RSAConference2019

San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: BAC-W12

Breaking the Blockchain: Real-World Use Cases, Opportunities and Challenges

Dr. Michael Mylrea

Senior Advisor for Cybersecurity & Blockchain Lead
Pacific Northwest National Laboratory

3/6/19 (Wednesday) 2:50 PM - Moscone South 303

Blockchain Definitions Vary Greatly and Are Rapidly Evolving

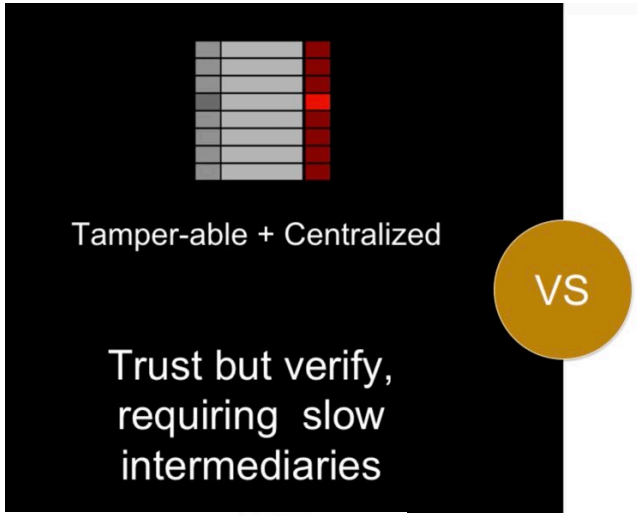
Blockchain - A distributed data base or digital ledger that records transactions of value using a cryptographic signature that is inherently resistant to modification

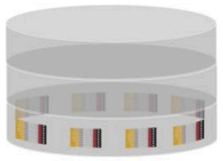
"Blockchain 2.0" - A "smart contract" represents a digital protocol that automatically executes predefined processes of a transaction without requiring the involvement of a third party

Blockchain Cybersecurity Goals

- Examine when, where and how to apply blockchain to solve complex cyber security challenges for critical energy infrastructure
- Develop blockchain smart contract for energy producers and consumers to transact and autonomously and securely regulate both supply and payment
- Increase the speed, scale and security of complex peer-to-peer transactions
- Autonomous detection of data anomalies to maintain integrity of critical systems
- Secure ledger for an array of vulnerable things
- Improve configuration management security across different enclaves
- Overcome security limitations of current cyber best practices - PKI, Patching, central data storage, etc.

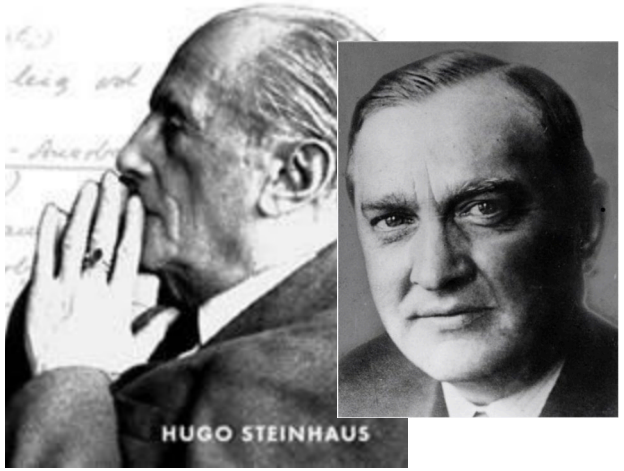
Blockchain Changes How We Trust





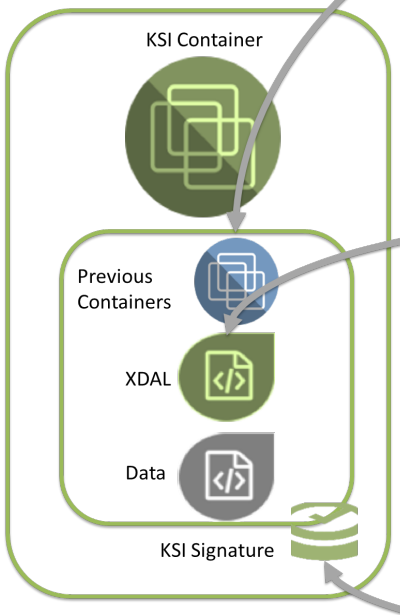
Immutable + Distributed

Trusted, immediately recorded and easily available



Blockchain is constantly in a self-reinforcing Nash Equilibrium state to keep the network Byzantine Fault Tolerant and maintain a stable state

Blockchain Provides Data Provenance and Attribution



Data Provenance
- Event Correlation
- Immutable Event History
- Data Accountability
- Data Flow Visibility
- Rollback / Remediation Inputs

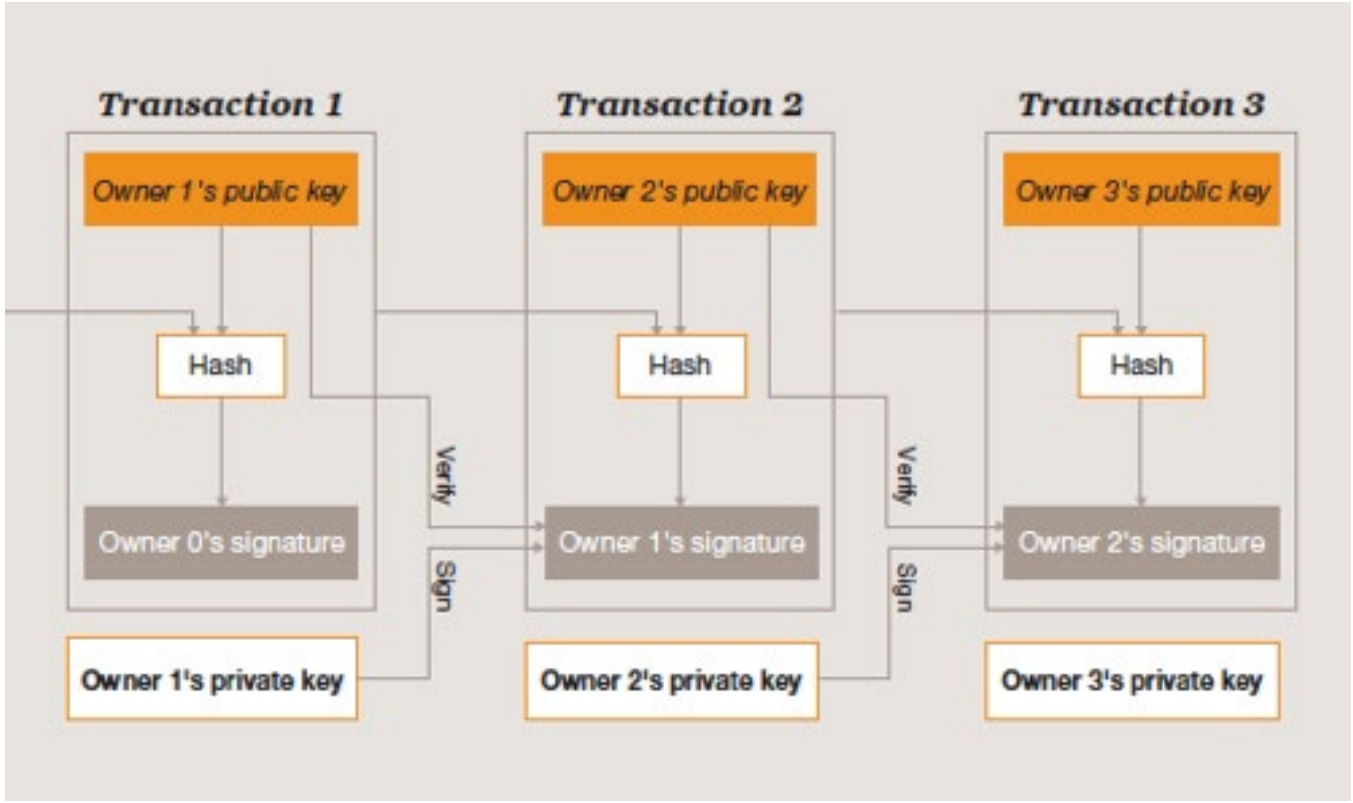
Data Attribution
- Geolocation
- Time to Live
- Data Addition Info
- Data Sharing Info
- Data Indexing and Search Tags
- Analytical Attributes

