# ASSURED CYBER SUPPLY CHAIN PROVENANCE USING PERMISSIONED BLOCKCHAIN

Sachin Shetty and Xueping Liang
Old Dominion University

Andrew Miller
University of Illinois Urbana-Champaign

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security | cred-c.org

# Blockchain Overview

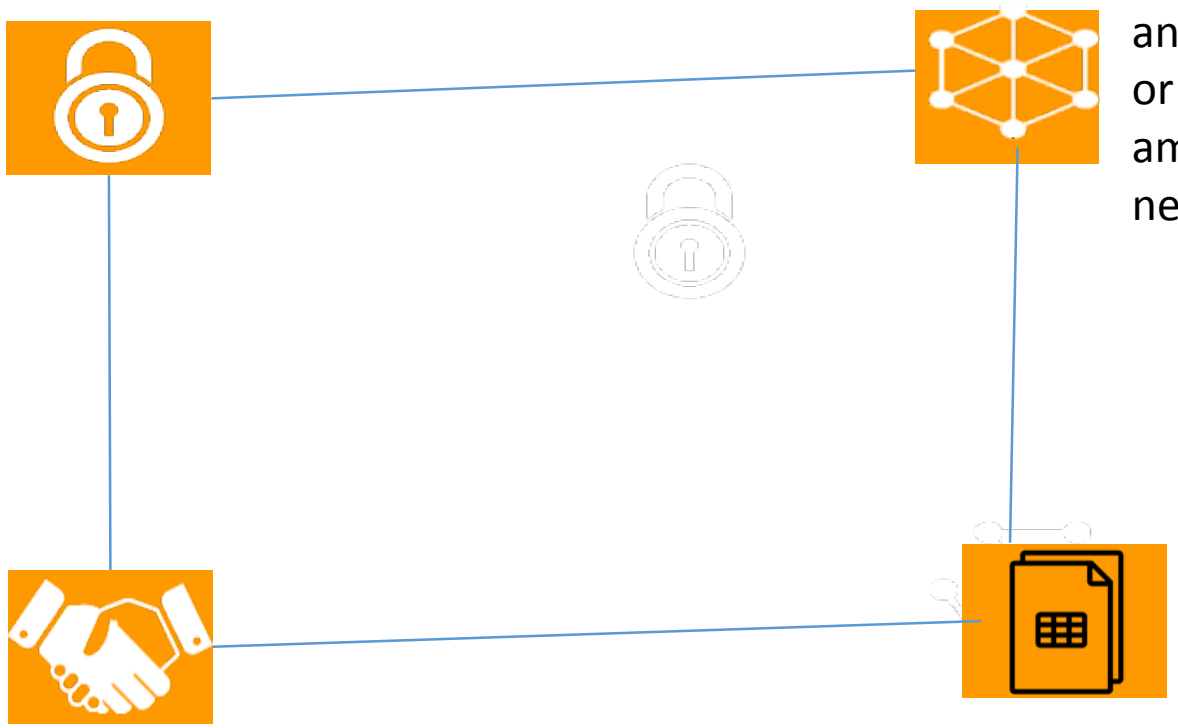
**Problem – How do distributed distrusting stakeholders agree on current system state?**

**Current Solution - Centralized trusted arbiter (ex. database) to report on current system state.**

**Desired Solution – If technology can help the stakeholders to reach consensus on history, agreement on current system state can be reached**

# Blockchain Overview

**Cryptographically Secure**
Public/Private signature technology applied to create transactions that establishes a shared truth.



