A Blockchain Based Trusted Information Exchange Framework

Sachin Shetty
Associate Professor
Virginia Modeling, Analysis and Simulation Center
Old Dominion University

Deepak Tosh
Cyber security Researcher
Computer Science
Norfolk State University

Outline

- Blockchain Overview
- Blockchain for Information Sharing
- Demo

Blockchain Overview

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

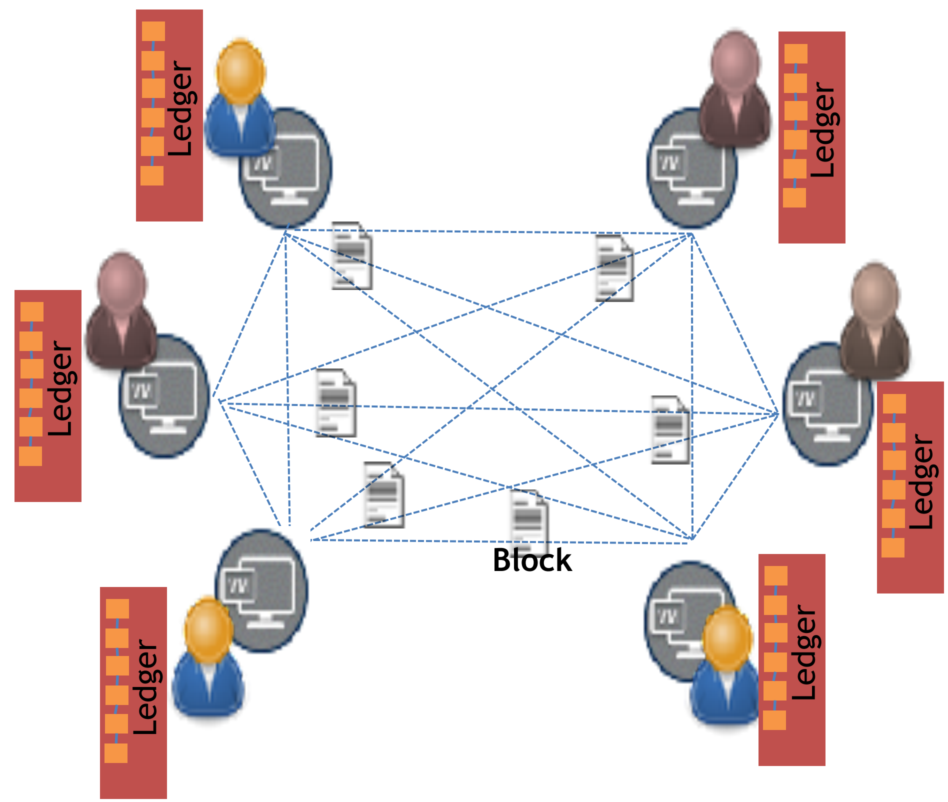
- **Solution - If technology can help the stakeholders to reach consensus on history, agreement on current system state can be reached**