KSI Signature
- Signing Entity
- Immutable Time
- Immutable Container Authenticity
- Independent Verification

Changing How We Trust Will Disrupt Many Sectors

Blockchain Transactions – Cryptographic Proof Replaces Third-Party Intermediary

- Blockchain enables peer-to-peer transaction conducted without the assistance of any third party intermediary.
- The public key can be used to view the transaction history of a user but it cannot be used to make a transaction unless the private key is also known. The private key is what is needed to access an account and actively execute a transaction.

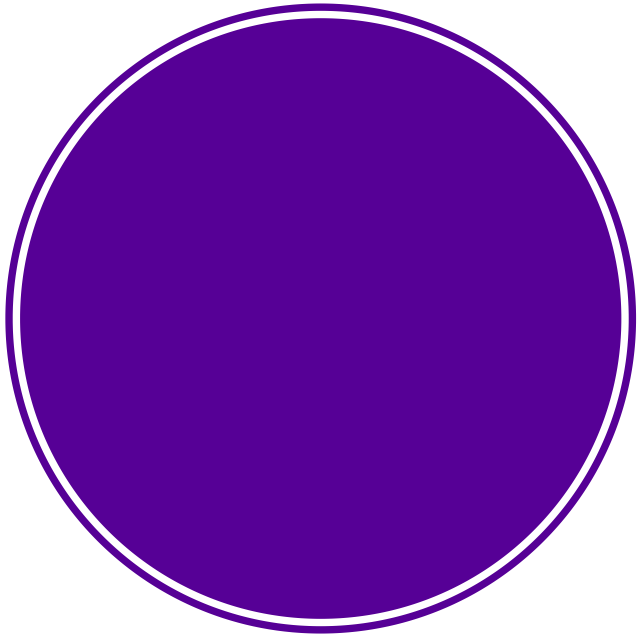


Current Cybersecurity Defenses are Not Keeping Up With Threat

Blockchain can provide a secure ledger for an Array of Vulnerable Internet of Things (IoT)

- 20.8 billion connected IoT devices by 2020 *(Gartner Inc.)*
- Spectre and Meltdown - Nearly every computer chip manufactured in the last 20 years contains fundamental security flaw
- By 2019 there will be 2 million cyber security positions that go unfilled.
- Cyber crime damage costs to hit $6 trillion annually by 2021.
- Cybersecurity spending to exceed $1 trillion from 2017 to 2021.
- Human attack surface to reach 6 billion people by 2022.
- Global ransomware damage costs are predicted to exceed $5 billion in 2017 — a 15X increase in two years and expected to worsen

Why Consider Blockchain? Current Cybersecurity Paradigms Broken and Challenge is Getting Worse!



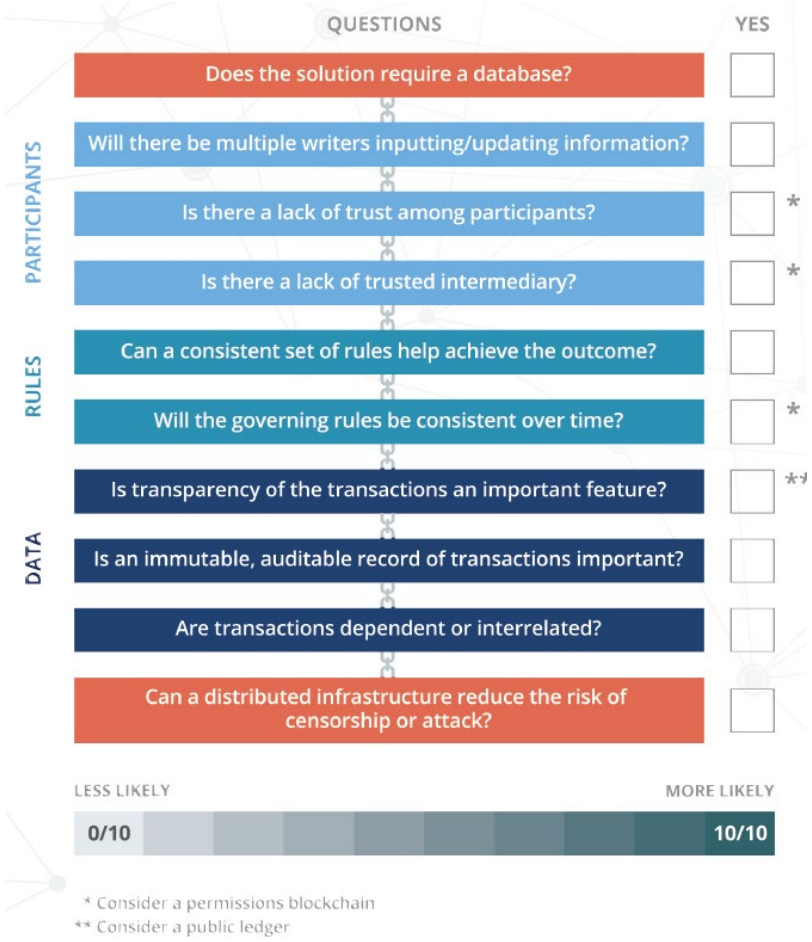
- Cybersecurity Paradigms are Broken
- Antiquated data management practices
- Security vulnerabilities and inefficiencies in how we collect, store and exchange electronic data
  - Moore's law
  - Need a secure ledger of things
  - PKI Inventory!
- Helps solve challenges with managing large data sets
- Privacy preserving Big Data
- Granular data attestation and provenance
- Cybersecurity optimization
- Smart contracts

