 0)
ETH: Share accepted (125 ms)!
ETH: 02/06/18-22:32:56 - New job from etc-us-east1.nanopool.org:19999
ETH - Total Speed: 13.099 Mh/s, Total Shares: 273, Rejected: 0, Time: 58:49
ETH: GPU0 13.099 Mh/s
GPU0 t=57C fan=94%
ETH: 02/06/18-22:33:12 - New job from etc-us-east1.nanopool.org:19999
ETH - Total Speed: 13.504 Mh/s, Total Shares: 273, Rejected: 0, Time: 58:49
```

- It is a collective effort where many workers, in a collective (i.e. the mining pool), contribute processing power to solve a PoW.
- A share is rewarded to each worker for any solved participation.
- If the pool wins the publishing of the block, the block reward is proportionally distributed to all workers participated in the round based on their shares and round difficulty.

Consensus Models - PoS



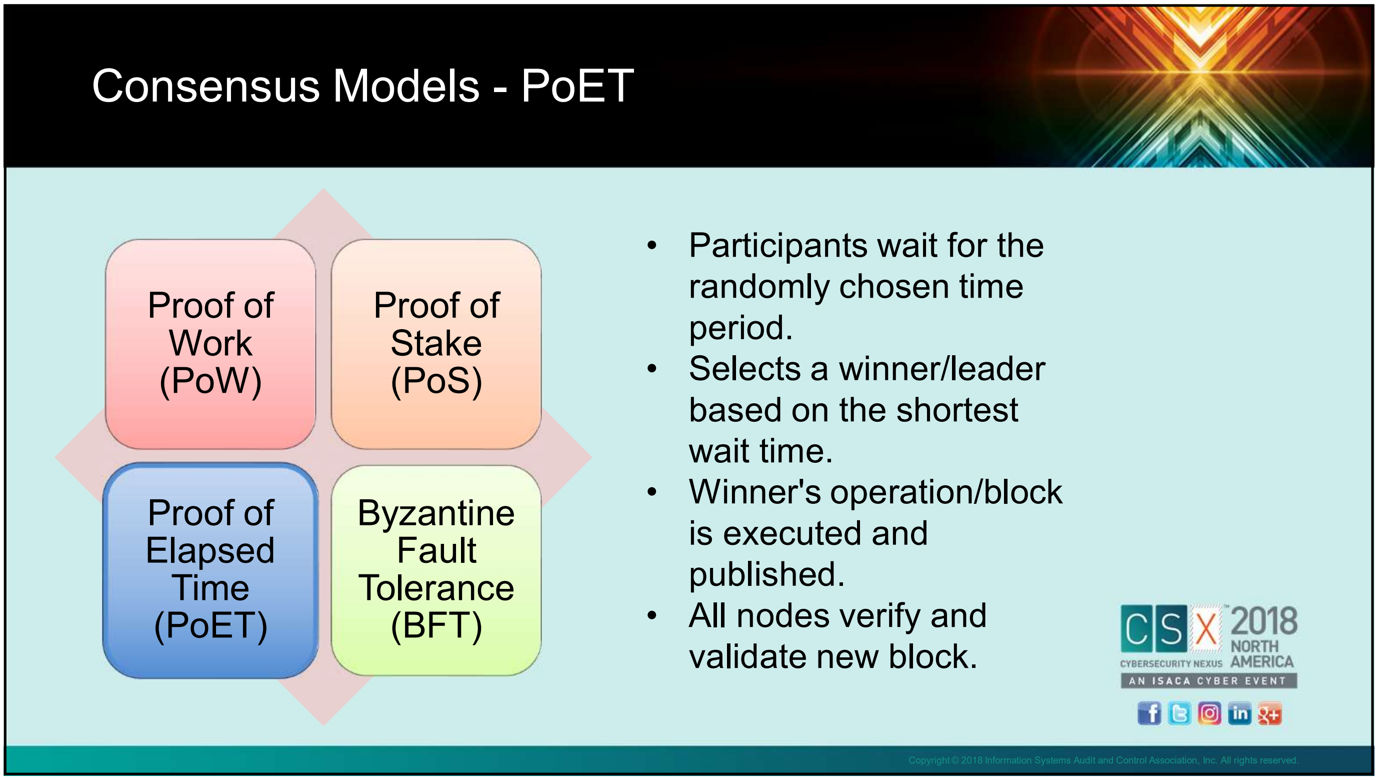
Proof of Work (PoW)

Proof of Stake (PoS)

Proof of Elapsed Time (PoET)

Byzantine Fault Tolerance (BFT)

- Participants gain the right to “mine” based on the stake deposited.
- Selects a winner/leader.
- Winner's operation/block is executed and published.
- All nodes verify and validate new block.



Consensus Models - PoET

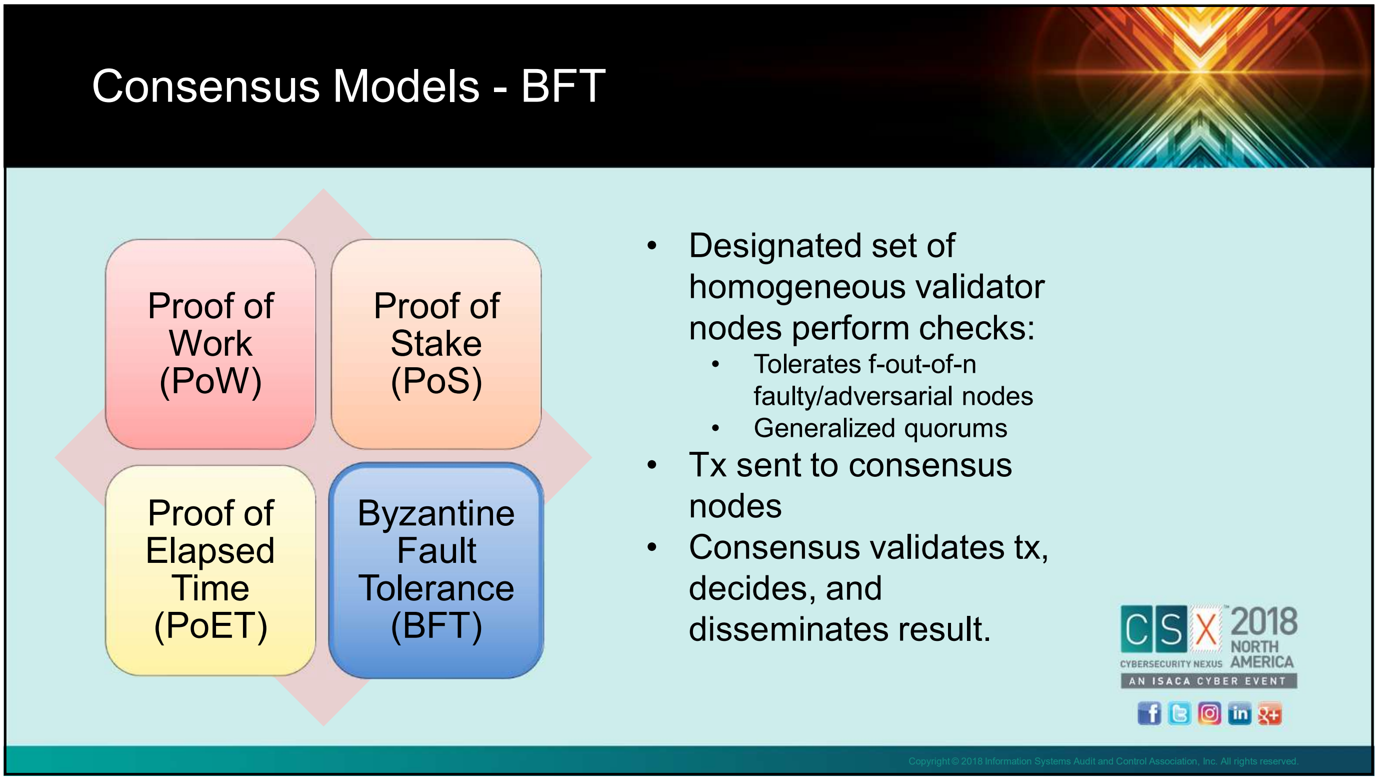
Proof of Work (PoW)

Proof of Stake (PoS)

Proof of Elapsed Time (PoET)

Byzantine Fault Tolerance (BFT)

- Participants wait for the randomly chosen time period.