**Distributed Network**
Replicas of distributed ledger and no single participant owns or can tamper. Consensus among majority participants is needed to update the database

**Consensus**
Consensus among majority participants is needed to update the database. Leverages validation rules provided by smart contract ("Business Logic")

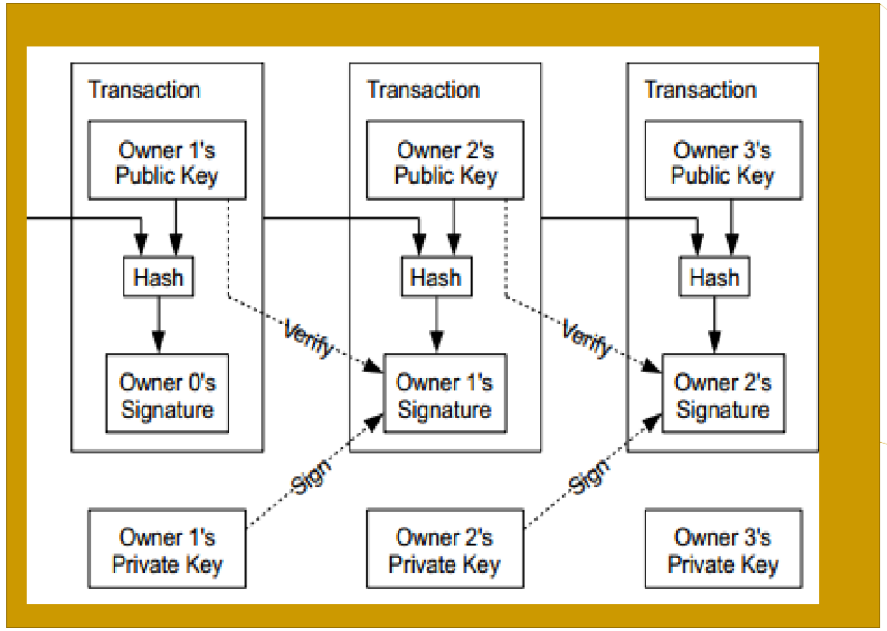
**IMMUTABLE LEDGER**
Append only database that holds immutable record of every transaction

# Blockchain Overview

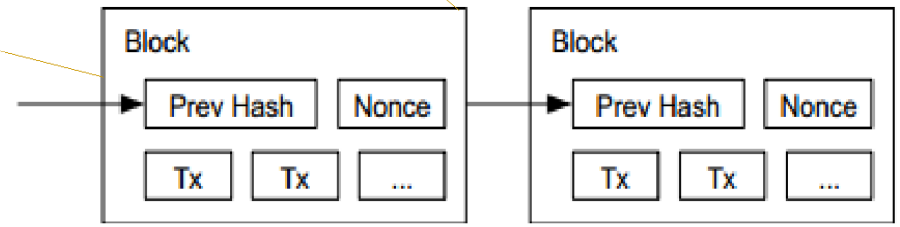
- **Why not use centralized databases?**
  - Single point of compromise/failure
  - Too much power vested in one entity
  - Challenging to get every entity to agree on the one arbiter to trust
- Blockchain eliminates the need for a centralized trusted database
  - Share databases across diverse boundaries of trust
  - Transactions leverage self-contained proofs of validity and authorization
  - Multiple nodes provide validation through consensus
  - Robustness without need for expensive replication and disaster recovery
  - Automatically self-configure and synchronize in peer-to-peer fashion

# Blockchain Overview

- **Chained sequence of hash records**
  - No entity can can change any past record.
- **Several procedures for adding blocks to blockchain**
- **Validation of blocks**
  - Enforced by consensus protocols