RSAConference2019

Technical Specification Requirements to Use Blockchain

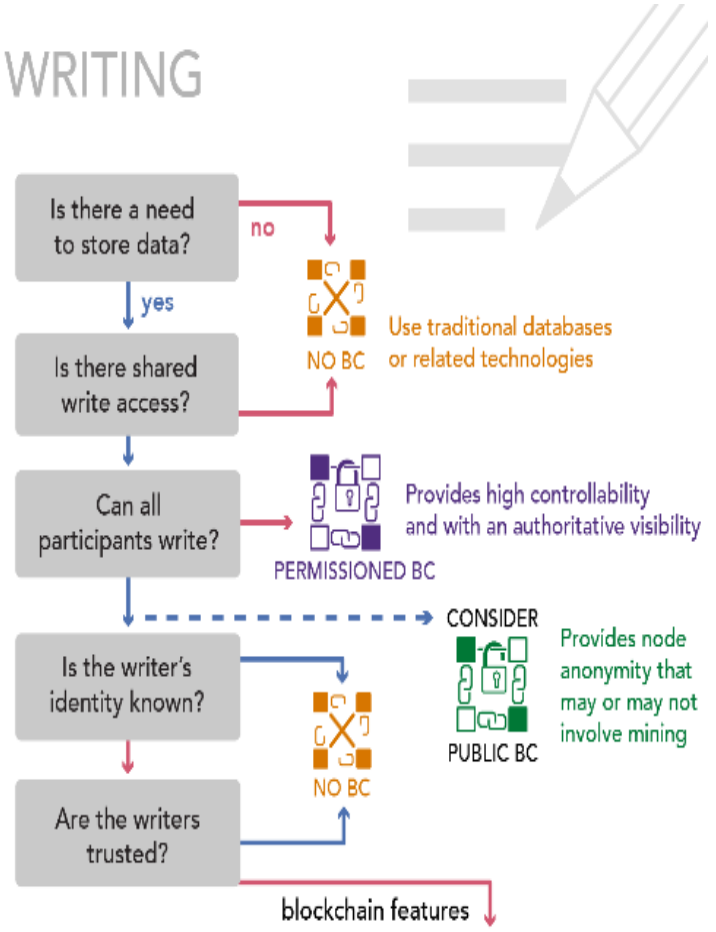
Lessons Learned

“Apply” Lessons Learned: When Should your Organization Consider Using Blockchain Technology?



Source: The Blockchain Ethical Design Framework. Georgetown University

Fundamentally, different blockchain (BC) technologies offer different “read and write” features. Although readability and writability features come with blockchains, they are also available with typical database technologies. The need to share, the writer’s identity, and trust are the key elements in this area to determine the need of a blockchain.



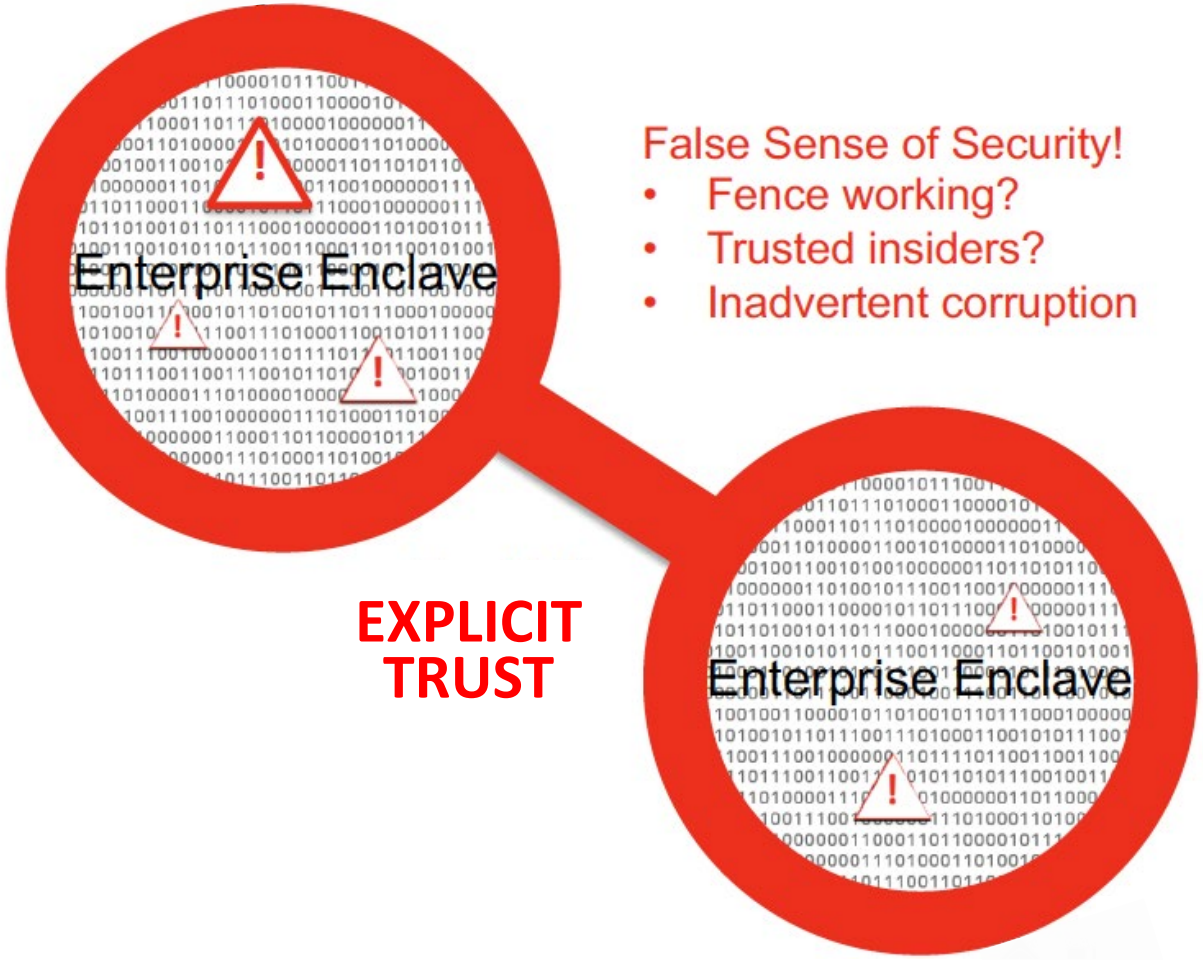
Source: Mylrea & Gourisetti, 2019

“Apply” Lessons Learned: When Should your Organization Consider Using Blockchain Technology?