- Selects a winner/leader based on the shortest wait time.
- Winner's operation/block is executed and published.
- All nodes verify and validate new block.



Consensus Models - BFT

Proof of Work (PoW)

Proof of Stake (PoS)

Proof of Elapsed Time (PoET)

Byzantine Fault Tolerance (BFT)

- Designated set of homogeneous validator nodes perform checks:
  - Tolerates f-out-of-n faulty/adversarial nodes
  - Generalized quorums
- Tx sent to consensus nodes
- Consensus validates tx, decides, and disseminates result.

Key Elements of Blockchain

Replication

- History of all transactions
- Append-only with immutable past
- Distributed and replicated

Cryptography

- Integrity of ledger
- Authenticity of transactions
- Privacy of transactions
- Identity of participants

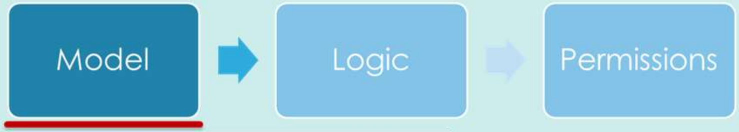
Consensus

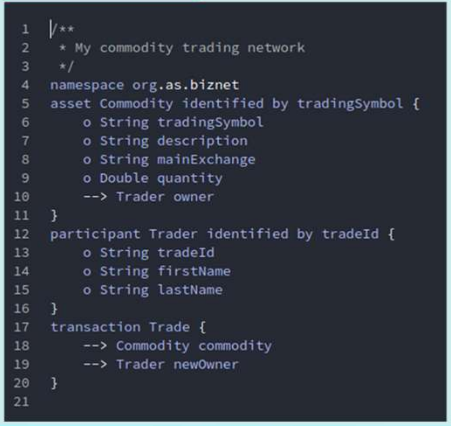
- Consensus protocol
- Shared control tolerating disruption
- Transactions validated

Business Logic

- Logic embedded in the ledger
- Executed together with transactions
- From simple “coins” to self-enforcing “smart contracts”

Typical Business Network





```
/**
 * My commodity trading network
 */
namespace org.as.biznet