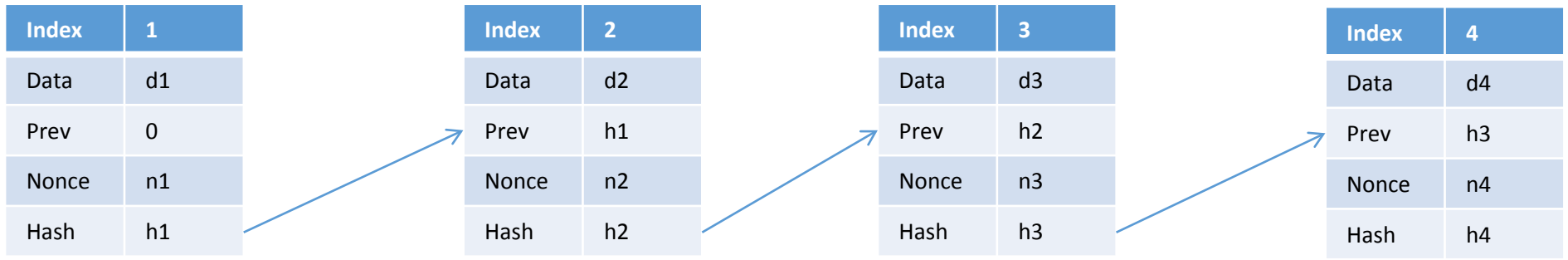

Source : Nakamoto, S (2008) Bitcoin: a peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf




CREDC

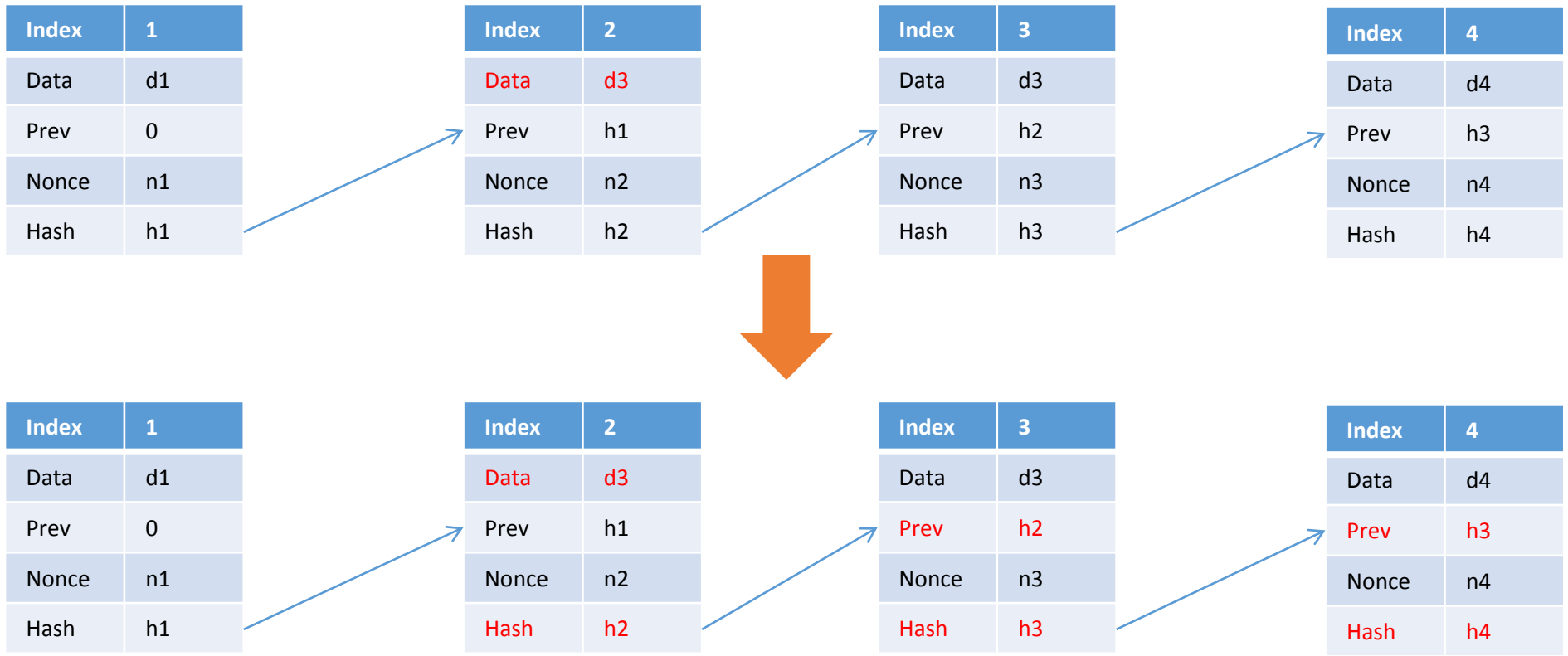
# Blockchain Overview

- **Hash Chain**
  - Building block of blockchains
  - Curbs centralized arbitrator's ability to modify history
  - Cryptographic hash function (SHA256).
  - Mathematically impossible to find two inputs with the same hash value.
  - Translates to every record (N) has a commitment to N-1 which is committed to record N-2 and so on and so forth