- Lack resources (Expertise and $ Funding)
- Data lack trustworthiness and Integrity
- Inputs can’t be verified
- Access control costs are prohibitive
- Existing solutions with asymmetric encryption and distributed data bases sufficient
- Data ownership, access and exchanges create new challenges
- Advantage to centralized data base
- Immutability is problematic
- Maintenance sustainability is unsure

Current Cyber Security Paradigms Broken for IoT Environments

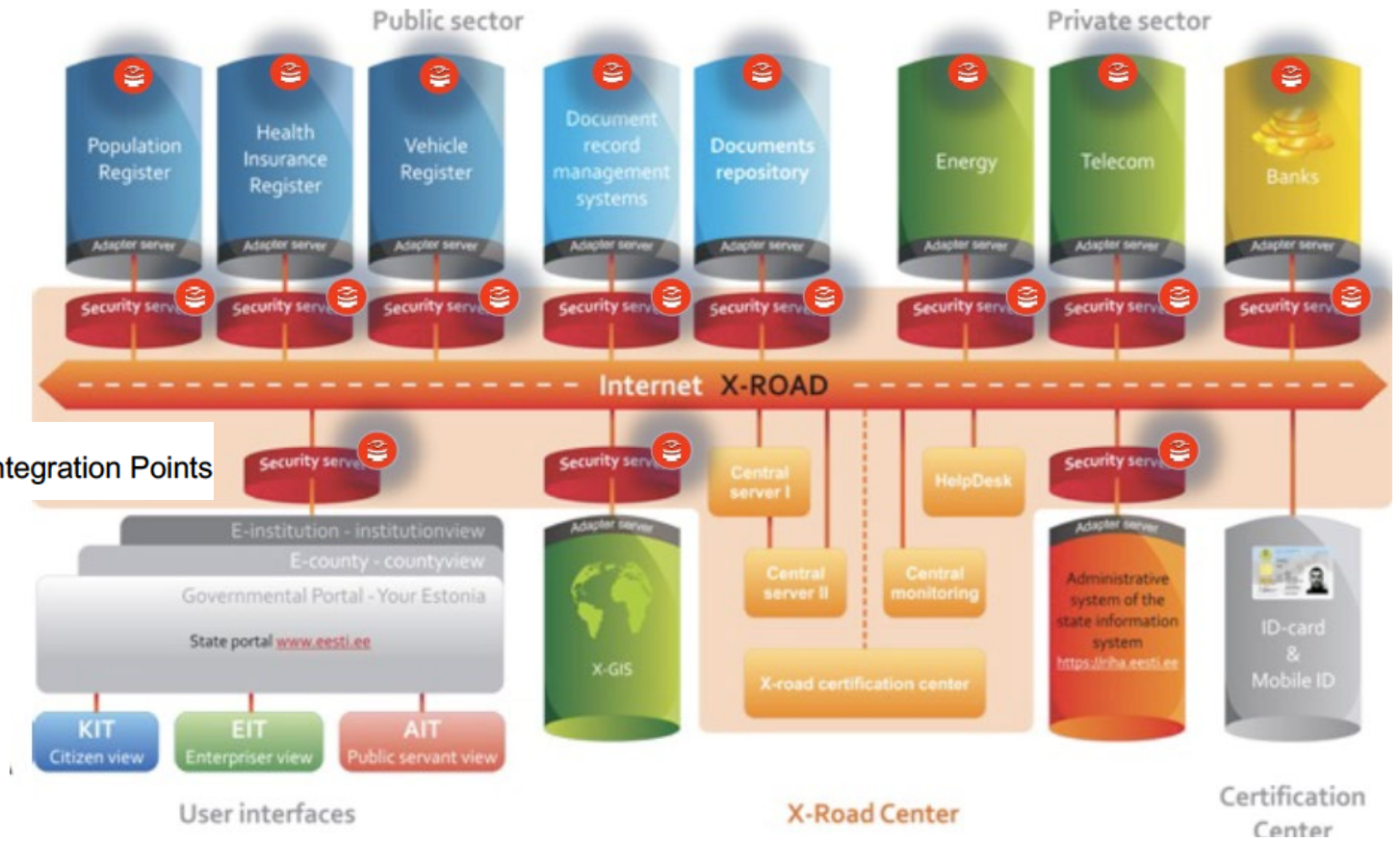
1. Perimeter control
2. Firewalls
3. Intrusion Detection System
4. Trusted insiders
5. Data in vaults
6. Security Event Monitoring Systems
7. Trusted Connections
8. Trust Partner's Security



Estonia's Use of Blockchain

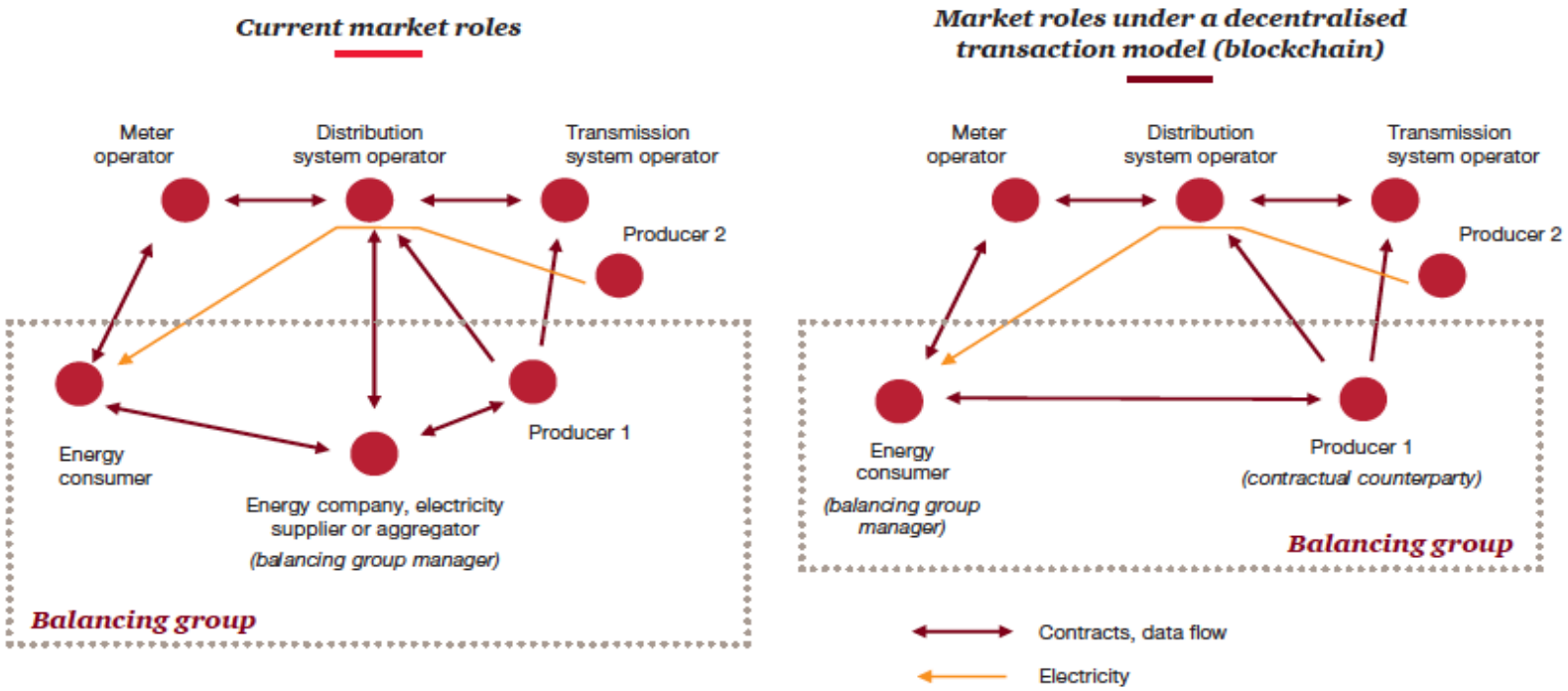
Guardtime's KSI Blockchain is implemented as an integrity layer throughout Estonian Government Networks.