asset Commodity identified by tradingSymbol {
    o String tradingSymbol
    o String description
    o String mainExchange
    o Double quantity
    --> Trader owner
}
participant Trader identified by tradeId {
    o String tradeId
    o String firstName
    o String lastName
}
transaction Trade {
    --> Commodity commodity
    --> Trader newOwner
}
```

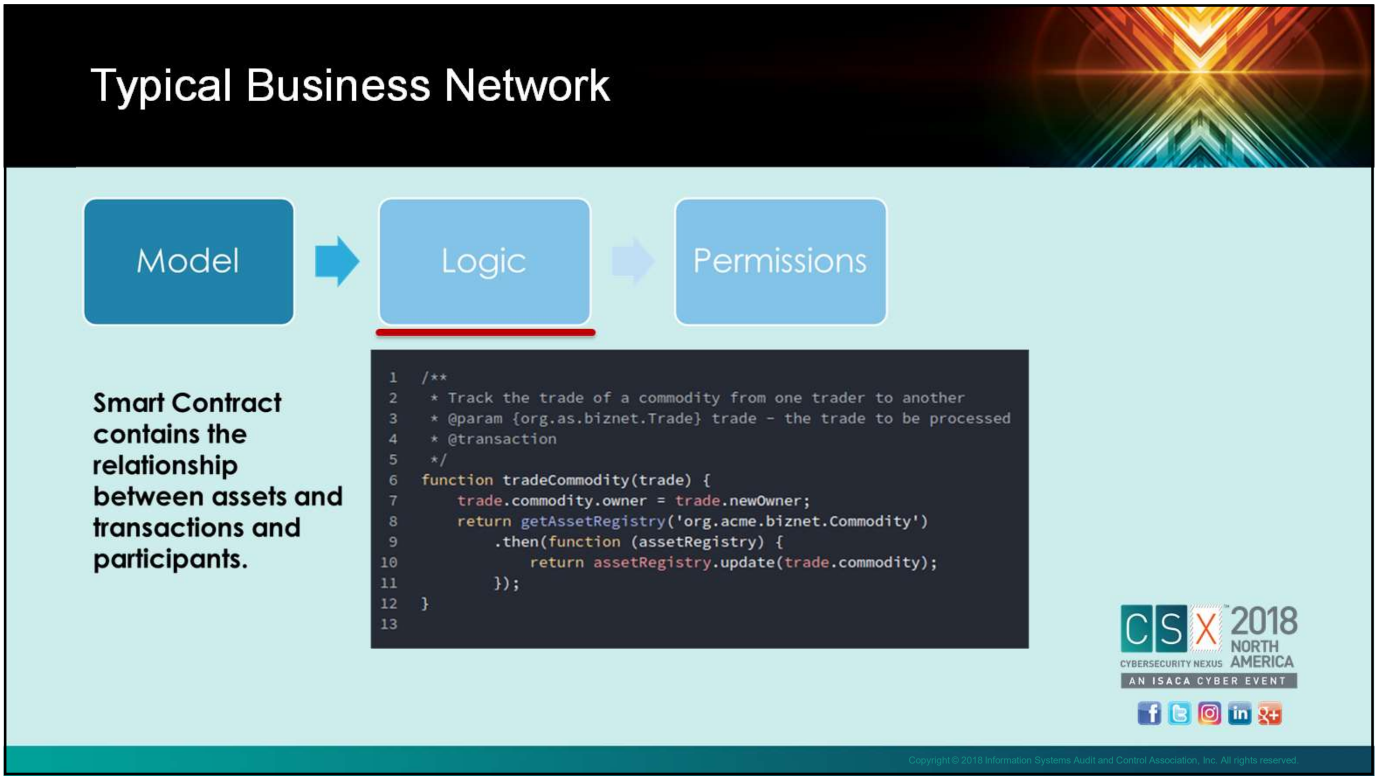
Asset

Participant

Transaction

Event

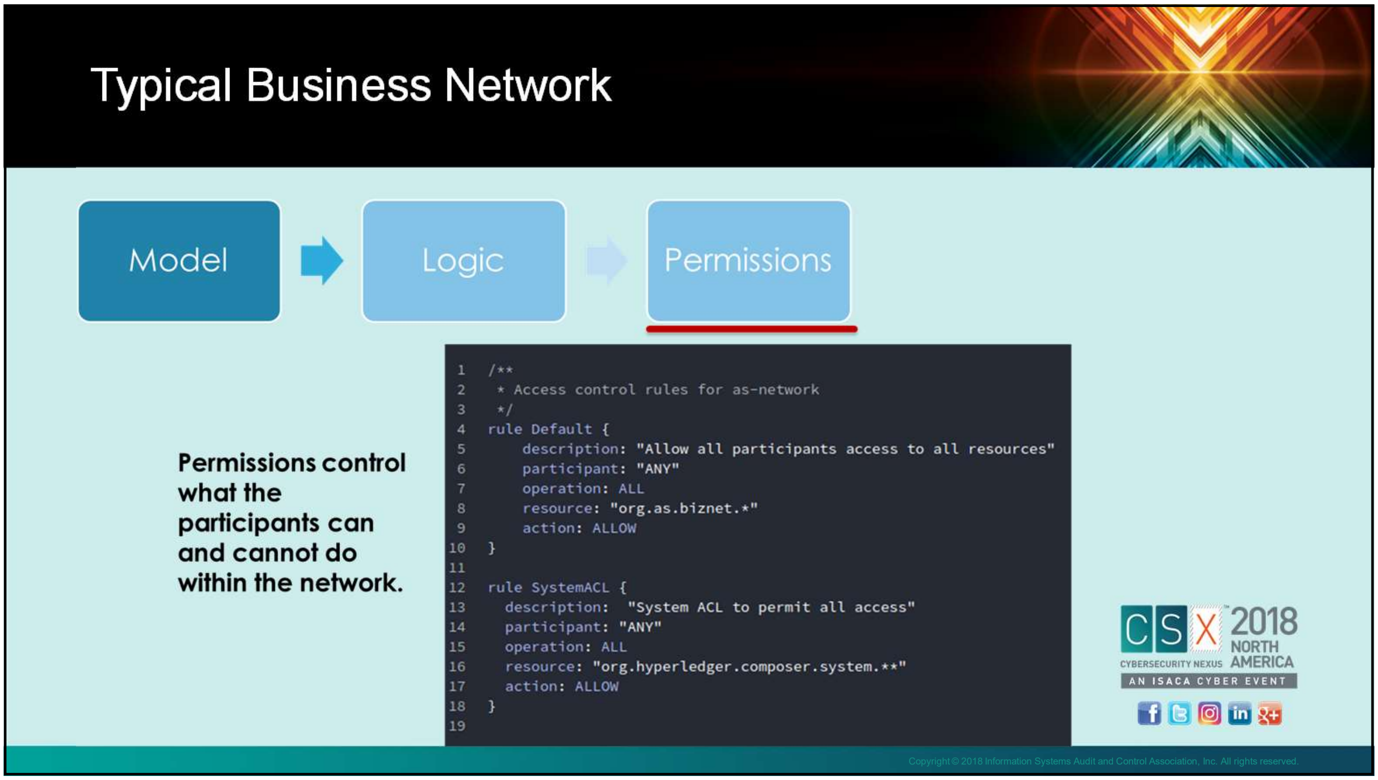
Query (reporting)



Typical Business Network

Smart Contract contains the relationship between assets and transactions and participants.

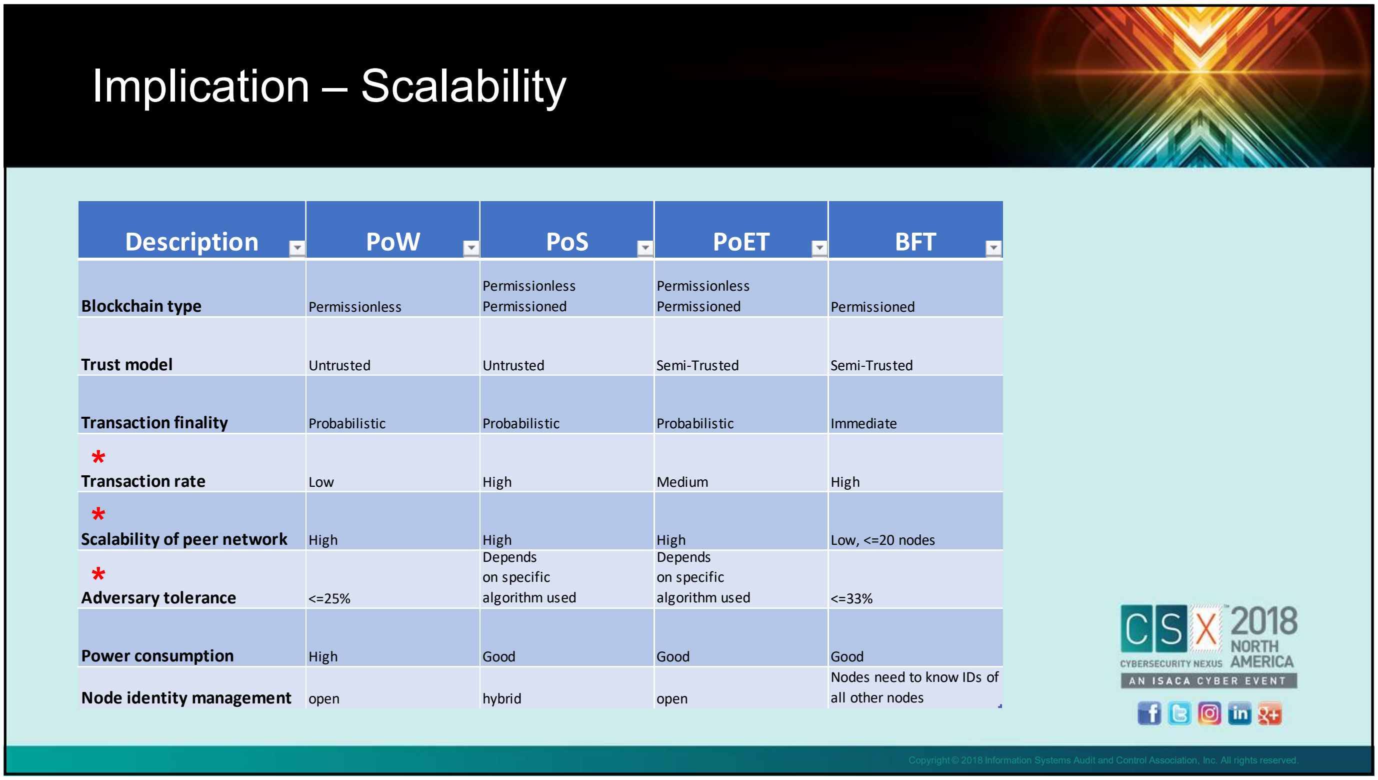
```
/**
 * Track the trade of a commodity from one trader to another
 * @param {org.as.biznet.Trade} trade - the trade to be processed
 * @transaction
 */
function tradeCommodity(trade) {
    trade.commodity.owner = trade.newOwner;
    return getAssetRegistry('org.acme.biznet.Commodity')
        .then(function (assetRegistry) {
            return assetRegistry.update(trade.commodity);
        });
}
```



Typical Business Network

Permissions control what the participants can and cannot do within the network.

