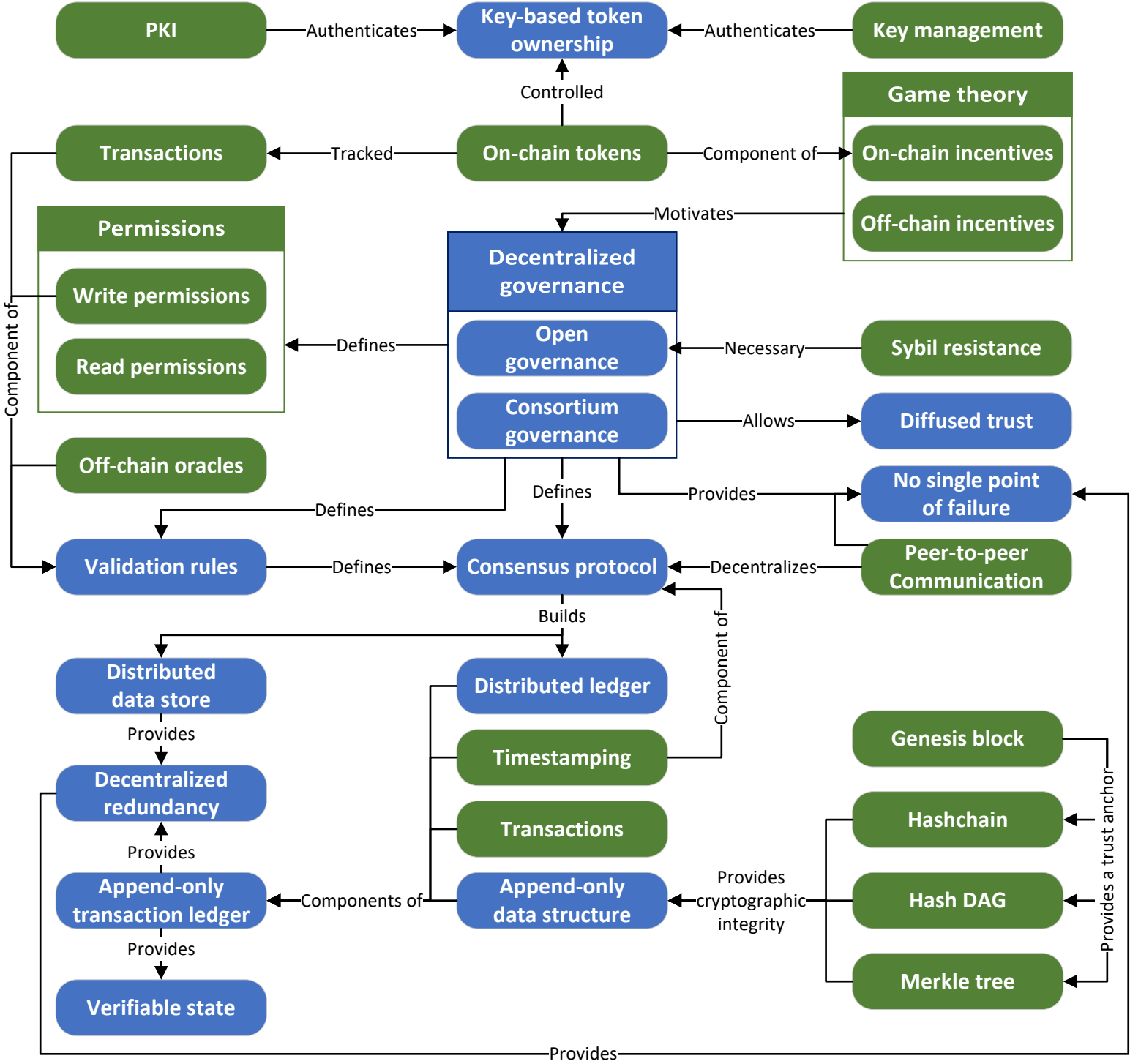
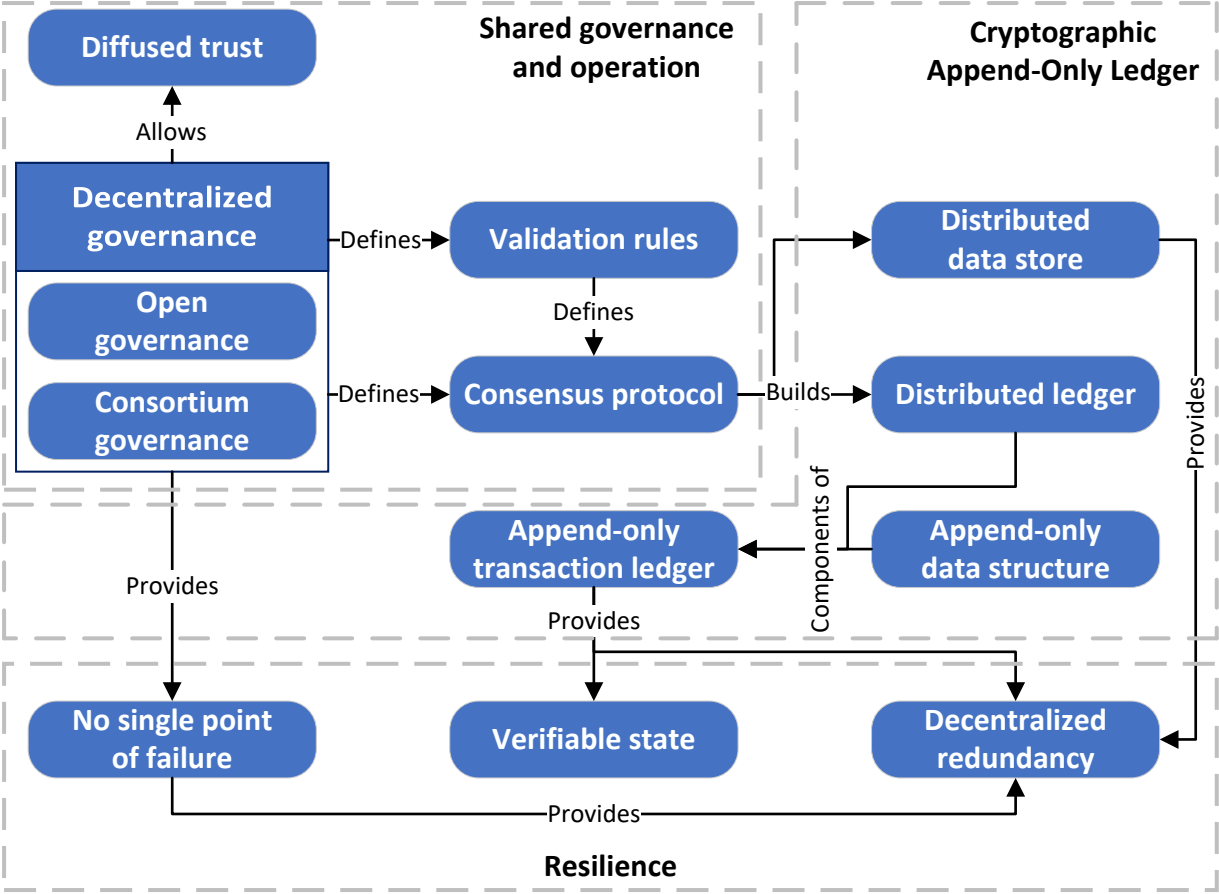
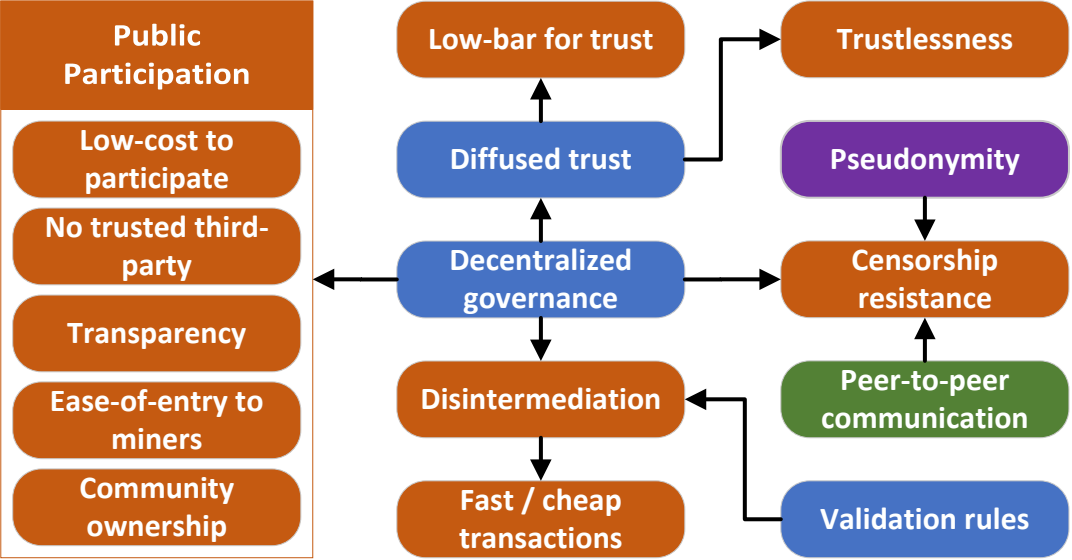
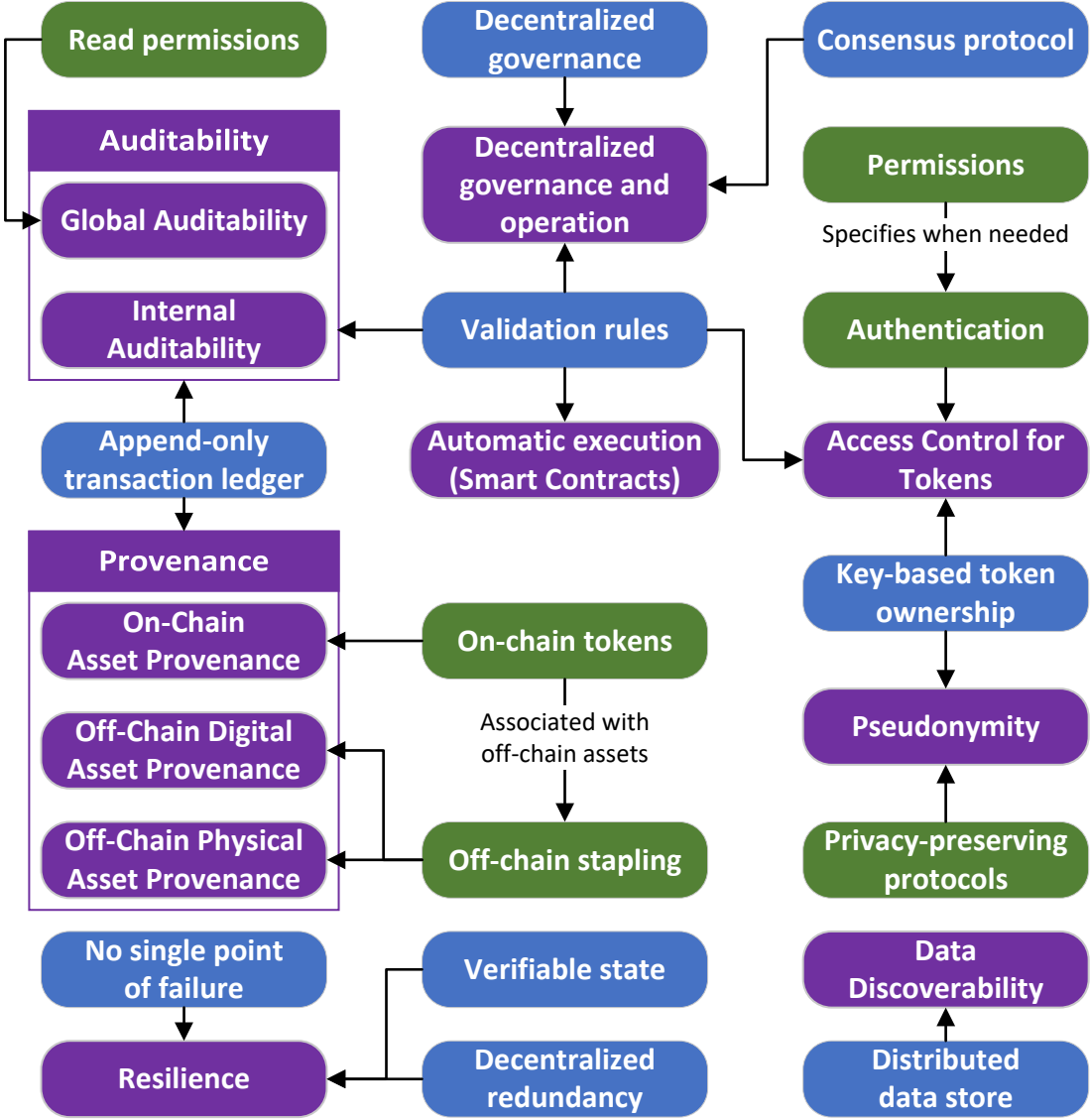

PKI
Authenticates
Key-based token ownership
Authenticates
Key management
Controlled
Game theory
Transactions
Tracked
On-chain tokens
Component of
On-chain incentives
Off-chain incentives
Motivates
Permissions
Decentralized governance
Write permissions
Read permissions
Defines
Open governance
Necessary
Sybil resistance
Consortium governance
Allows
Diffused trust
Component of
Off-chain oracles
Defines
Defines
Provides
No single point of failure
Validation rules