There is complete transparency and accountability between citizens and government.



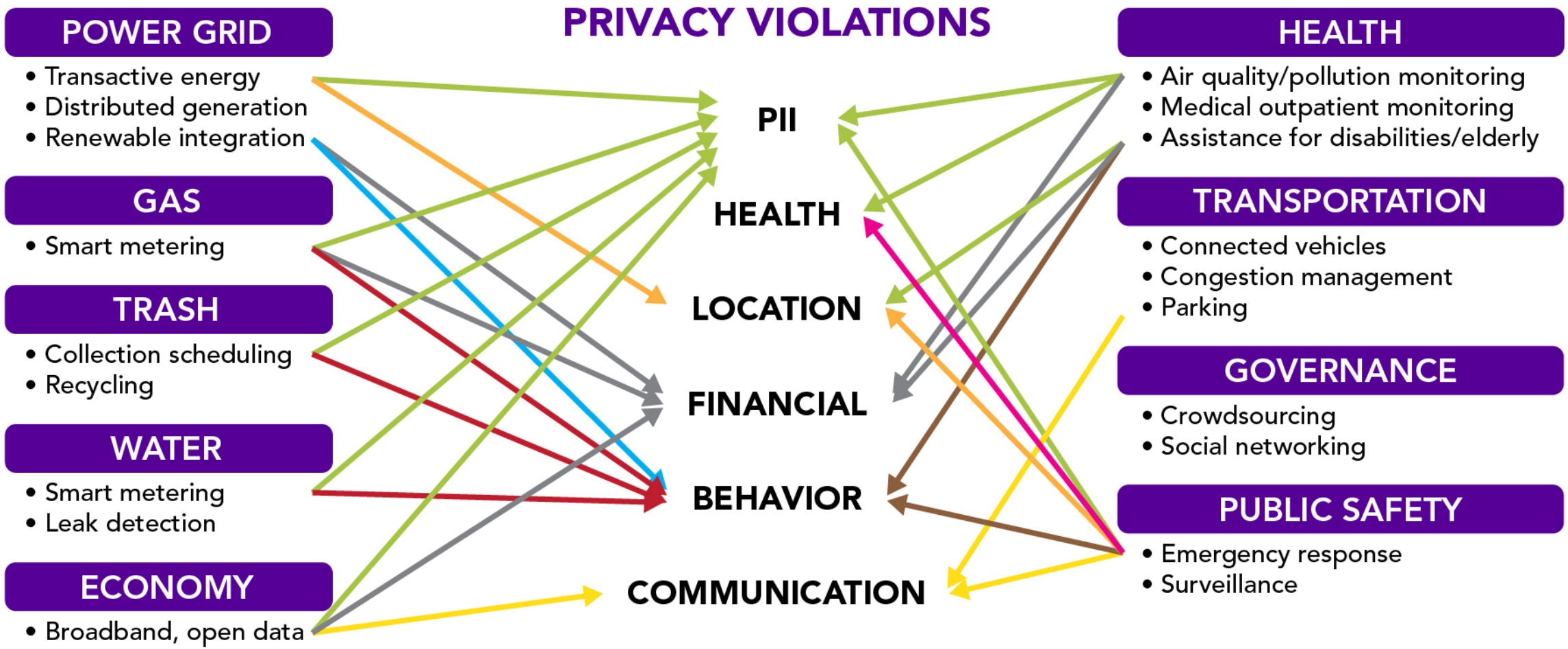
- Proves when the "Something" was submitted
- Wide distribution and publication – anyone can do the calculations
- One-second rounds ensure fast response for proof of participation

Application to Energy Sector – A More Secure Decentralized Energy Transaction and Supply System

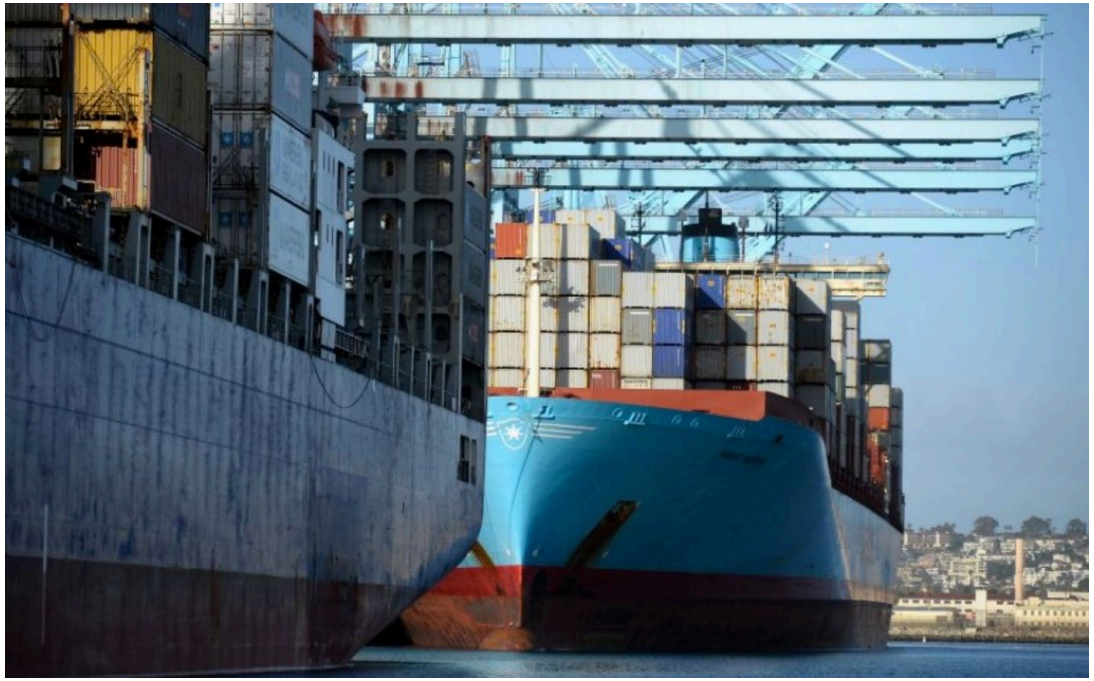


Potential radically simplify today's multi-tiered system, in which power producers, transmission system operators, distribution system operators and suppliers transact on various levels, by directly linking producers with consumers

Blockchain for Data Privacy & Security



Blockchain – Securing Critical Complex Systems of Systems with a Changing Risk Profile