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

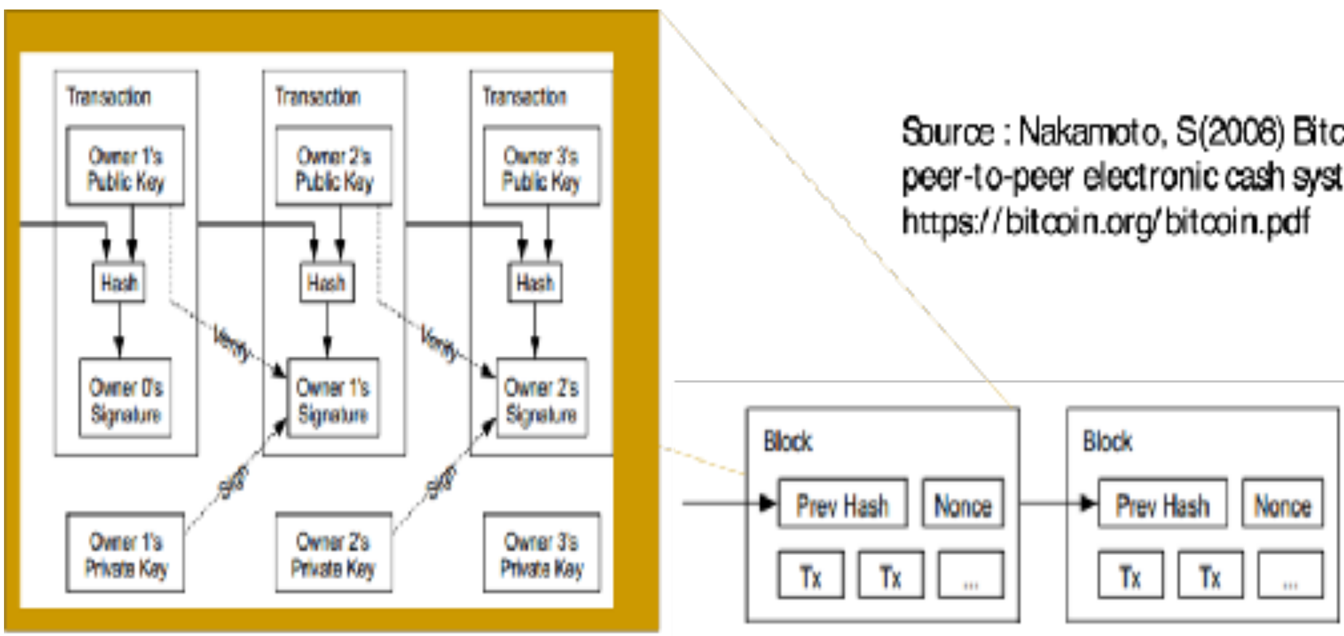
Blockchain Overview

- **Decentralized Network**
  - Peer-to-Peer Architecture
  - Nodes can join/leave freely
  - No central arbitrator
  - Redundancy and robustness to link failures
- **Distributed Consensus**
  - Transaction record
  - Distributed public ledger
