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

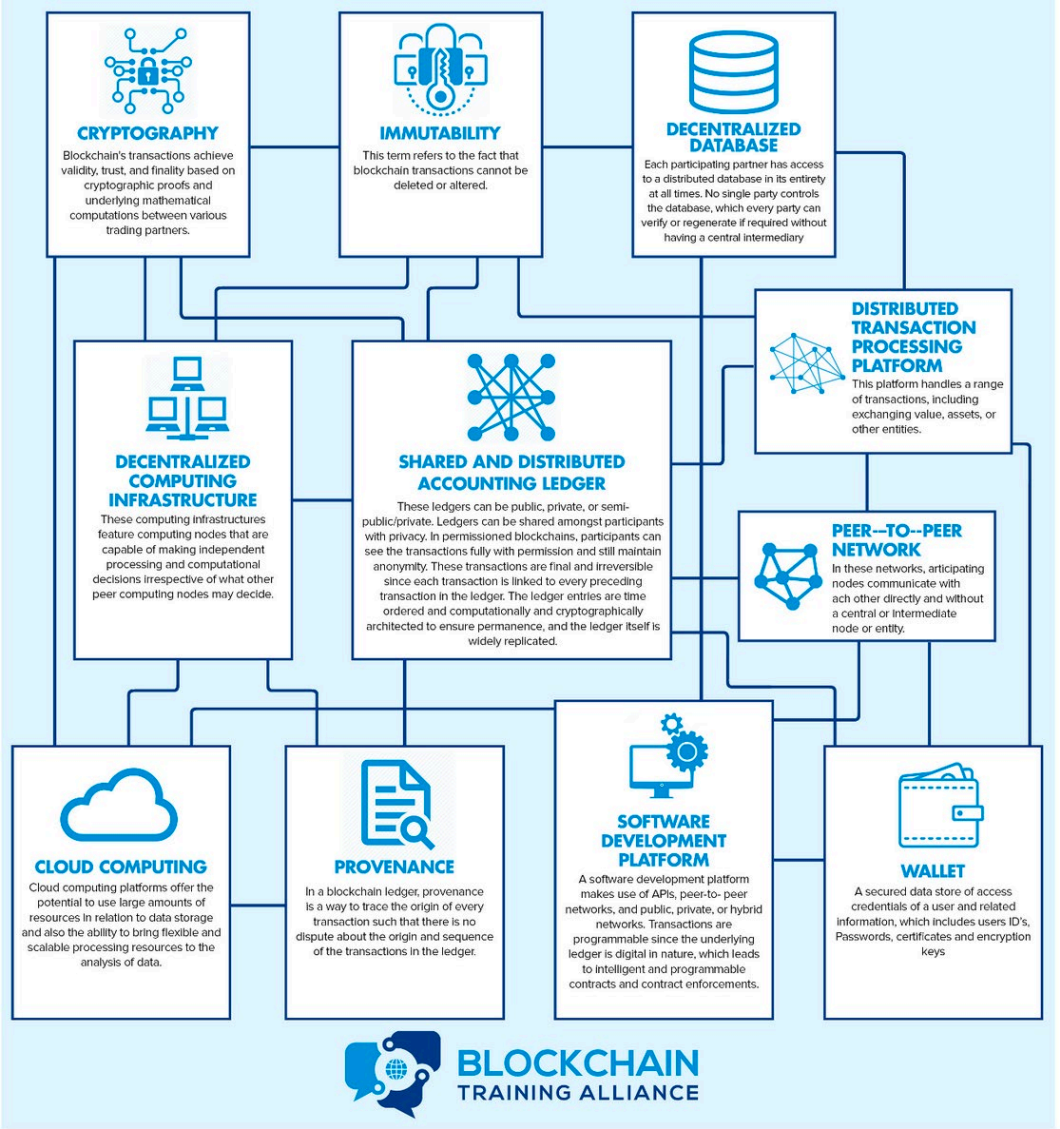
#RSAC

Blockchain Definitions & Use Cases Vary Greatly and Are Rapidly Evolving

BLOCKCHAIN

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

“Blockchain “Smart Contract” represent a digital protocol that automatically executes predefined processes of a transaction without requiring the involvement of a third party