Next Gen – Actural Services Autonomous Dynamic Supply Chain Security

Configuration Management Security for Complex Systems

Source: http://www.cityam.com/271486/ey-maersk-and-microsoft-putting-boats-blockchain-marine

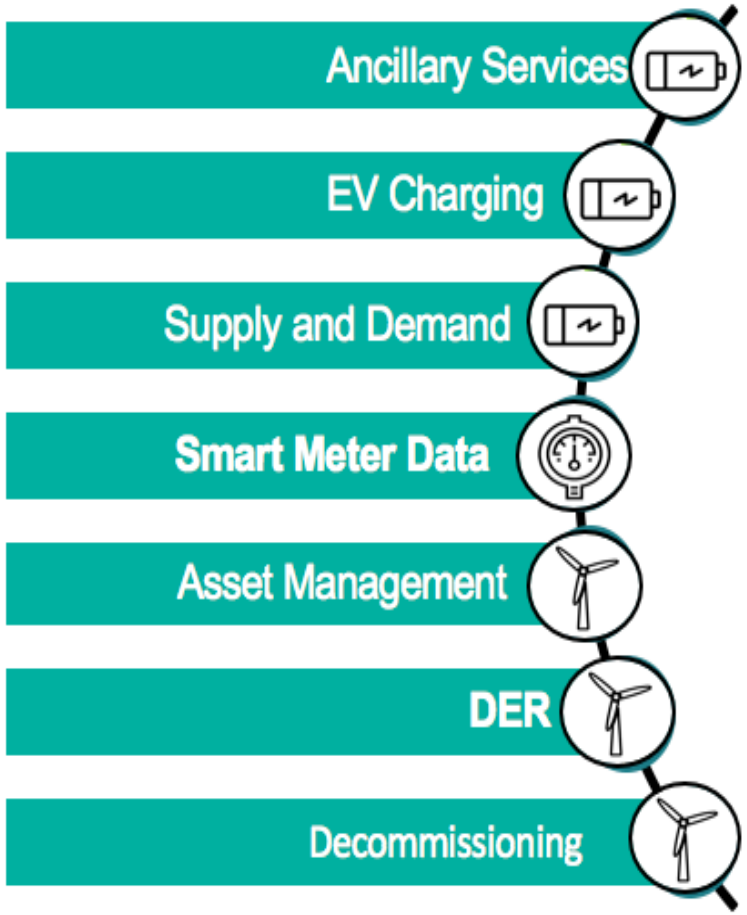
RSAConference2019

Real World Use Cases

Lessons Learned

Secure Ledger of Things for Internet of Things

Blockchain Enables Multiple Use Cases Across the Energy Environment and Utilities Value Chain



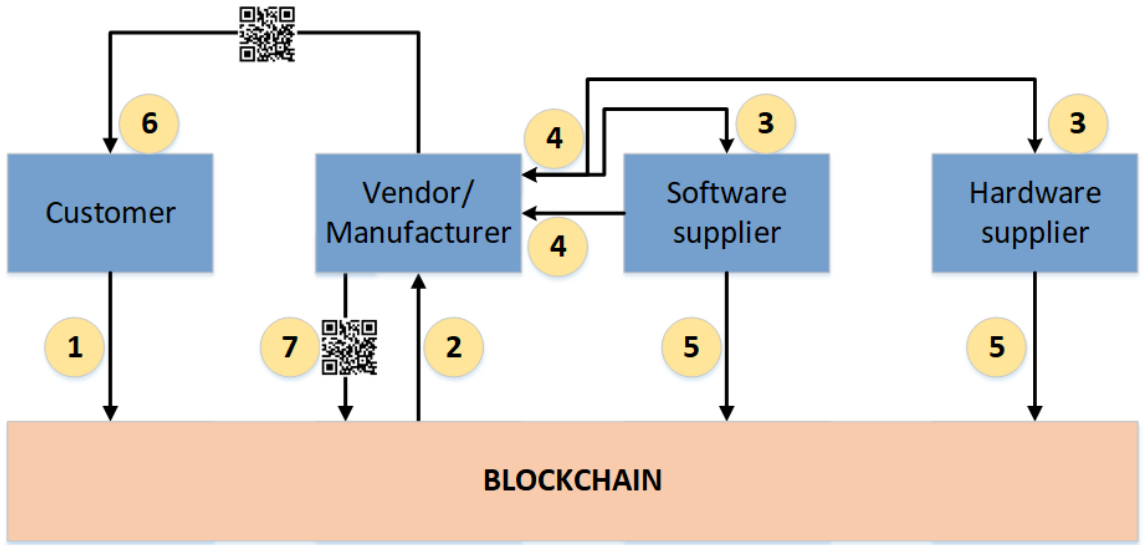
Source: Neil Gerber, IBM Hyperledger

Cybersecurity Use Cases

Physical Supply Chain	Secure Records Management	IoT Management and Control	Cloud Management and Control	Digital Lifecycle Management
• Cross Organizational Track and Trace • Distributed Anti-Counterfeit • Enhanced Visibility, Traceability, and Accountability • Distributed Single Point of Truth • Feedback Loop and Customer Empowerment	• Cross Organizational Workflow Execution • Federated Records Processing • Portable Record Version and Processing History • Distributed Single Point of Truth • Cross Boundary Event Accountability	• Streamlined Version Control • Configuration and Update Control • Decentralized Onboarding and Device Identity Management • Cryptographic Data Capture and Provenance • Dynamic D2D Communities	• "In-Cloud" Composite Event Capture and Distribution • Streamlined Event Correlation and Baseline Comparison • Decentralized Control and Alerting Capabilities • Streamlined and Portable Remediation, Evidence and Proof • Composite Insider Threat Awareness	• Cross Organizational Application Vetting and Reuse • Secure Version Control • Cryptographic Regression Proof • Linked Test, Results, and Configuration Proofs • Accountable and Verifiable SDLC