  - Validation by committee
- **Cryptographically Secure**
  - Immutable audit trail
  - Data tampering prevented



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

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

Index	1
Data	d1
Prev	0
Nonce	n1
Hash	h1

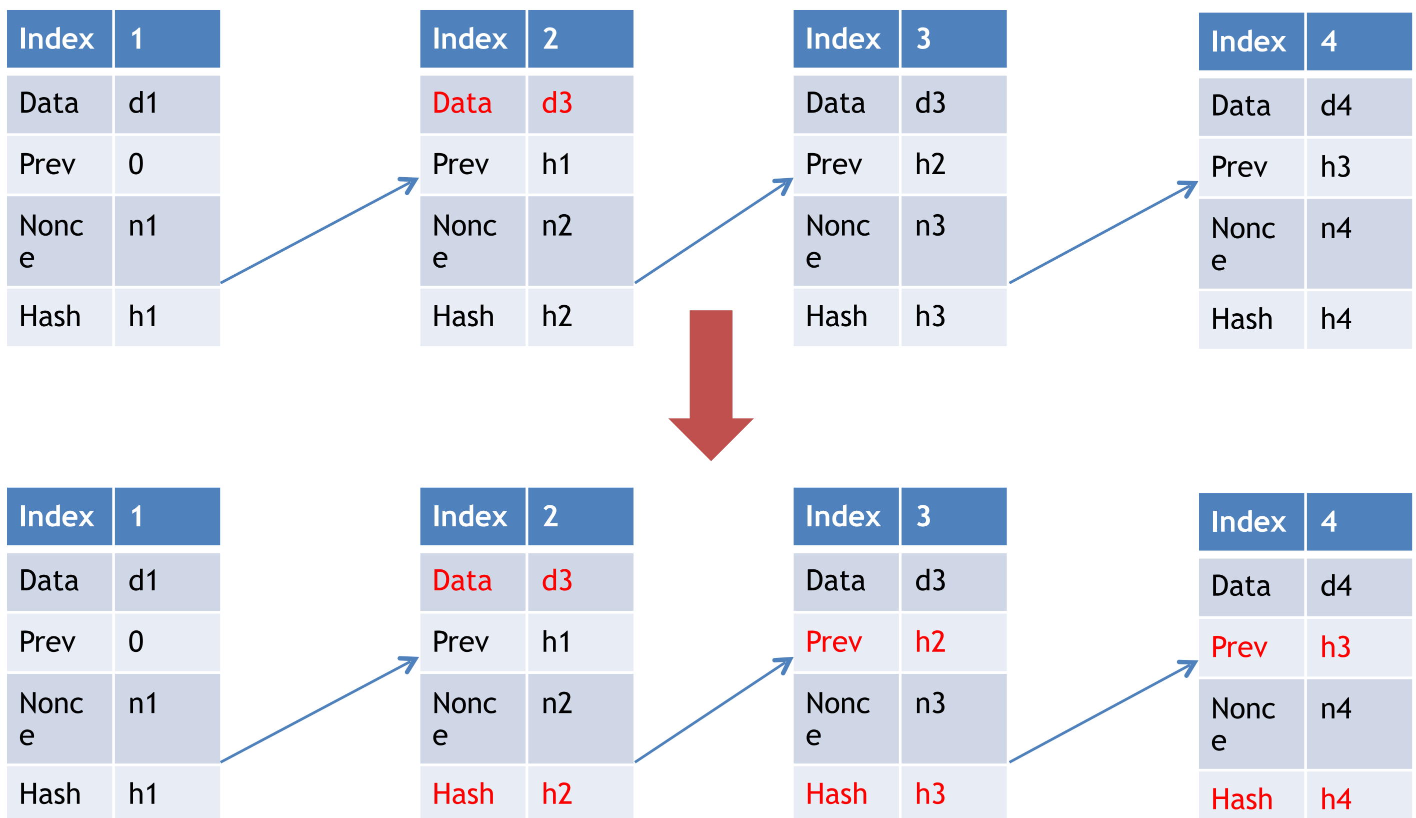
Index	2
Data	d2
Prev	h1
Nonce	n2
Hash	h2