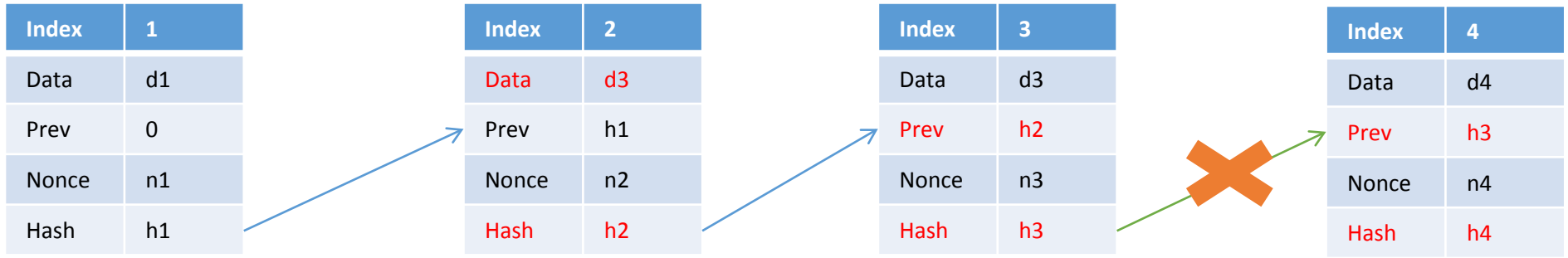
# Blockchain Overview

- **Attack on hashed chain**



# Blockchain Overview

- **Propagation of attack in hashed chain**
  - Changing record N results in changes to final hashes of records N+1, N+2, etc

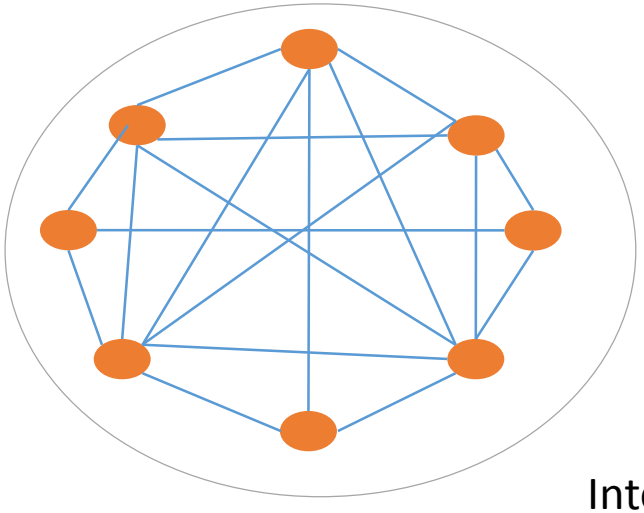


# Blockchain Overview

- Proof of Work
  - Carry out large computation and prove that computation was successfully
  - No additional work to check the proof
  - Limits the rate of new blocks and expensive to add invalid blocks
  - Aids in deciding between competing chains
- Proof of Stake
  - Achieve consensus by eliminating expense proof of work
  - Block creation tied to amount of stake
- Byzantine Fault Tolerance
  - Trusted entities work together to add records
  - Voting process for accepting a block on the chain