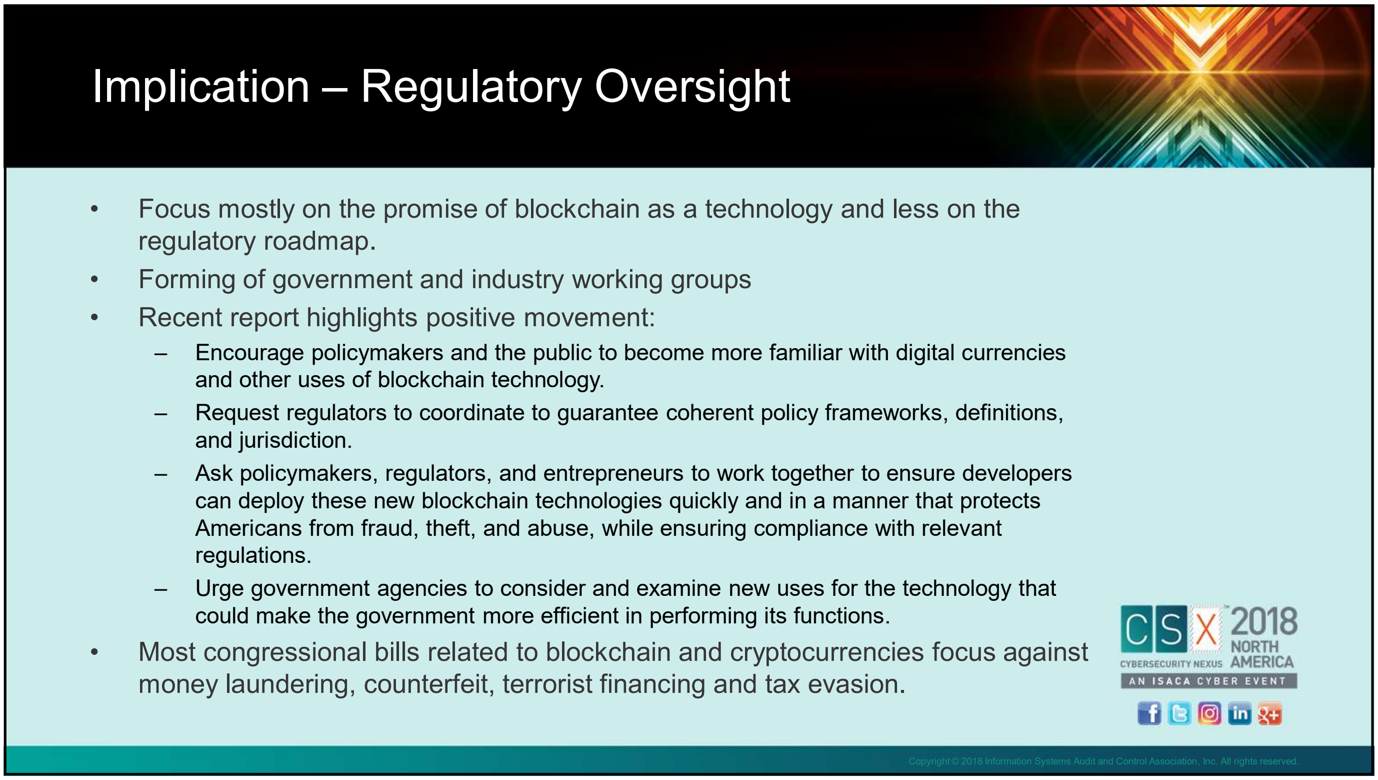
```
/**
 * Access control rules for as-network
 */
rule Default {
    description: "Allow all participants access to all resources"
    participant: "ANY"
    operation: ALL
    resource: "org.as.biznet.*"
    action: ALLOW
}

rule SystemACL {
  description:  "System ACL to permit all access"
  participant: "ANY"
  operation: ALL
  resource: "org.hyperledger.composer.system.**"
  action: ALLOW
}
```



Implication – Scalability

Description	PoW	PoS	PoET	BFT
Blockchain type	Permissionless	Permissionless Permissioned	Permissionless Permissioned	Permissioned
Trust model	Untrusted	Untrusted	Semi-Trusted	Semi-Trusted
Transaction finality	Probabilistic	Probabilistic	Probabilistic	Immediate
* Transaction rate	Low	High	Medium	High
* Scalability of peer network	High	High	High	Low, <=20 nodes
* Adversary tolerance	<=25%	Depends on specific algorithm used	Depends on specific algorithm used	<=33%
Power consumption	High	Good	Good	Good
Node identity management	open	hybrid	open	Nodes need to know IDs of all other nodes

CSX 2018 NORTH AMERICA CYBERSECURITY NEXUS AN ISACA CYBER EVENT

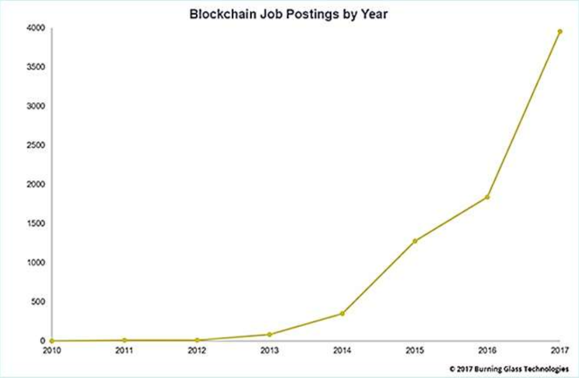


Implication – Regulatory Oversight

- Focus mostly on the promise of blockchain as a technology and less on the regulatory roadmap.
- Forming of government and industry working groups
- Recent report highlights positive movement:
  - Encourage policymakers and the public to become more familiar with digital currencies and other uses of blockchain technology.
  - Request regulators to coordinate to guarantee coherent policy frameworks, definitions, and jurisdiction.
  - Ask policymakers, regulators, and entrepreneurs to work together to ensure developers can deploy these new blockchain technologies quickly and in a manner that protects Americans from fraud, theft, and abuse, while ensuring compliance with relevant regulations.
  - Urge government agencies to consider and examine new uses for the technology that could make the government more efficient in performing its functions.
- Most congressional bills related to blockchain and cryptocurrencies focus against money laundering, counterfeit, terrorist financing and tax evasion.

CSX 2018 NORTH AMERICA CYBERSECURITY NEXUS AN ISACA CYBER EVENT

Implication – Expertise



© 2017 Burning Glass Technologies

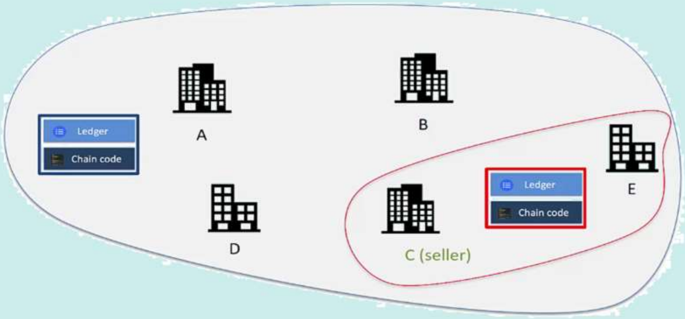
- Talents are hard to find.