Index	3
Data	d3
Prev	h2
Nonce	n3
Hash	h3

Index	4
Data	d4
Prev	h3
Nonce	n4
Hash	h4

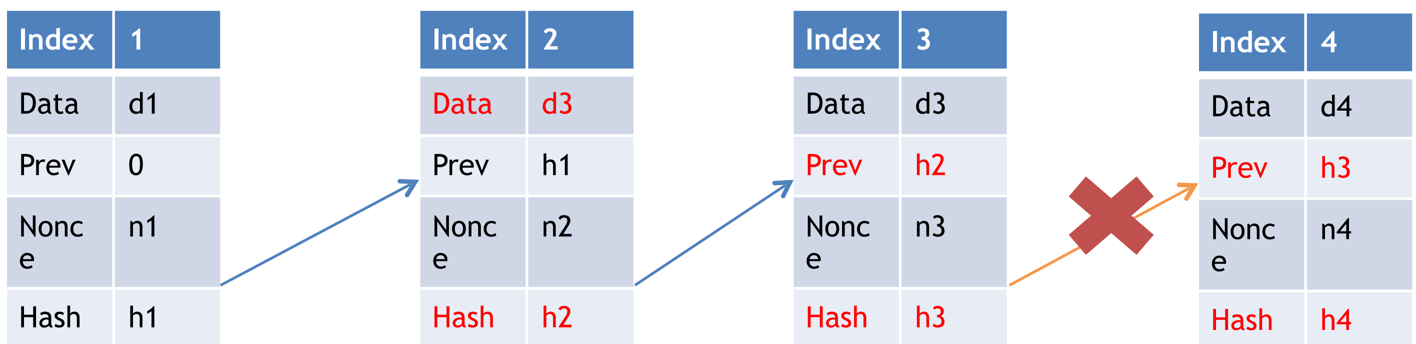
Blockchain Overview

- **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

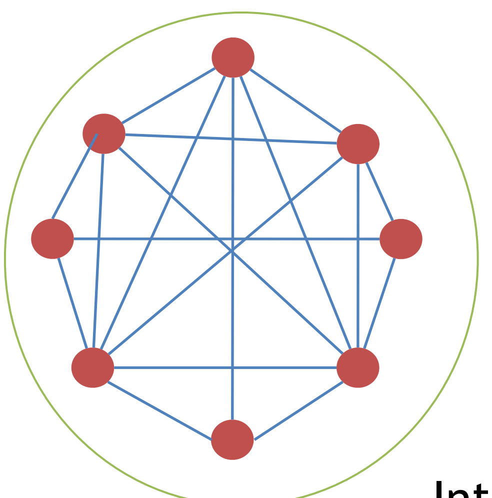


Blockchain Overview

- Proof of Work
  - Carry out large computation
  - Prove that computation was successfully
  - No additional work to check the proof
  - Limits the rate of new blocks
  - Expensive to add invalid blocks
  - Aids in deciding between competing chains by choosing the one with the most work.
- 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

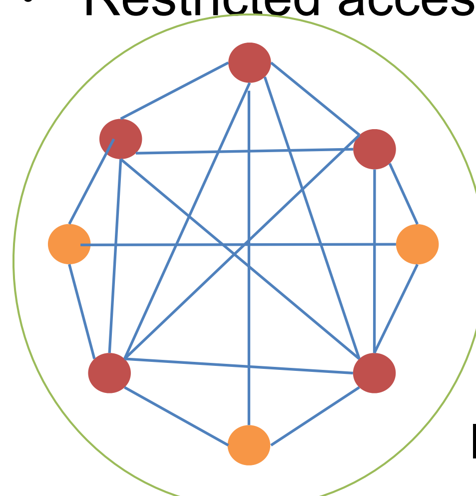
Blockchain Overview

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



Internet

- Permissioned Blockchain Infrastructures
  - Private network
  - Participation by members only
  - Trusted validators
  - Customized consensus protocol
  - Members set rules
  - Restricted access



Intranet

Blockchain Overview

- Incentives in permissionless infrastructure
  - Miners ensure sustainability of system
  - Incentive is the capital invested in Bitcoin
  - Payoffs in Bitcoin involves moving money around
- Incentives in permissioned infrastructure
  - How to build payoff into consensus protocol to share cyber threats?

