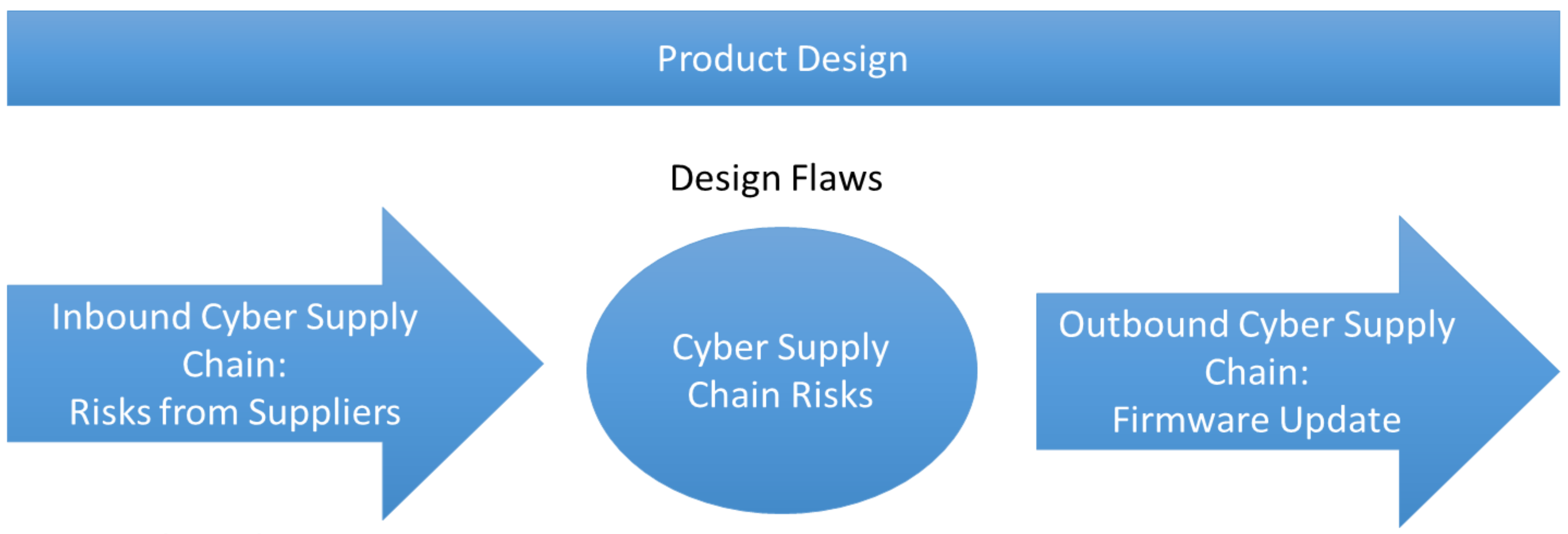
CREDC

Blockchain Based Cyber Supply Chain Provenance

Xueping Liang, Deepak Tosh and Sachin Shetty

LACK OF TRUSTED THIRD PARTY

- Globalization of cyber supply chain has resulted in software and firmware developed by subcontractors who use third party software or IT systems that can be difficult to audit during malfunction
- Dependency on third-party services has resulted in an increase in threats, such as, counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices across several stages in the cyber supply chain


Product Design
Design Flaws
Inbound Cyber Supply Chain: Risks from Suppliers
Cyber Supply Chain Risks
Outbound Cyber Supply Chain: Firmware Update

- Data breaches
- Network Disruption
- Insider threats
- Unnecessary functionality