  - Consultants
  - Developers (front and backend)
  - Testers/Quality assurance
  - Few core developers maintain the development of the platform.
- Skills are more specialized.
- Be prepared to pay and compete on offers to candidates.

Implication – Security and Privacy

- The design and access control play crucial roles in reducing the threats to the network.
- Public blockchain are prone to 51%(majority), and Race/Finney attacks (exploit latency).
- Well-defined business processes to map/model into smart contracts.
- Smart contracts are buggy!
  - 34,200 out of 1 million (3%) smart contracts have some forms of trace vulnerabilities based on MAIAN. [Parity bug ~ $300M]
  - Review of Ethereum smart contract indicated bugs per line of code exceeds 100 per 1000 lines, or 2X to 6X the industry average.
    - Security flaws → loss of money or control possible for users or owners.
    - Doesn't do what it claims, either in the description or code comments.
- Secure coding practice, testing and code maintenance

Implication – Security and Privacy

- Key management
- Validation of transactions
- Rollback of transactions
- Data privacy



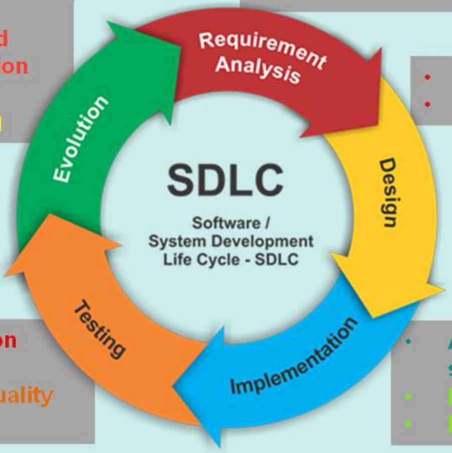
CSX 2018 NORTH AMERICA
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Pain & Gain

- Identify accurate use cases
- Map business processes into smart contracts

- Training/sustaining staff and skillsets
- Conduct initial and ongoing certification
- Perform periodic monitoring/testing

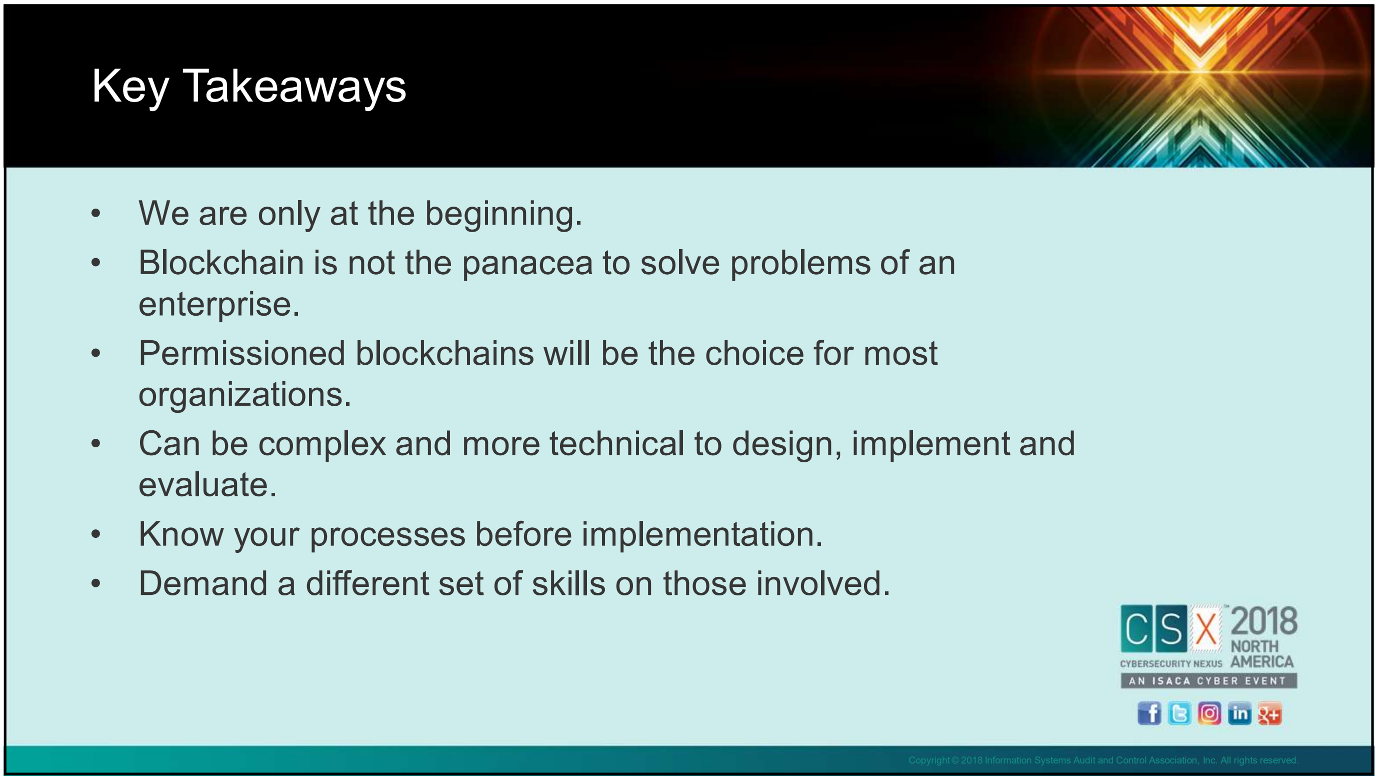
- Develop applications
- Code maintenance



- Verify implementation correctness
- Conduct UAT and quality assurance

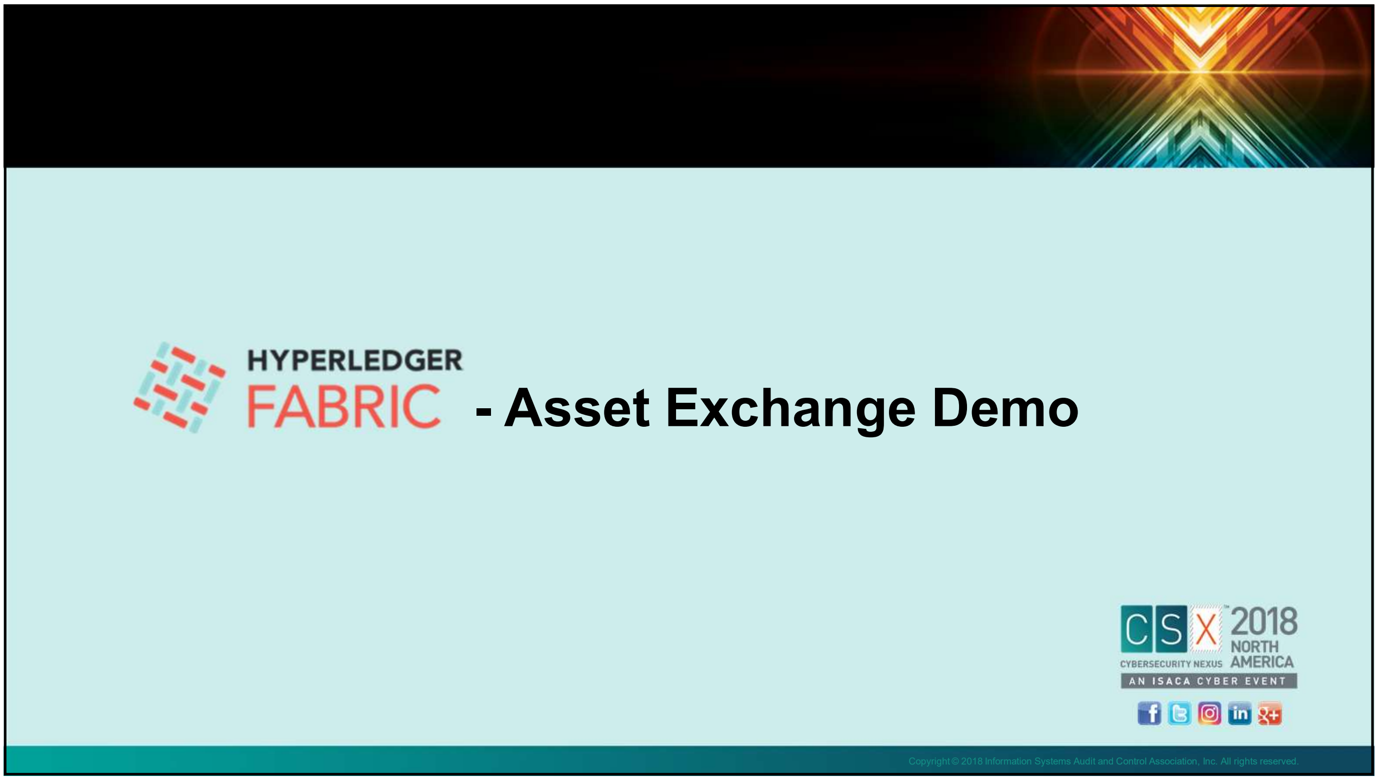
- Automate and streamline operations
- Reduce costs
- Improve revenues

CSX 2018 NORTH AMERICA
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT



Key Takeaways

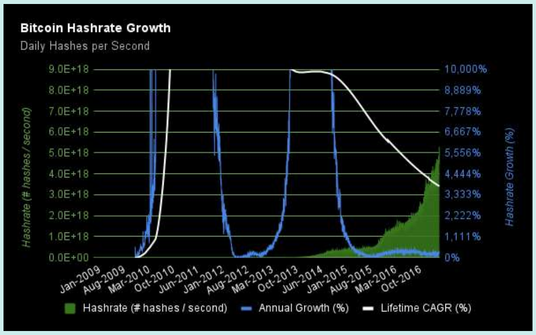
- We are only at the beginning.
- Blockchain is not the panacea to solve problems of an enterprise.
- Permissioned blockchains will be the choice for most organizations.
- Can be complex and more technical to design, implement and evaluate.
- Know your processes before implementation.
- Demand a different set of skills on those involved.



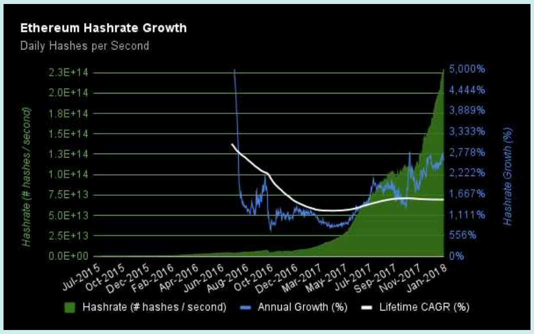
HYPERLEDGER FABRIC - Asset Exchange Demo

Backup Slides

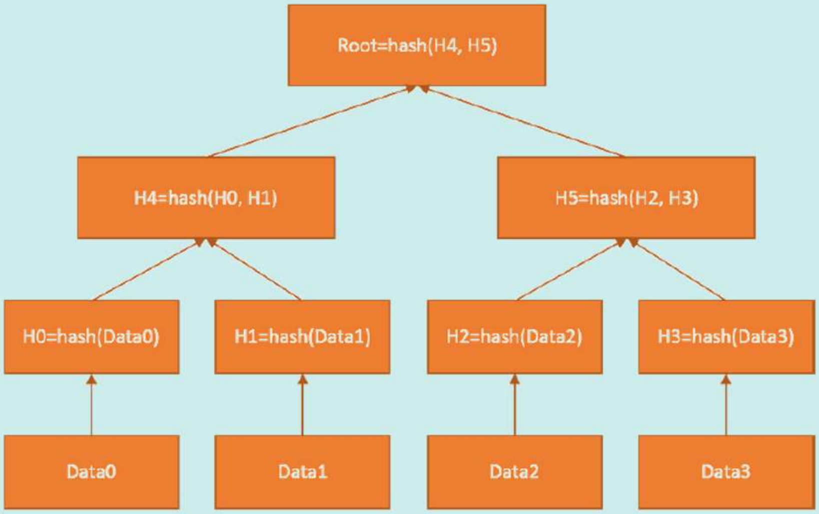
Hash Rate



- *Green area: Chain's hashing power (number of hashes per second);*
- *Blue line: Annual % change in chain's hashing power;*
- *White line: Compounded, annual % change in hashing power over life of chain.*



Merkle Tree



Root=hash(H4, H5)

H4=hash(H0, H1)

H5=hash(H2, H3)

H0=hash(Data0)

H1=hash(Data1)

H2=hash(Data2)

H3=hash(Data3)

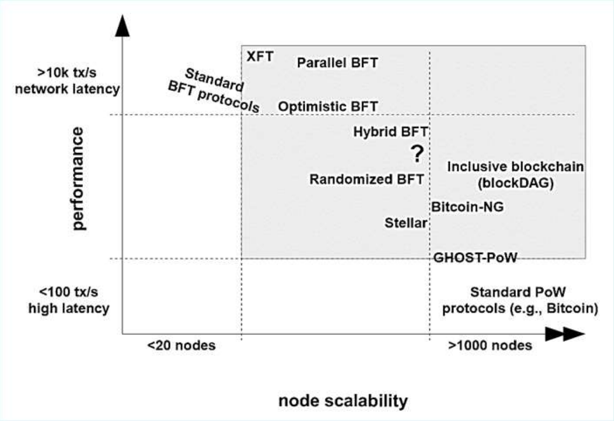
Data0

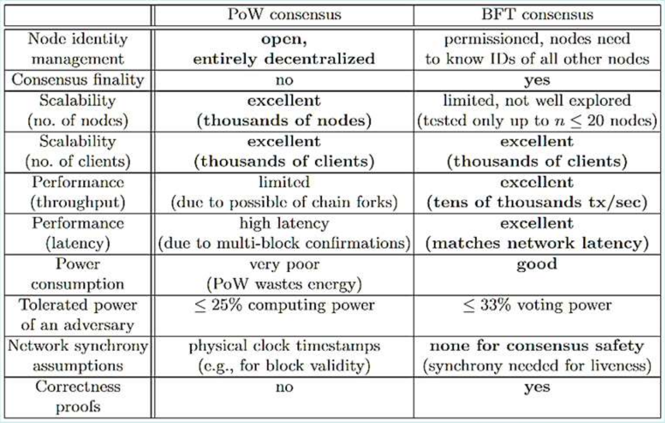
Data1

Data2

Data3

Implication – Scalability

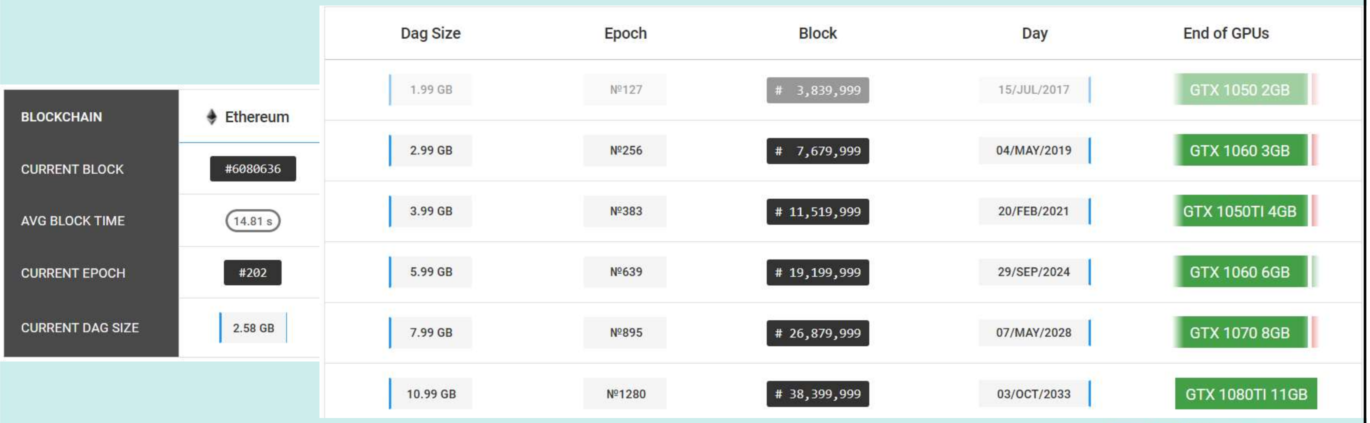




	PoW consensus	BFT consensus
Node identity management	**open, entirely decentralized**	permissioned, nodes need to know IDs of all other nodes
Consensus finality	no	**yes**
Scalability (no. of nodes)	**excellent (thousands of nodes)**	limited, not well explored (tested only up to $n \leq 20$ nodes)
Scalability (no. of clients)	**excellent (thousands of clients)**	**excellent (thousands of clients)**
Performance (throughput)	limited (due to possible of chain forks)	**excellent (tens of thousands tx/sec)**
Performance (latency)	high latency (due to multi-block confirmations)	**excellent (matches network latency)**
Power consumption	very poor (PoW wastes energy)	**good**
Tolerated power of an adversary	$\leq 25\%$ computing power	$\leq 33\%$ voting power