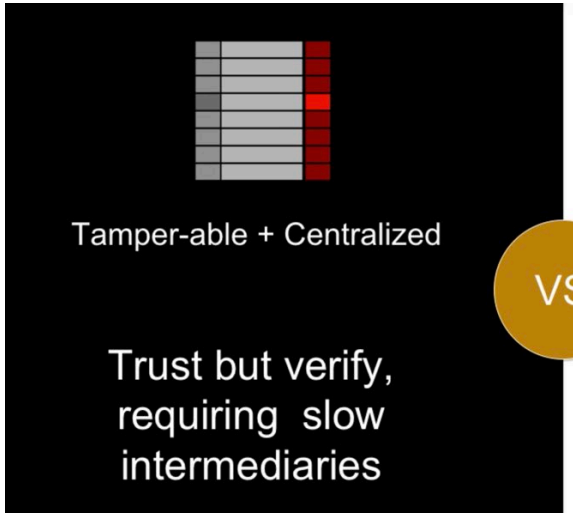


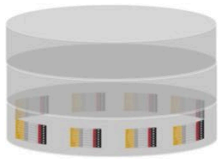
Blockchain Use Cases and Goals

Various project partners, board members and advisors from industry, academia and government

- 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 more autonomously and securely and to regulate both supply and payment
- Increase the speed, scale and security of complex peer-to-peer transactions to accelerate decarbonization and decentralization
- More autonomous detection of data anomalies to maintain integrity of critical systems
- Secure ledger for an array of vulnerable things
- Improving asset management management and supply chain security