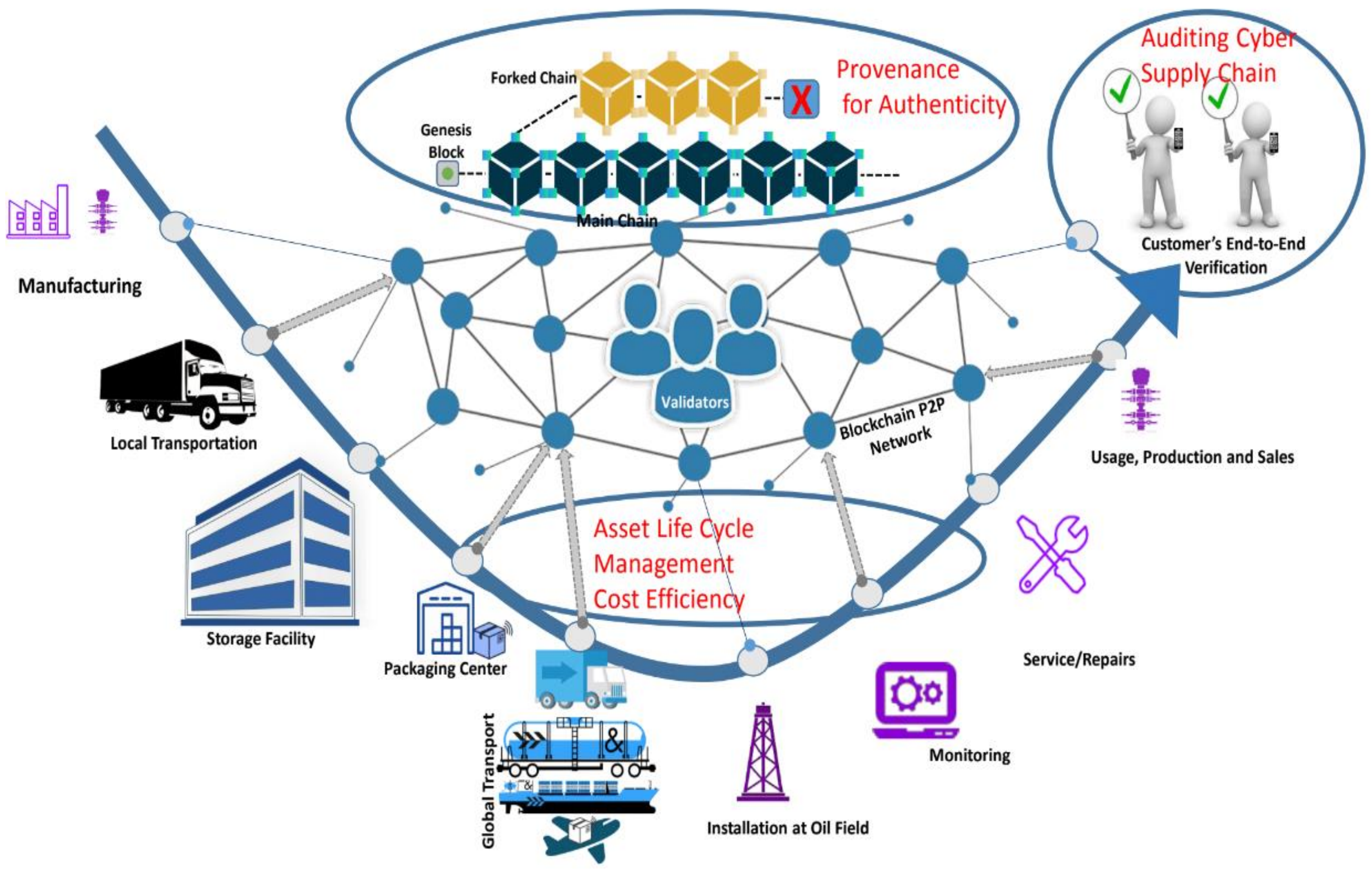
- Counterfeit
- Theft
- Tampering

RESEARCH VISION

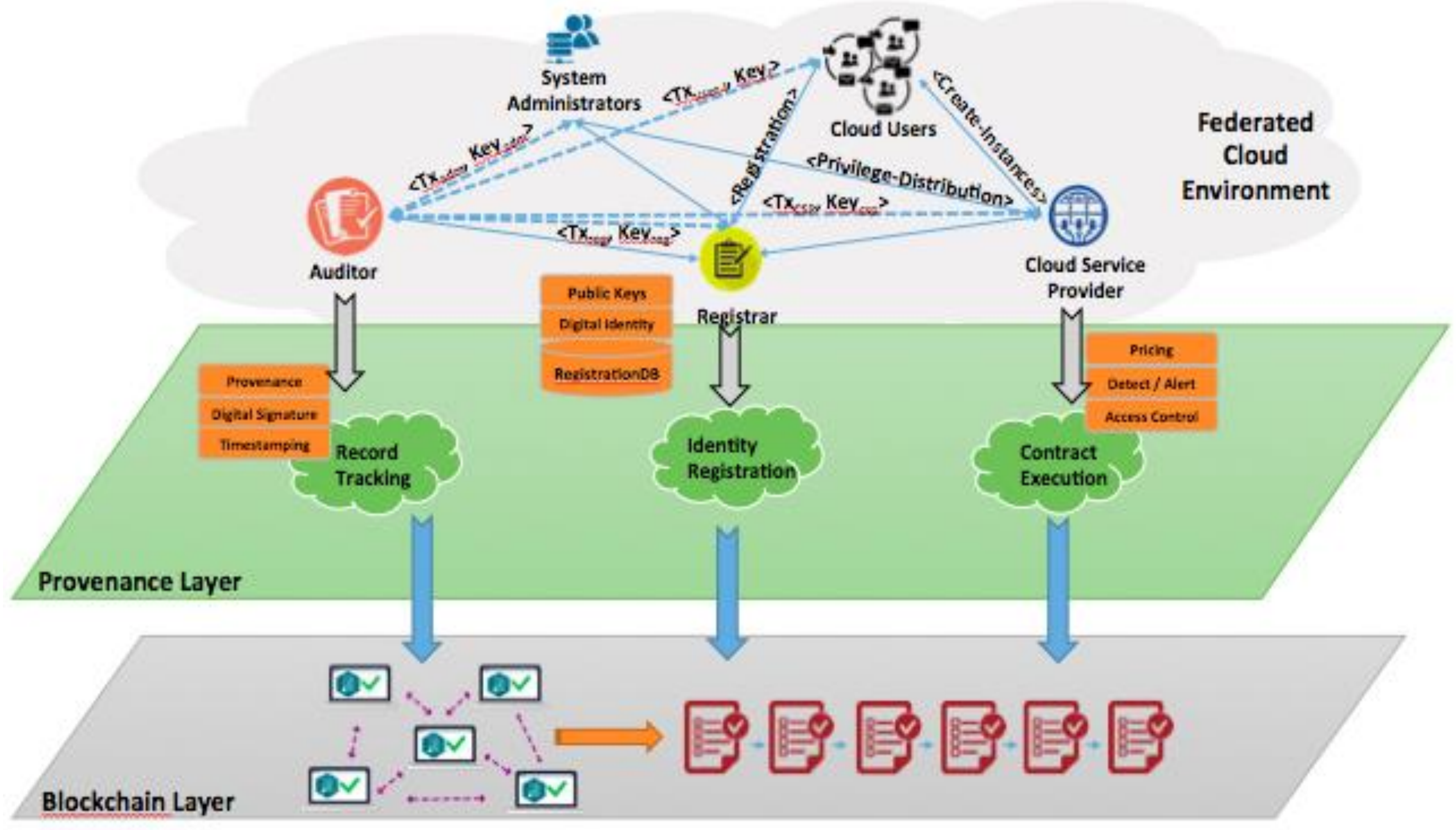
A Blockchain-Empowered Provenance of Cyber Supply Chain tool that will record the provenance for software and firmware at all stages of a cyber-supply chain to ensure authenticity and quality control.