Network synchrony assumptions	physical clock timestamps (e.g., for block validity)	**none for consensus safety** (synchrony needed for liveness)
Correctness proofs	no	**yes**

M. Vukolic: The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication, IBM Research.

DAG and Block Size

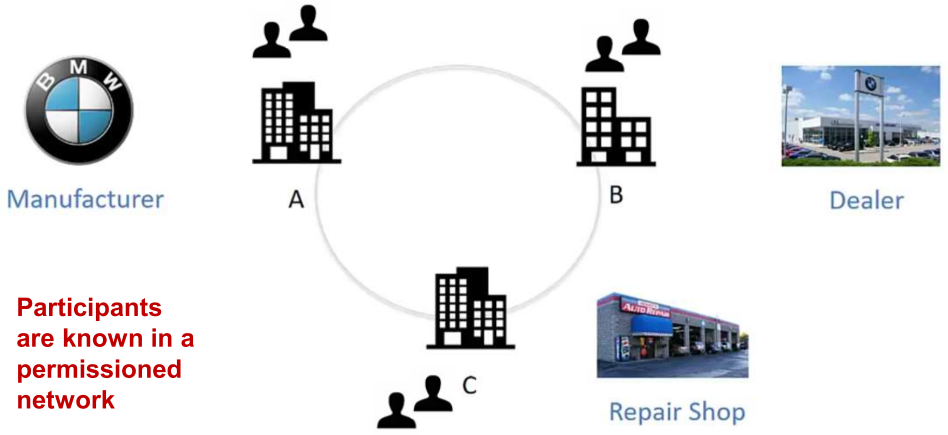


BLOCKCHAIN	Ethereum
CURRENT BLOCK	#6080636
AVG BLOCK TIME	14.81 s
CURRENT EPOCH	#202
CURRENT DAG SIZE	2.58 GB

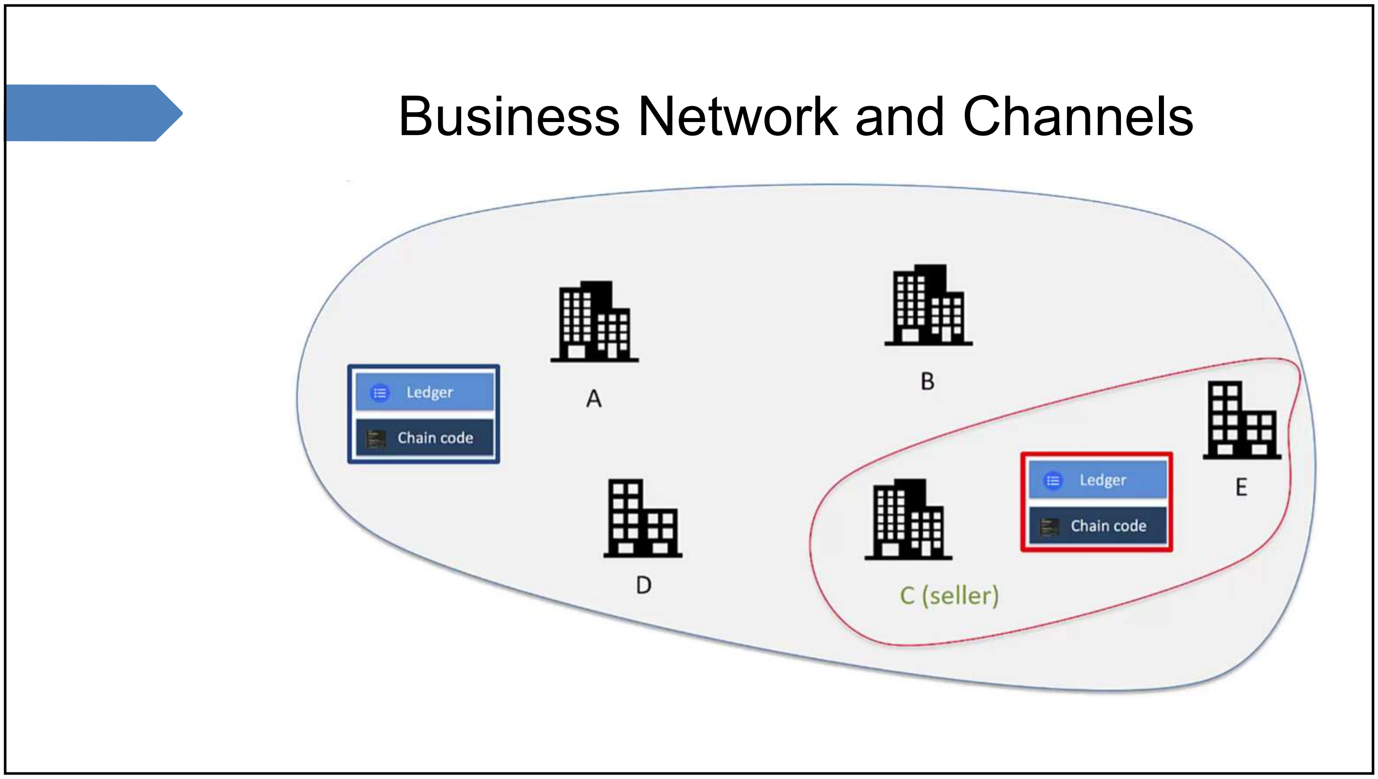
Dag Size	Epoch	Block	Day	End of GPUs
1.99 GB	№127	# 3,839,999	15/JUL/2017	GTX 1050 2GB
2.99 GB	№256	# 7,679,999	04/MAY/2019	GTX 1060 3GB
3.99 GB	№383	# 11,519,999	20/FEB/2021	GTX 1050TI 4GB
5.99 GB	№639	# 19,199,999	29/SEP/2024	GTX 1060 6GB
7.99 GB	№895	# 26,879,999	07/MAY/2028	GTX 1070 8GB
10.99 GB	№1280	# 38,399,999	03/OCT/2033	GTX 1080TI 11GB

CSX 2018 NORTH AMERICA
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

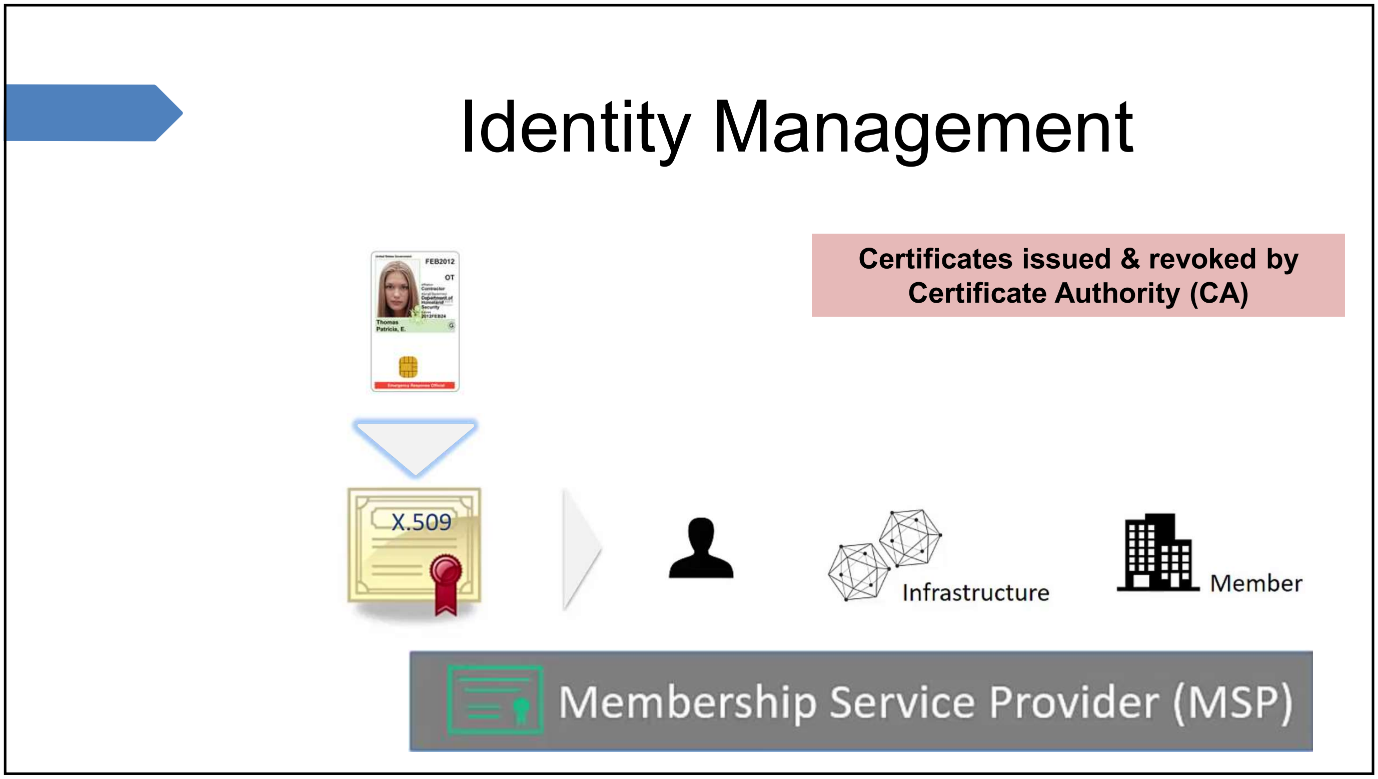
Permissioned Network



Participants are known in a permissioned network



Business Network and Channels

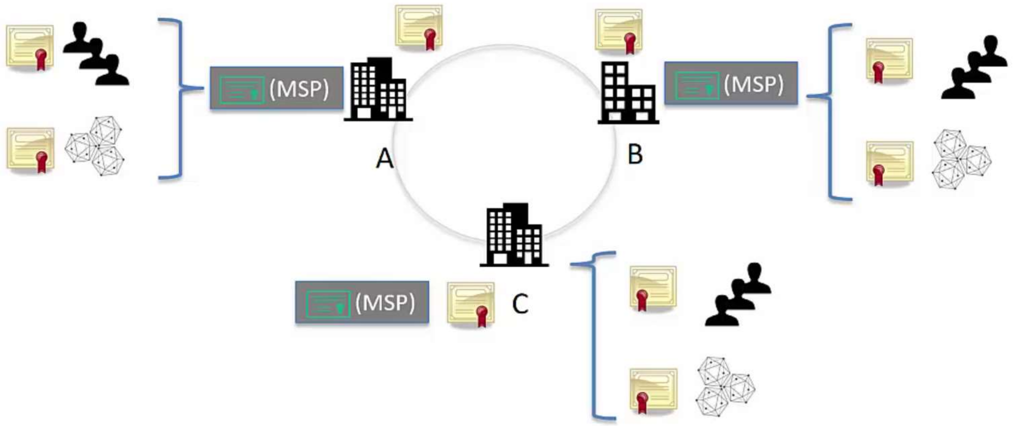


Identity Management

Certificates issued & revoked by Certificate Authority (CA)

Membership Service Provider (MSP)

Typical HLF Network


(MSP)
A
(MSP)
B
(MSP)
C