Blockchain Summary

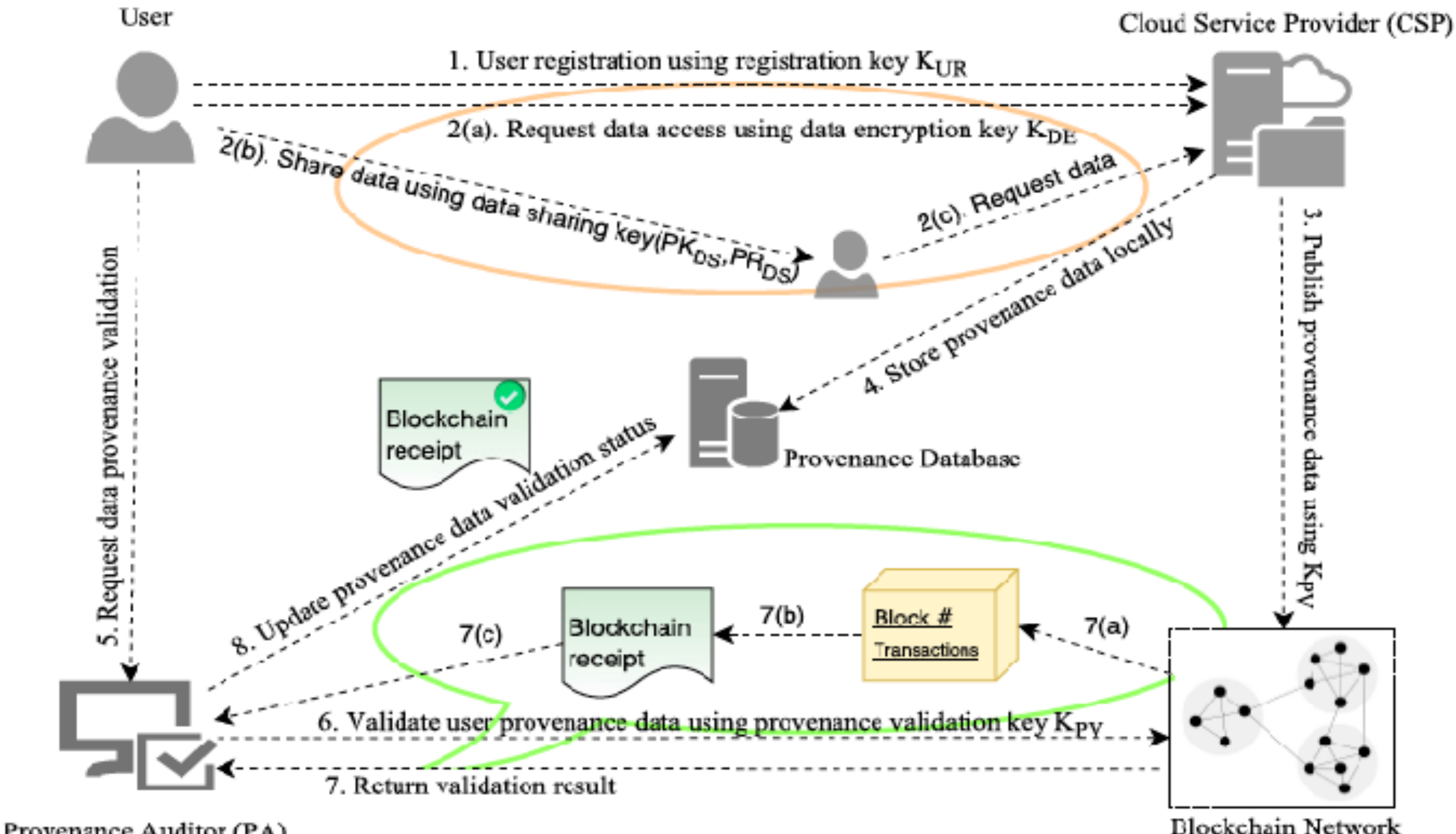
- No need to trust each other or have a trusted third party
- Distributed system
- Agreement on history translates to agreeing on system state
- Nth record in the hash chain commits to all previous records.
- Any change in previous record invalidates hash chain
- A blockchain is a hash chain with procedures for validity and resolve disagreements
  - Permissionless vs Permissioned infrastructure
  - Proof of Work vs Proof of Stake vs Proof of Storage, etc

Trusted Information Exchange Framework Needs

- Anonymity
- Privacy
- Integrity of Entities exchanging information
- Integrity of Stored Information
- Inability to attribute to individuals sha information
- Eliminating free-riders
- Avoid spurious information

Same as anonymity

ProvChain



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

Information Exchange using Blockchain

- **Integrity of participating entity**
- Each entity can be deployed onto the blockchain with an identifier (ID)

- Blockchain will not allow the un-authorized changing of ID

- Blockchain will not allow the un-authorized addition of an entity to the system

- It will be trivial for the Blockchain to check if a particular ID is valid and exists in the system

Information Exchange using Blockchain

- **Integrity of historic transactions**
- Transaction can be represented as message, command, data exchange, action within the system

- Historical transcripts are easily tracked for each particular entity

- Blockchain will not allow the alteration of historical transcripts

- If alteration is attempted, detection will be easy

- Once detected the majority (validators) will reject the change

Information Exchange using Blockchain

- **Integrity of data transmission**
- Data in transit can be spoofed or intercepted

- Blockchain can be used to determine who should message who, if this rule changes without authorization blockchain will not allow it and detection will occur

- If the attacker intercepts message in transit additional encryption will be needed such as public private key