RESEARCH APPROACH

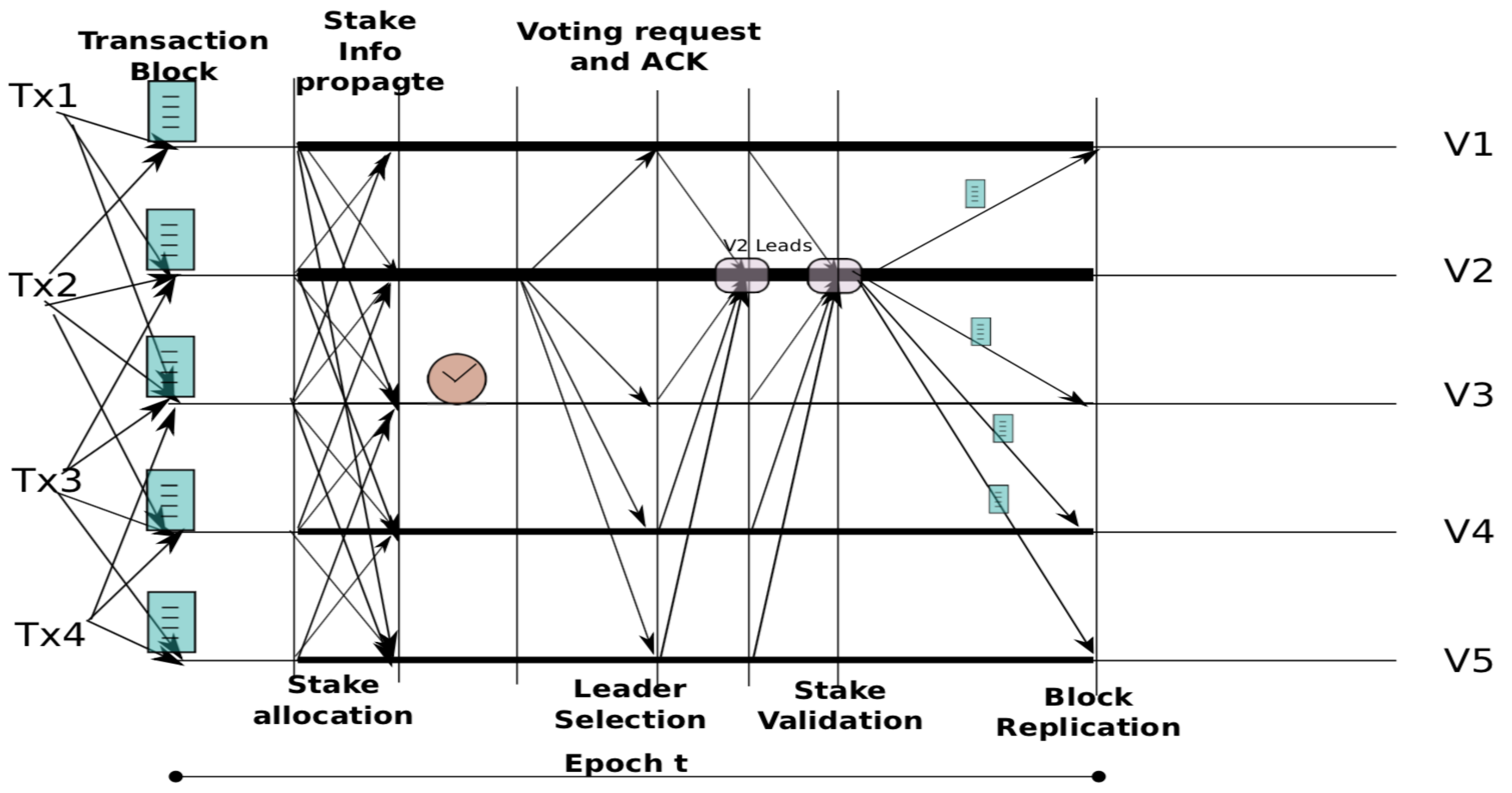
- Identify the **software and firmware design** in the cyber supply chain which will be tracked and encoded in the blockchain transaction
- Develop a methodology for **encoding** of the **supply chain operations** into transactions while balancing tradeoff between validation accuracy and latency.
- Develop **customized consensus engine** which balances tradeoff between **scalability** and security rules encoded by participators.
- Develop a **security** mechanism for blockchain transactions based on **threshold encryption**.
- Develop game theoretic based **incentive** mechanism to ensure maximum **participation** by cyber supply chain stakeholders



BLOCKCHAIN BASED CYBER SUPPLY CHAIN



PRELIMINARY RESULTS



Developed PoS based Energy-efficient consensus protocol

- Validators who commit transactions offer securities in the form of stakes
- Opportunistic use of under-utilized resources for realizing the consensus in energy-efficient way
- Reward of dedicating resources to maintain consensus
- Malicious actions in consensus are prevented through penalizing stake

BENEFITS

- **Auditing Cyber Supply Chain** - Provides an auditable record of software and firmware products.
- **Automating Management of Asset Life Cycle** - Track all changes to software and firmware and assets and share records among cyber supply chain participators.
- **Provenance for Authenticity** - Detect counterfeit software by tracking all changes to software and ensuring all design changes are in accordance to specifications
- **Cost-Efficiency** - Tracking of performance of the software and firmware that will help identify inefficient processes and unnecessary functionality. This will result in reducing costs associated with maintenance, operation, patching, uptime, downtime, etc.

COLLABORATION OPPORTUNITIES

Seeking collaborative opportunities from industry partners:

- Inputs on developing taxonomy for Blockchain based cyber supply chain
- Insights into incentivizing participation of stakeholders in Blockchain network

✓ Contact: sshetty@odu.edu

✓ Activity webpage: https://cred-c.org/researchactivity/assured-cyber-supply-chain-provenance-using-permissioned-blockchain

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY