DHS Identity Innovation Grants Digital Bazaar

HSHQDC-16-C-00058

Manu Sporny - CEO, Digital Bazaar
Chairman of Payments & Credentials Community Groups at W3C

Goals of this Session

- Brief analysis of Blockchain technologies
- Key takeaways
- Global standardization of identity Blockchains
- The Promise of an Identity Blockchain Ecosystem

Security Capabilities of Blockchain Technologies

Principle	Bitcoin	Ethereum	Stellar	IPFS	Blockstack	Hashgraph
Confidentiality	None	None	None	Hash-based content addresses	None	None
Information Availability	Block Mirroring	Block Mirroring	Ledger Mirroring	Graph and file Mirroring	Block Mirroring / DHT Mirroring	Hashgraph Mirroring; optional event history
Integrity	Multiple block verifications	Multiple block verifications	Latest block verification	Hash-based content addressing	Multiple block verifications	Consensus with probability one
Non-repudiation	Digital signatures	Digital signatures	Digital signatures	Digital signatures	Digital signatures	Digital signatures
Provenance	Transaction inputs/outputs	Ethereum state machine and transition functions	Digitally signed ledger transition instructions	Digital signatures and versioning	Transaction inputs & outputs and virtualchain references	Hashgraph Mirroring; optional event history
Pseudonymity	Public keys	Public keys and contract addresses	Public keys	Public keys	Public keys, but public information encouraged	Not supported; could be layered
Selective Disclosure	None	None	None	None	Selective access to encrypted storage	Not supported; could be layered

Performance Capabilities of Blockchain Technologies

Principle	Bitcoin	Ethereum	Stellar	IPFS	Blockstack	Hashgraph
Consistency	Block verifications. 30-60 minutes	Block verifications. 20-60 minutes	Single block verification. Less than 1 minute	P2P mirroring. Limited primarily by network I/O. Several seconds for files less than 128KB.	Block verifications. 30-60 minutes	Consensus with probability one; Byzantine agreement, but attackers must control less than one-third
System Availability	Block verifications. 30-60 minutes	Block verifications. 20-60 minutes	Single block verification. Less than 1 minute.	Single storage request response. Several seconds for files less than 128KB	Block verifications. 30-60 minutes	Virtual voting; DoS resistant w/o proof-of-work, fast gossip
Failure Tolerance	Longest chain wins	Longest chain wins	Last balloted block always has consensus.	Content address hash. Highly resilient against network partitioning	Longest chain wins	Strong Byzantine fault tolerance
Scalability	Block size. 7 transactions per second	Block size. 7-20 transactions per second	Thousands to tens of thousands of transactions per second.	Thousands to tens of thousands of transactions per second. Scales linearly as nodes are added.	Block size. 7 transactions per second	Thousands to tens of thousands of transactions per second. Limited by bandwidth only
Latency	Block verifications. 30-60 minutes	Block verifications. 20-60 minutes	Single block verification. Less than 1 minute.	Single storage request response. Several seconds for files less than 128KB.	Block verifications. 30-60 minutes	Virtual voting; limited only by exponentially fast gossip protocol
Auditability	Full	Full	Full	Difficult	Full	Configurable
Liveliness	Full	Full	Full	Fails if nodes storing data fail	Full	Full
Denial of Service Resistance	Spend Bitcoin	Spend Ether	Spend Stellar	Files are only mirrored if requested	Spend Bitcoin	Signed State / Proof-of-stake / < 1/3 attackers
System Complexity	Medium	High	Medium	Medium	Medium High	Low, but not full system