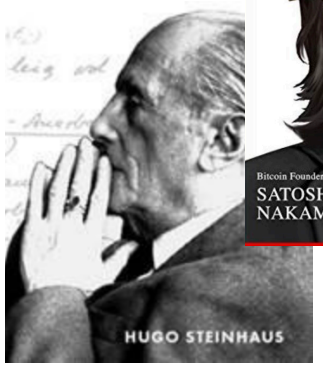
Blockchain Changes How We Trust





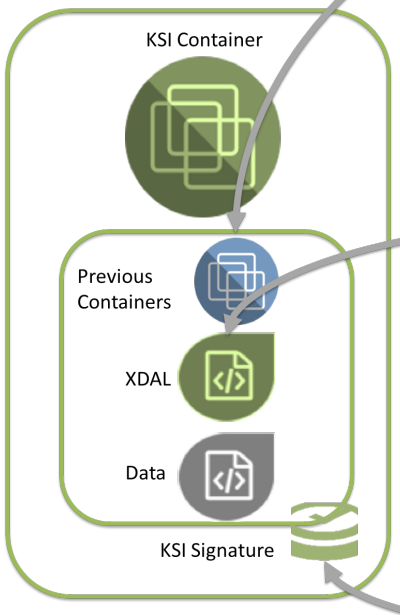
Immutable + Distributed

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



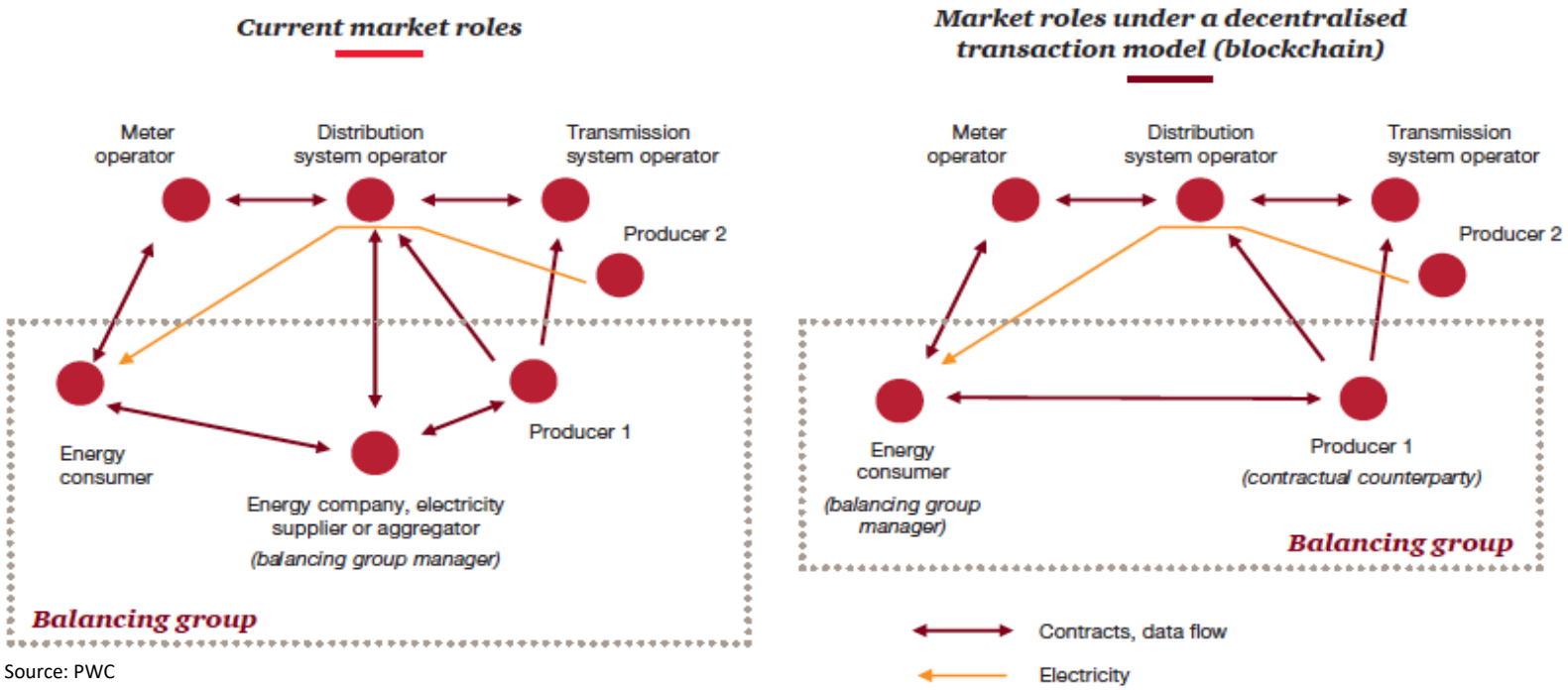
Data Provenance
- Event Correlation
- Immutable Event History
- Data Accountability
- Data Flow Visibility
- Rollback / Remediation Inputs