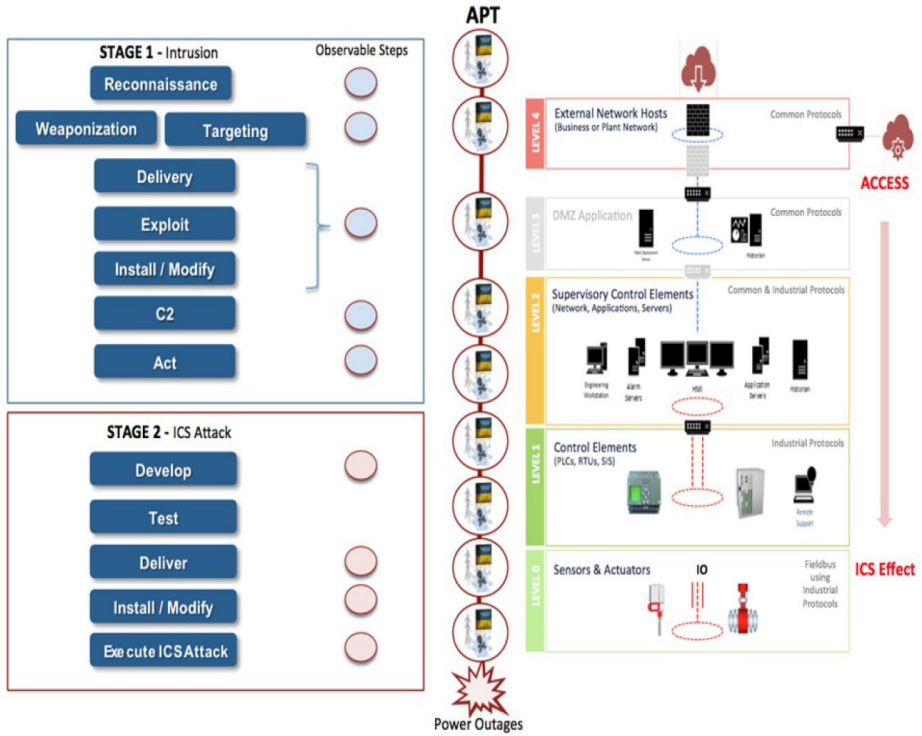
Use Case 1: Supply Chain Security

- Spectre and Meltdown – Nearly every computer chip manufactured in the last 20 years contains fundamental security flaw



1. **Order placement:** Customer pushes "must haves", system requirements to blockchain
2. Vendor picks up the order
3. Vendor approaches suppliers (software, hardware, etc.) for principle components
4. Suppliers provide the required principle components
5. Supplier pushes the principle component information to the blockchain
6. Vendor dispatches the system with QR code to customer. Scanning the code would list all information about principle components, risks, vulnerabilities and other data
7. Vendor pushes system information (risks, vulnerabilities, and other data) to blockchain

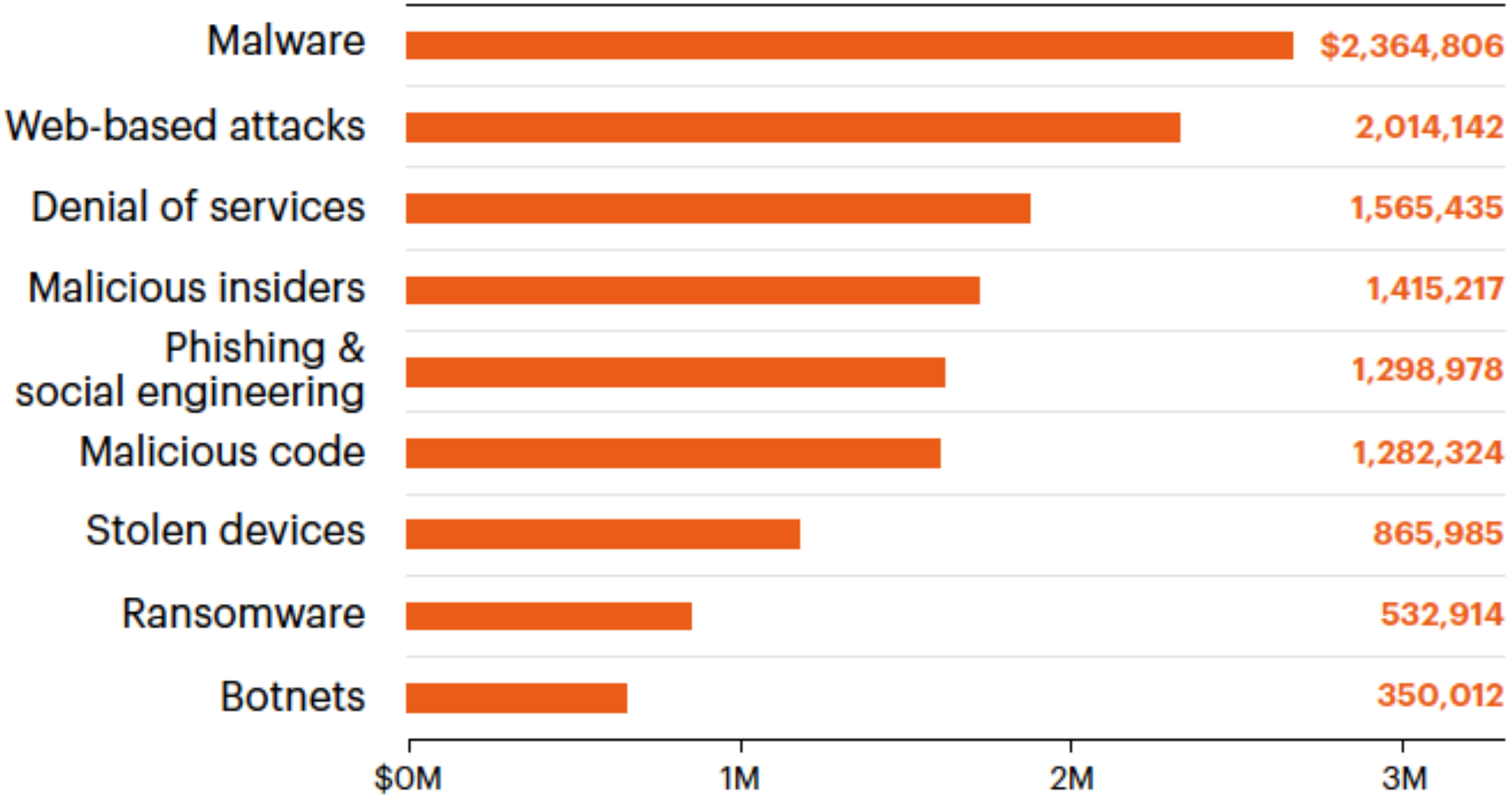
Use Case 2: Integration of Blockchain to Prevent Configuration & Identity Management Cyber Vulnerabilities