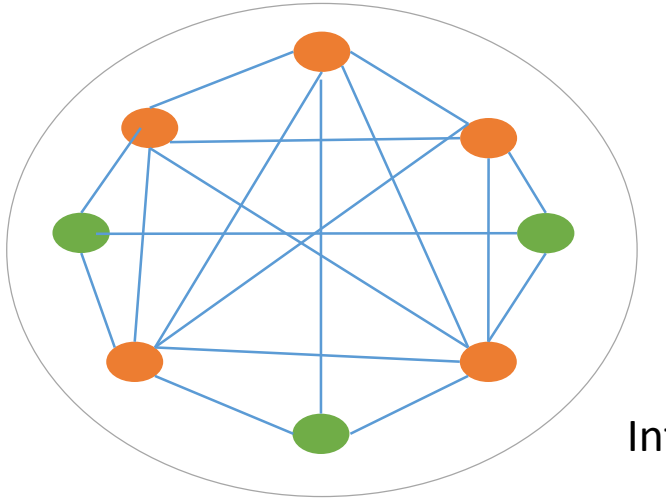
# Blockchain Overview

- Permissionless Blockchain Infrastructures
  - Open access on the Internet
  - Anonymous validators
  - Proof of Work consensus
  - Public network



Internet

- Permissioned Blockchain Infrastructures
  - Private network
  - Participation by members only
  - Trusted validators
  - Customized consensus protocol



Intranet

# Blockchain Challenges

- Scalability and Validation Speed
  - Blockchain platforms take 10 min or longer to confirm transactions and 7 transactions/sec maximum throughput
  - Cannot yet match speed of mainstream payment processor
  - Bottlenecks in Blockchain architecture limit high throughput and low latencies
  - Parameterization of block sizes and intervals will not be sufficient for high load blockchain deployments
  - Need for scalable consensus protocols, network topology and storage
- Incentives in permission-less infrastructure
  - Miners ensure sustainability of system
  - Incentive is the capital invested in Bitcoin
- Incentives in permissioned infrastructure
  - How to build payoff into consensus protocols to store provenance records?

# Blockchain Challenges

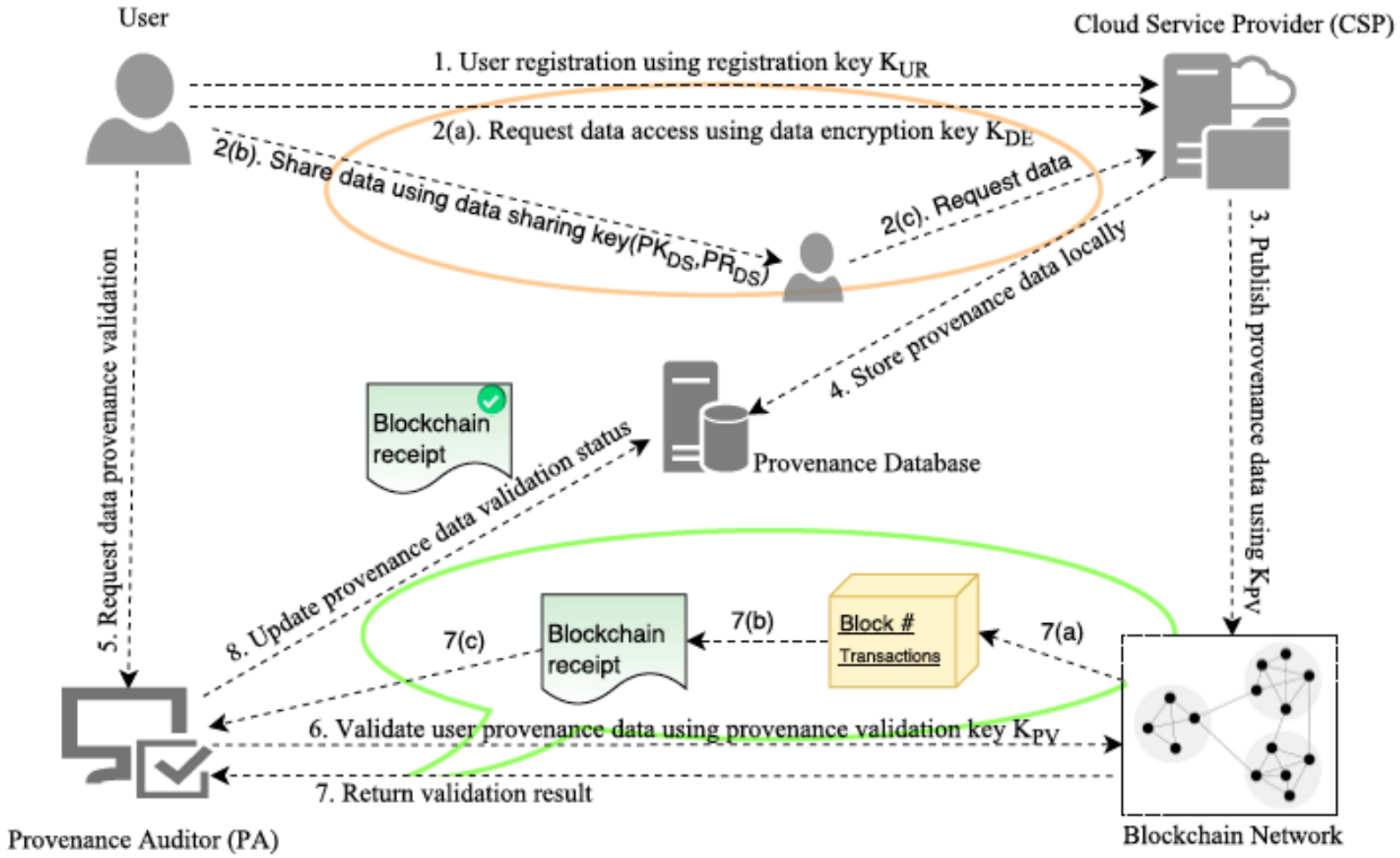
- Privacy
  - Data breach attacks on permissioned blockchain platforms
  - Need for privacy guarantees in case of attack on validating nodes
  - Tradeoff between resilience and privacy
  - Need to include cryptographic techniques, such as, multi-party computation, homomorphic encryption, etc within permissioned blockchain platforms