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

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

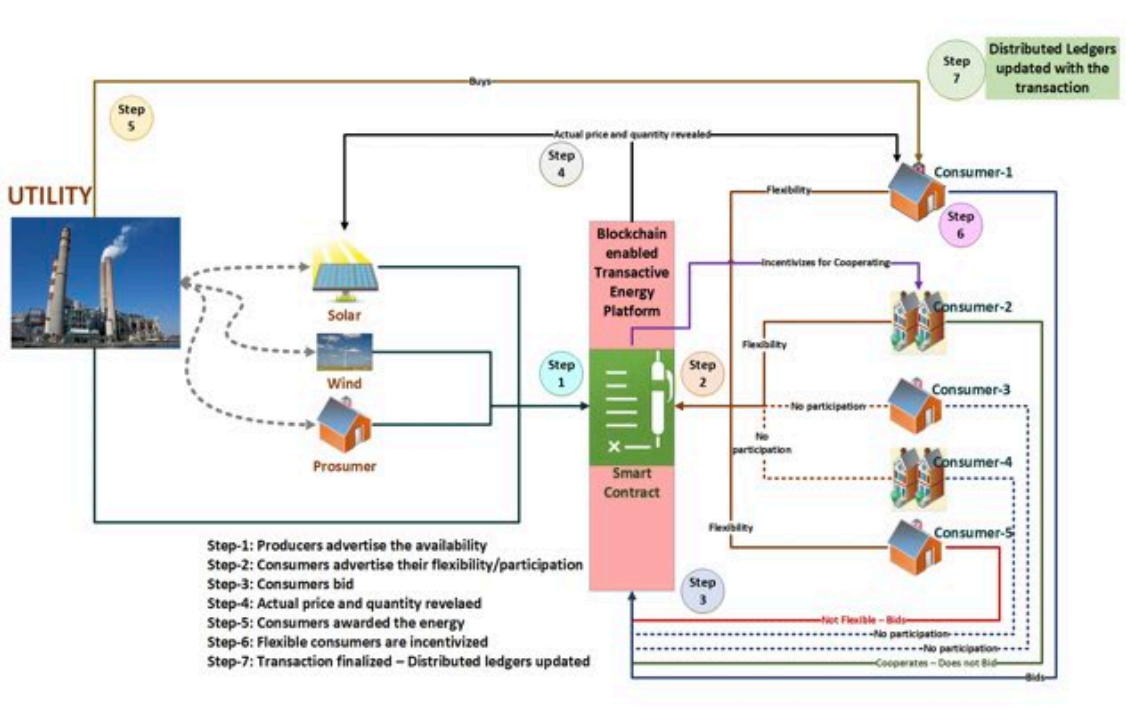


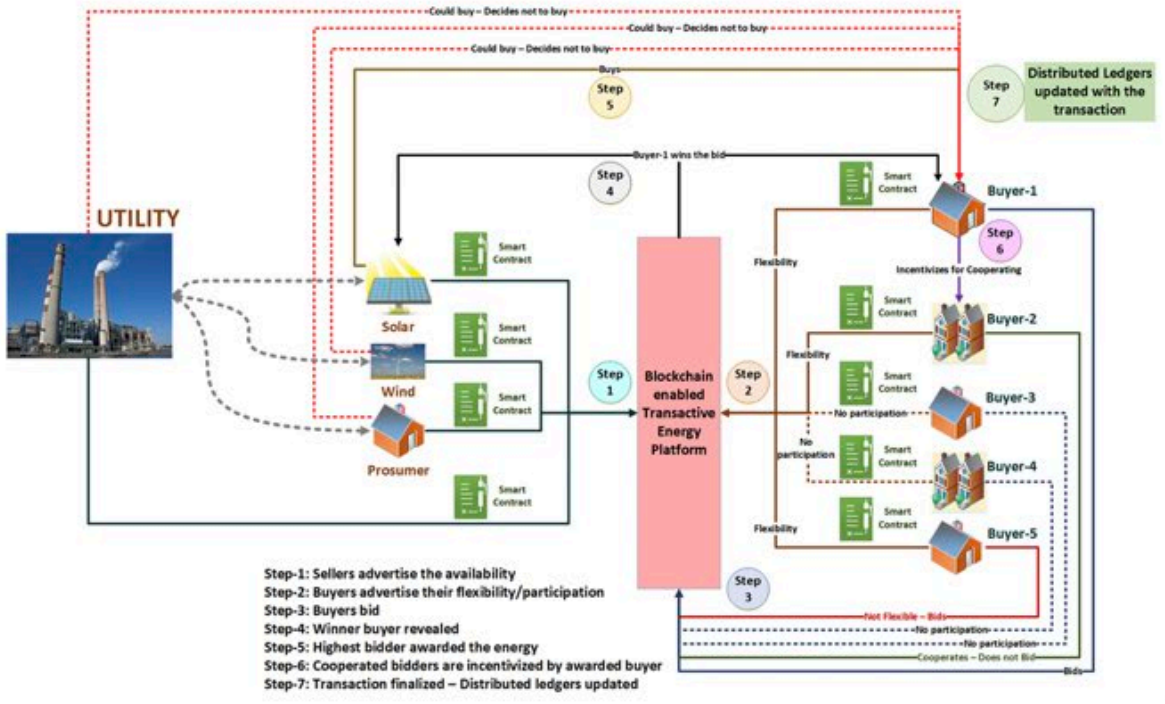
Source: PWC

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 Transactions – Cryptographic Proof Replaces Third-Party Intermediary

- Blockchain enables peer-to-peer transactions conducted without the assistance of a 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.





Source: Mylrea & Gourisetti

Applying Blockchain Technology to Solve Complex Cybersecurity Challenges with Operational Technology

Pacific Northwest
NATIONAL LABORATORY

RSAConference2019

Blockchain Shows Potential to Increase Trustworthiness of an Array of Vulnerable Things

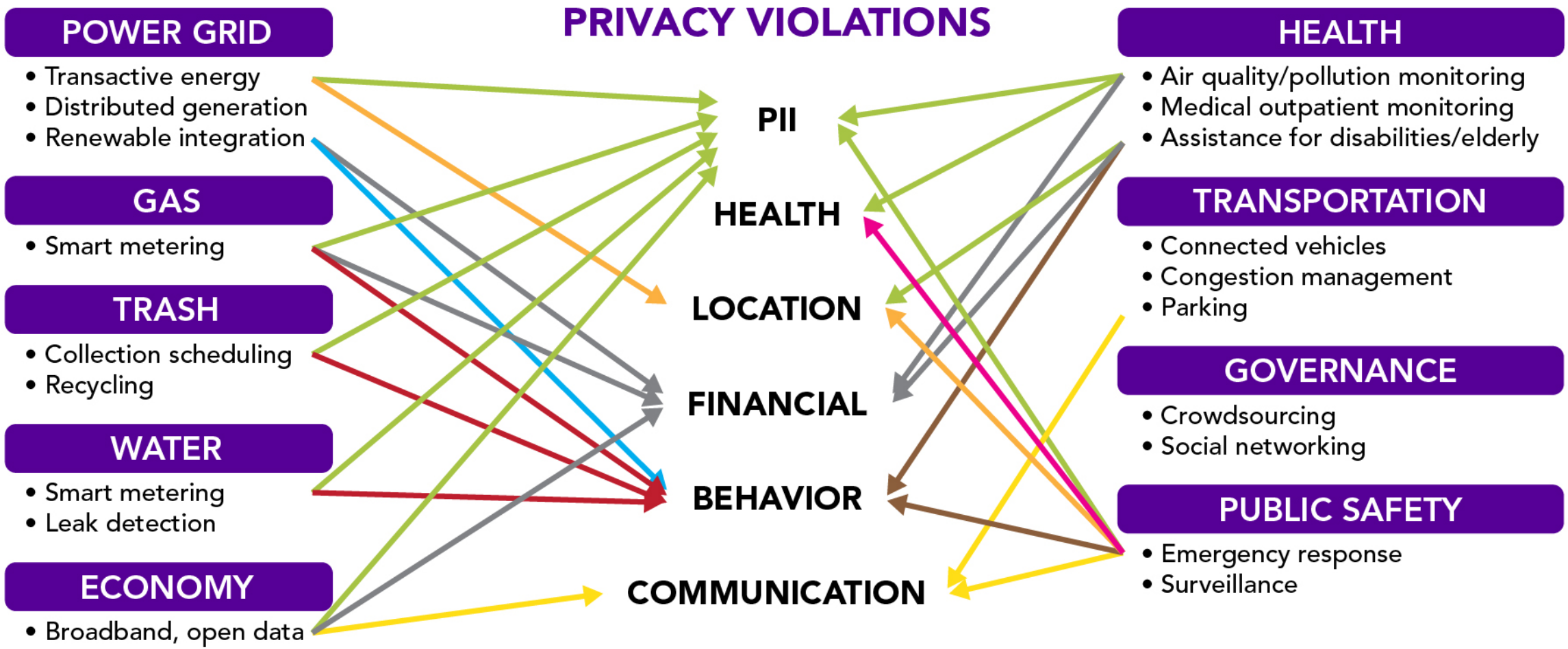
Cyber And Physical Systems, IT and OT, are Converging In Critical Infrastructures Expanding the Attack Surface

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

Blockchain for Data Privacy & Security



What have we learned from real world use cases?

Use Cases & Lessons Learned

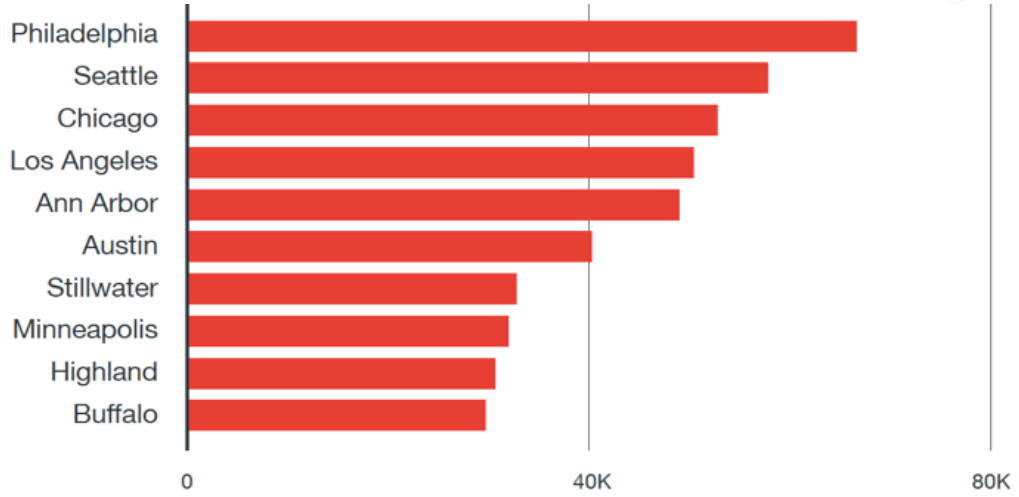
Lessons Learned & Recommendations

- Know Your Critical Cyber Assets
- Monitor Your Critical Cyber Assets
- Test & Understand Risk Associated with Critical Cyber Assets
- Legacy facility related control systems are not “Smart,” safe or efficient
- A lot “Smart” industrial controls systems are NOT Cyber smart

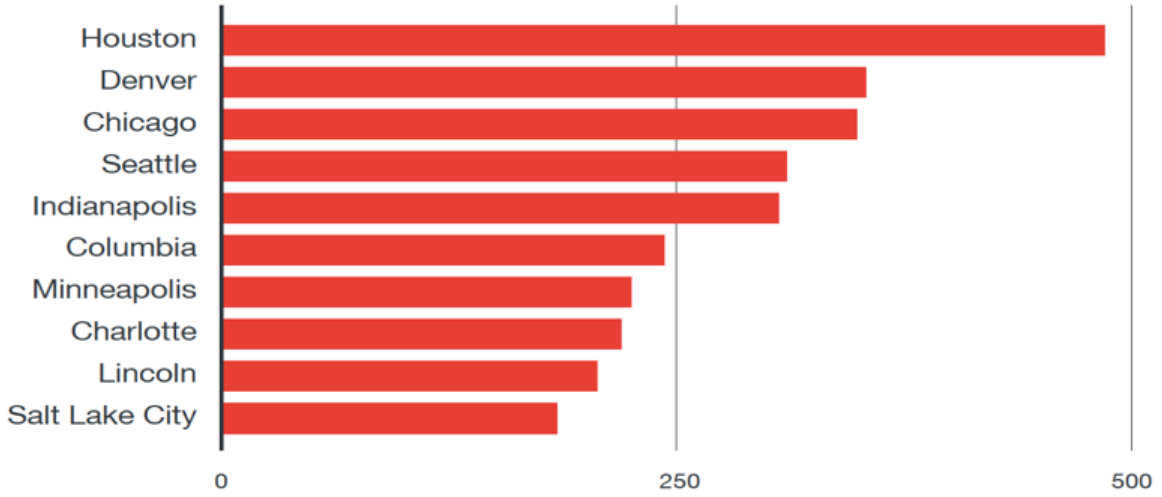
HOW HACKED WATER HEATERS COULD TRIGGER MASS BLACKOUTS

Pacific Northwest NATIONAL LABORATORY

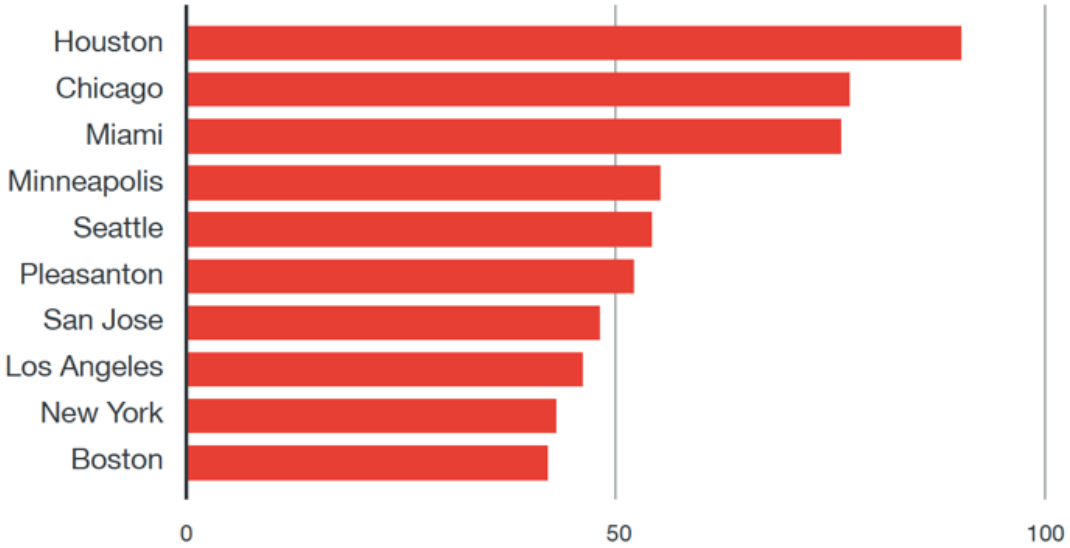
Publicly Exposed Systems



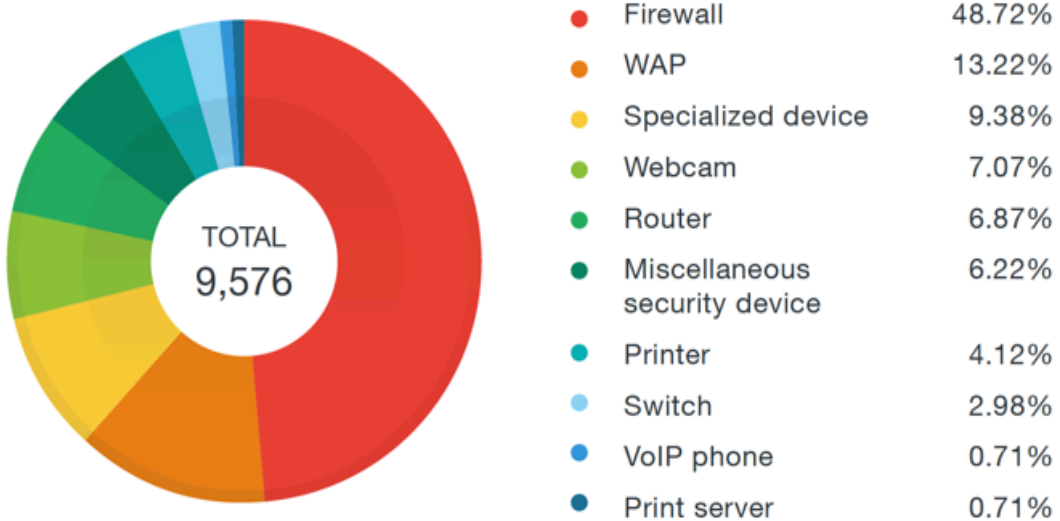
Education



Energy



BacNet Facilities