'Crash Override': The Malware that Took Down a Power Grid

How Hacked Water Heaters Could Trigger Mass Blackouts

Use Case 3: Asset Management and Governance

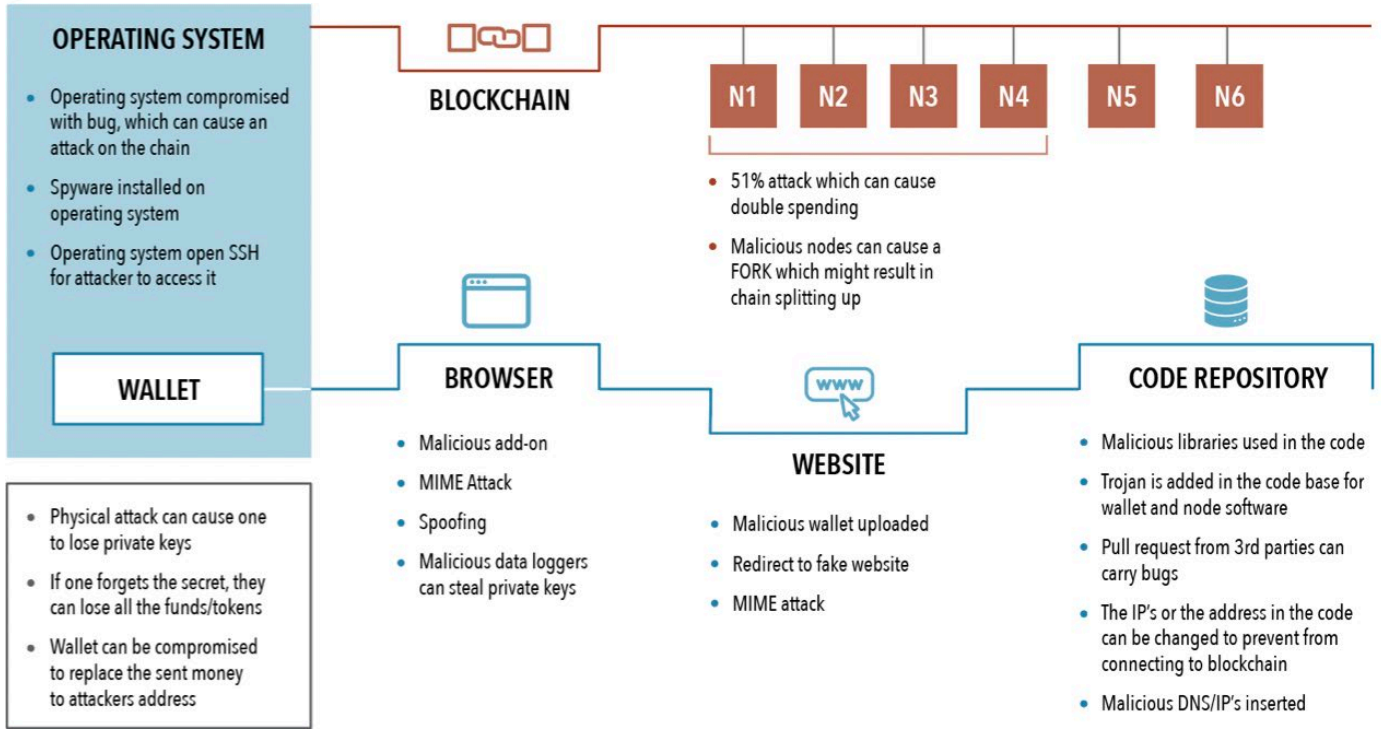


RSAConference2019

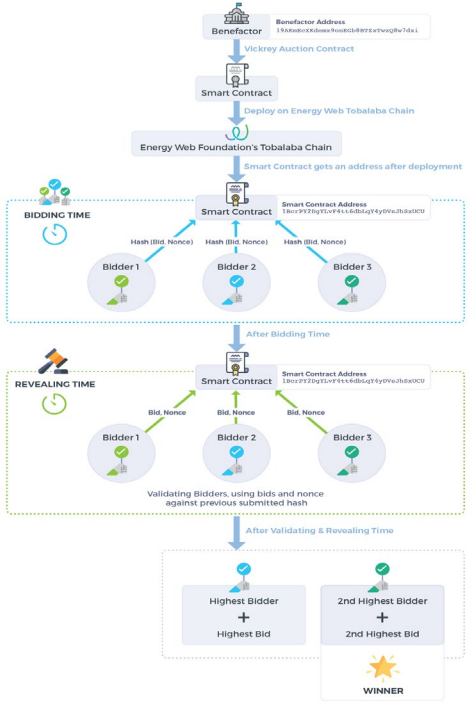
Blockchain Challenges

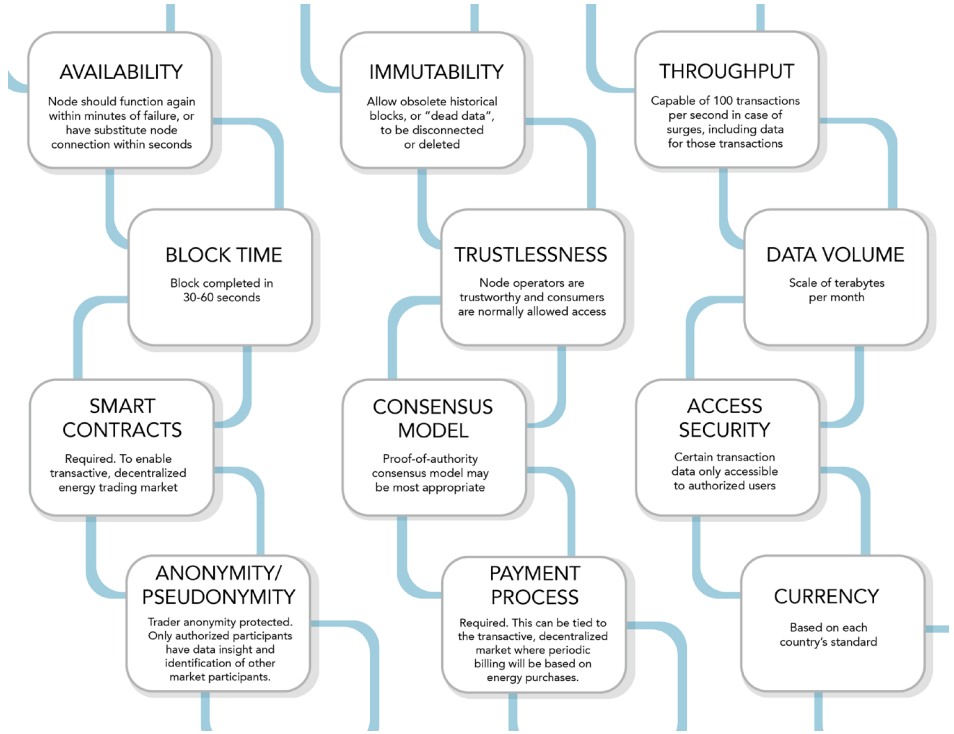
Lessons Learned

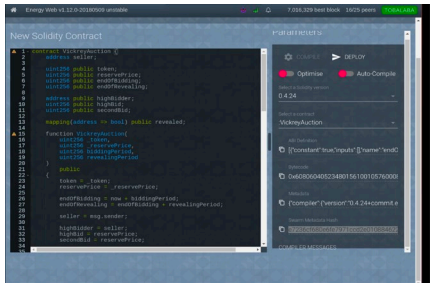
- Lack of policy and procedures and agreed upon definitions
- Resistance to change, culture, leadership
- Lack of legal, regulatory, standards
- Workforce development & education
- Interoperability & scalability
- Making changes in immutable ledgers is tough!
- Server location
- Transaction speed and latency, legacy systems, flat it – ot networks
- Cyber security
- Human error – how do we protect us from ourselves?
- Length of blockchain
- Complex systems of systems – remain complex systems



Blockchain Smart Contract Test Bed







Vickrey Auction

Dr. Michael Mylrea

Senior Advisor, Cybersecurity & Energy Technology | Blockchain Lead

Pacific Northwest National Lab

michael.mylrea@pnnl.gov