# Blockchain Development Platforms

- Ethereum
  - Generalized blockchain platform
- Multichain
  - Permissioned blockchain network
- **Hyperledger Fabric**
  - Open standard for blockchain for business
- Tierion
  - Supports integration of applications within blockchain network
- Guardtime
  - Industrial scale blockchain service with keyless signature infrastructure and secure one way function

# Provchain

**Research Goal** - Develop blockchain based data provenance capability for cloud to allow tracking of data from its creation to its current state or end state which enables transparency and accountability




Xueping Liang, Sachin Shetty, Deepak Tosh, Charles Kamhoua, Kevin Kwiat, Laurent Njilla, "ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability", The 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), May 14-17 2017.



**Funded by Air Force Research Lab**

# CREDC Project- Cyber Supply Chain Provenance

- Problem
  - Address cyber supply chain risks due to lack of trust in software and firmware developed by third party vendors
  - Lack of scalability in solutions such as side channel fingerprinting, reverse engineering, formal methods deployed at chip level

- Approach
  - Blockchain-based data provenance capability to certify software and firmware at all stages of EDS cyber supply chain
  - Encode firmware/software design and has values in the blockchain
  - Hash values and firmware/software designs delivered through cyber supply chain and participators can ensure authenticity by verifying hash values

# CREDC Project- Cyber Supply Chain Provenance

- Challenges
  - Identify business rules to balance between resilience and scalability
  - Changes in business rules results in chain forks.
  - Privacy attacks on permissioned blockchain platforms

- Ongoing and Future Work
  - Customized consensus protocols to validate the transactions containing software and firmware hardware design
  - Develop methodology to encode the firmware/software design in transactions
  - Develop privacy mechanism based on threshold encryption

# CYBER RESILIENT ENERGY DELIVERY CONSORTIUM


http://cred-c.org

@credcresearch

facebook.com/credcresearch/

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security