Blockchains:

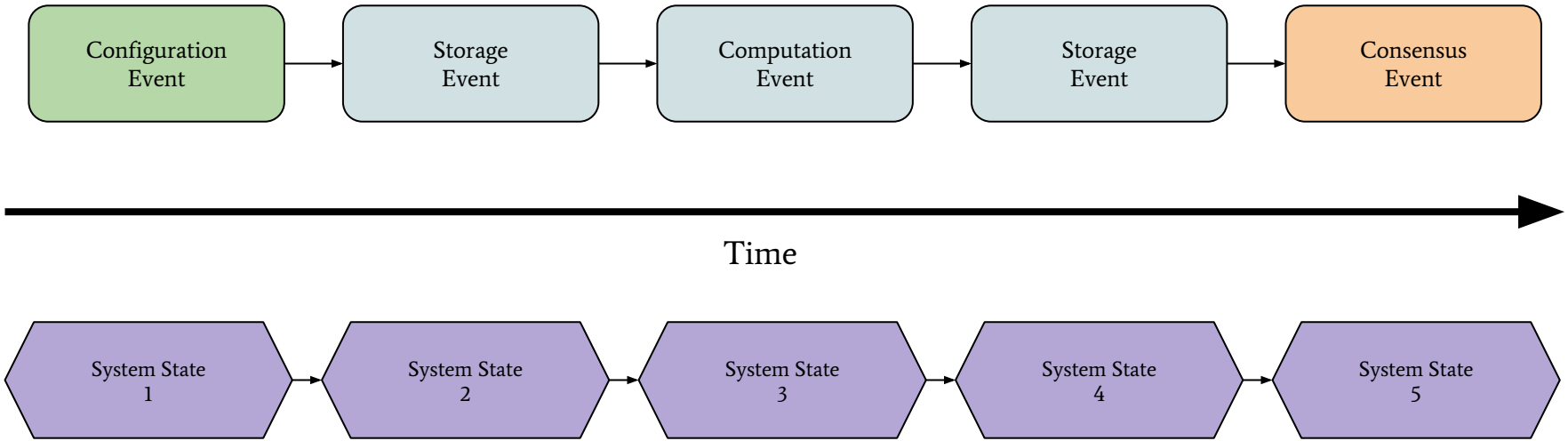
The Bits That Could Be Standardized

Manu Sporny - CEO - Digital Bazaar

Research Into Decentralized Ledger 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

Blockchain = State Machine + Events



Breakout Session: Could We Standardize These?

- Basic Data Model for Blockchain (State Machine + Events)
- Consensus Algorithms (Proof of Work, Stellar Consensus, Hashgraph)
- Storage Algorithms (Merkle Trees, MerklePatriciaTrees, Linked List)
- Signature Algorithms (JOSE, LD Signatures, HD Keys, Proof of Publication)
- Web-based Access Protocol (Create, Status, Sync, Add, Query)
- Work in Progress: Flex Ledger