Information Exchange using Blockchain

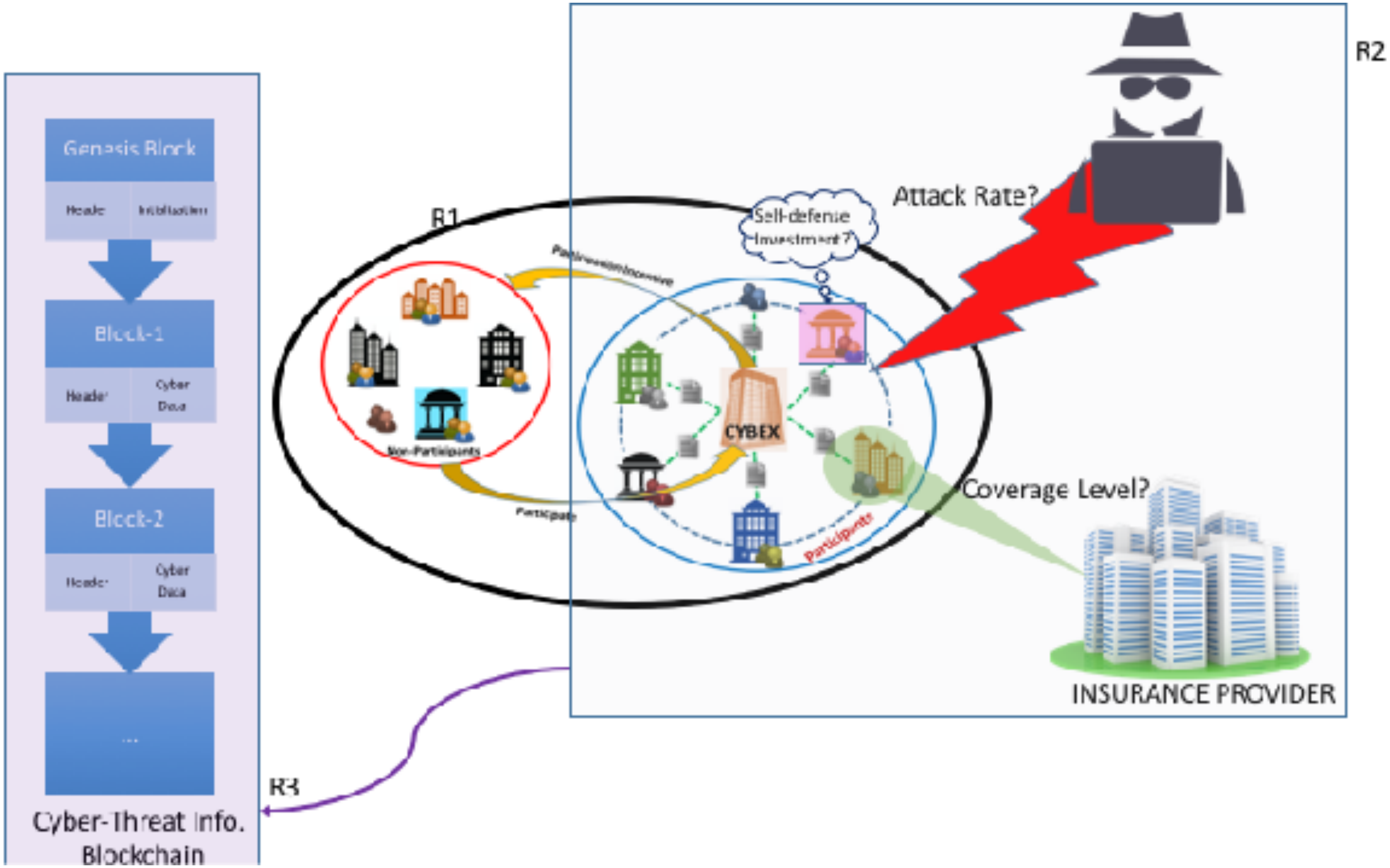
- **Integrity of stored data**
- Data records from entities stored in datacenters can be timestamped on the blockchain

- Any changes to the data will require authorization by the blockchain

- Blockchain will not allow changes to the history of data

- If un-authorized changes occur, blockchain can determine the faulty change, not allow the change, and report.

Information Exchange Game Model



[R2]*Deepak Tosh, Iman Vakilinia, **Sachin Shetty**, Shamik Sengupta, Charles A. Kamhoua, Laurent Njilla, Kevin Kwiat , "Three Layer Game Theoretic Decision Framework for Cyber-Investment and Cyber-Insurance,"* 8th Conference on Decision and Game Theory for Security

Thank You

Sachin Shetty
sshetty@odu.edu
www.odu.edu/~sshetty

Deepak Tosh
dktosh@nsu.edu