Key Takeaways

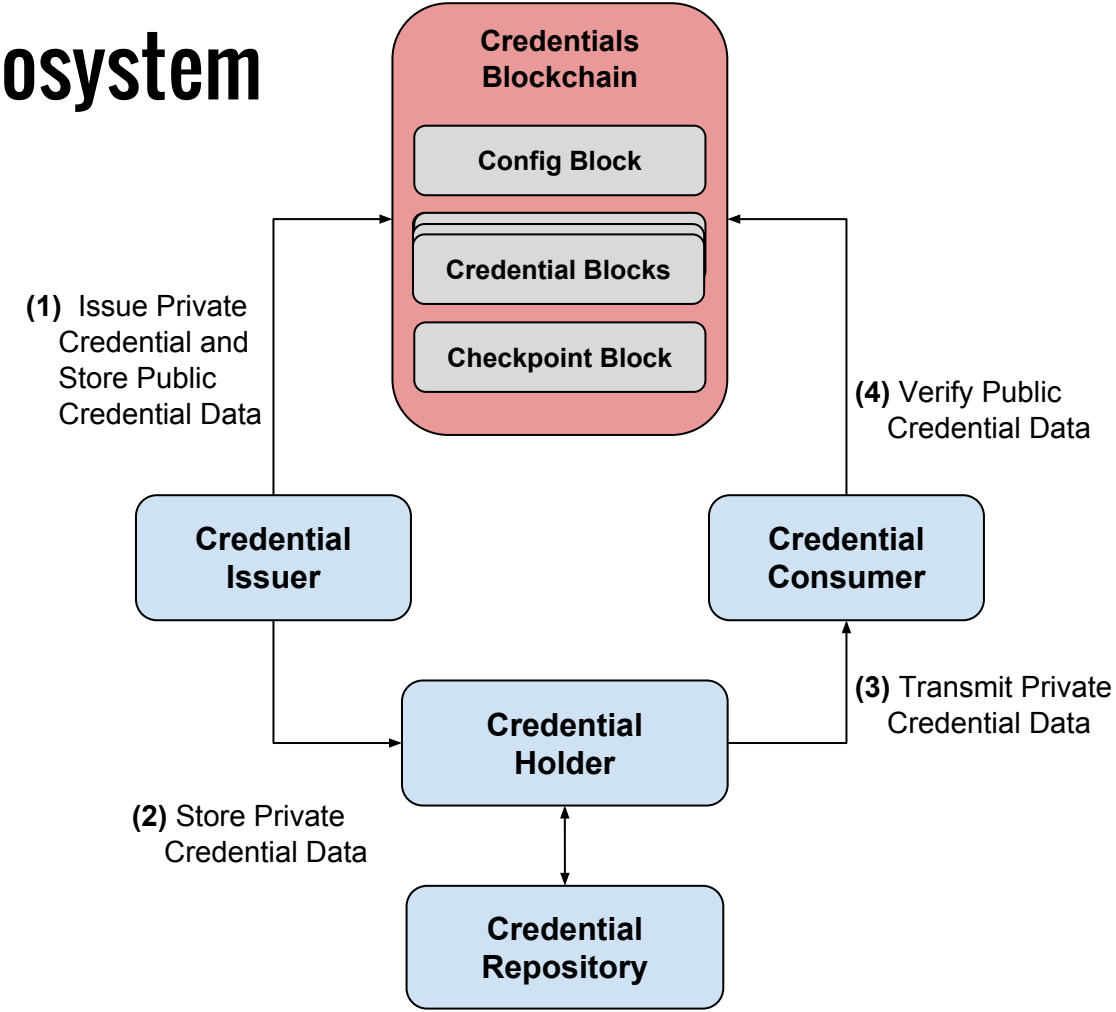
- Blockchains are useful when loosely coupled organizations want to share and audit information
- Blockchain technologies make important trade-offs, most (but not all) are ill suited for identity management
- Blockchains are only part of the identity ecosystem
- Blockchains are not interoperable yet - no standards

Standardization at World Wide Web Consortium?

- W3C composed of 400+ member organizations
- Builds the next generation Web
- Incubating standards-track work on Verifiable Claims, Credentials, and Blockchain
- Digital Bazaar submitting requirements/specs for Blockchain Identity Ecosystem - Verifiable Claims, Flex Ledger

Blockchain Identity Ecosystem

- Issuers
- Holders
- Repositories
- Consumers
- Blockchain



The Promise of a Blockchain Identity Ecosystem

- International (W3C) standards for credential management
- Real-time verification of a doctor's license status
- Drug delivery supply chain auditability
- Insurance claim fraud detection
- Continuing education validation