Defines
Consensus protocol
Decentralizes
Peer-to-peer Communication
Builds
Component of
Distributed data store
Distributed ledger
Provides
Timestamping
Genesis block
Decentralized redundancy
Transactions
Hashchain
Provides
Provides cryptographic integrity
Provides a trust anchor
Append-only transaction ledger
Components of
Append-only data structure
Hash DAG
Provides
Merkle tree
Verifiable state
Provides


Diffused trust
Shared governance and operation
Cryptographic Append-Only Ledger
Allows
Decentralized governance
Defines
Validation rules
Open governance
Defines
Consortium governance
Defines
Consensus protocol
Builds
Distributed data store
Distributed ledger
Provides
Components of
Append-only transaction ledger
Append-only data structure
Provides
Provides
No single point of failure
Verifiable state
Decentralized redundancy
Provides
Resilience


Public Participation
Low-cost to participate
No trusted third-party
Transparency
Ease-of-entry to miners
Community ownership
Low-bar for trust
Diffused trust
Decentralized governance
Disintermediation
Fast / cheap transactions
Trustlessness
Pseudonymity
Censorship resistance
Peer-to-peer communication
Validation rules


Read permissions
Decentralized governance
Consensus protocol
Auditability
Decentralized governance and operation
Permissions
Global Auditability
Specifies when needed
Internal Auditability
Validation rules
Authentication
Append-only transaction ledger
Automatic execution (Smart Contracts)
Access Control for Tokens
Provenance
Key-based token ownership
On-Chain Asset Provenance
On-chain tokens
Off-Chain Digital Asset Provenance
Associated with off-chain assets
Pseudonymity
Off-Chain Physical Asset Provenance
Off-chain stapling
Privacy-preserving protocols
No single point of failure
Verifiable state
Data Discoverability
Resilience
Decentralized redundancy
Distributed data store