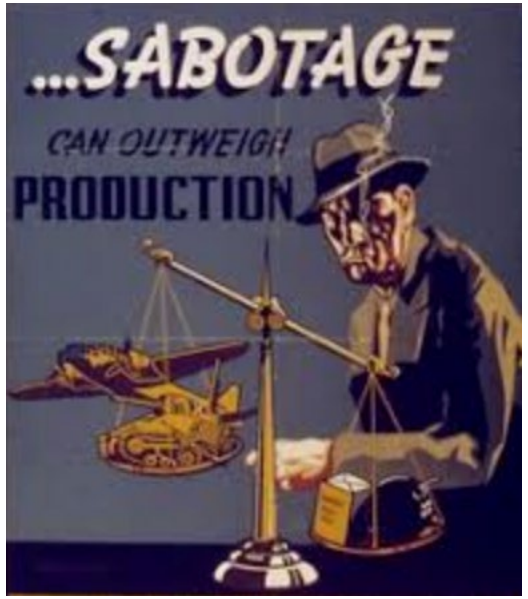


Government

Source: Trend Micro

FAREWELL DOSSIER – Supply Chain Attack

Use Cases & Lessons Learned



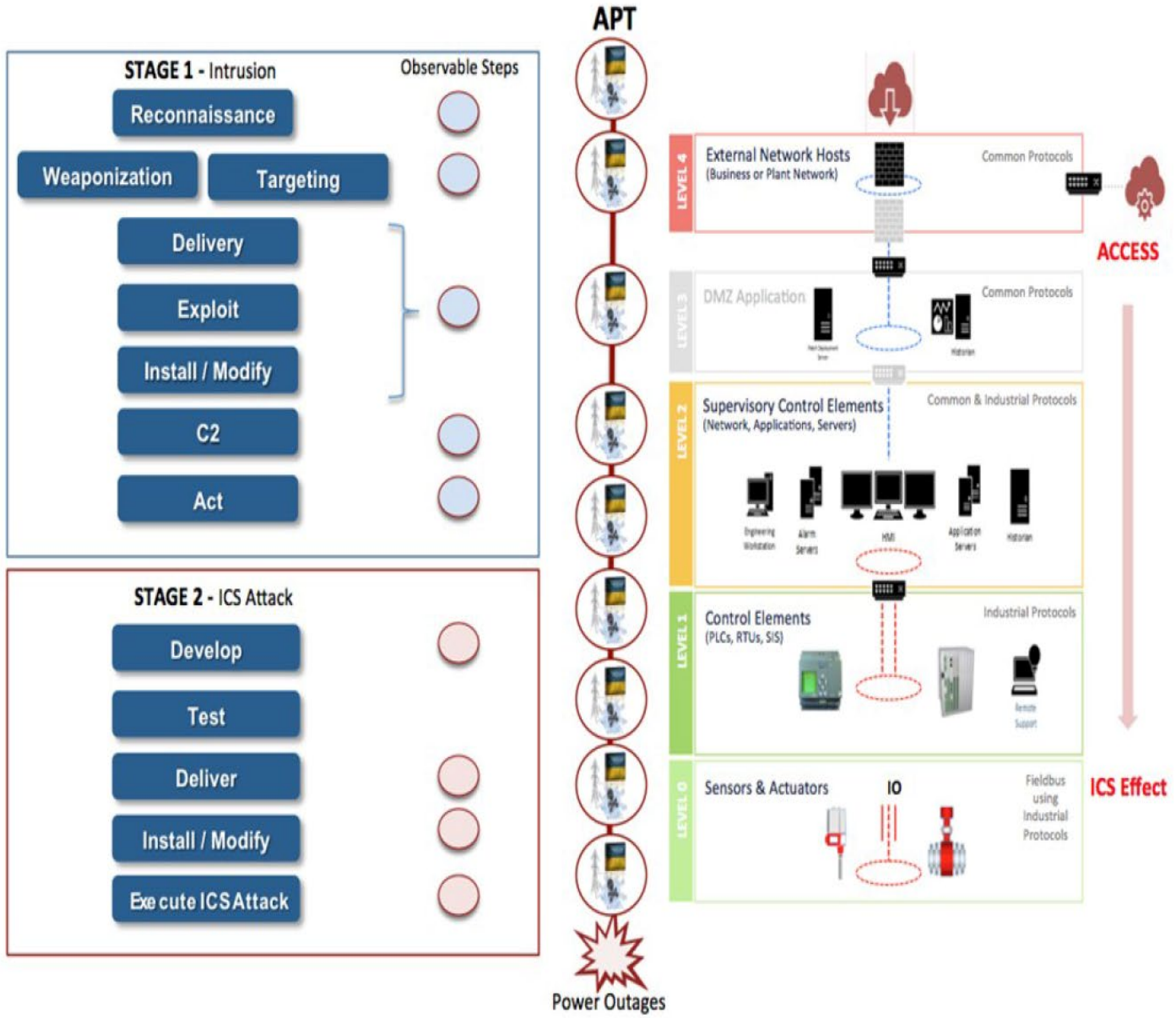
- Global supply chains are becoming increasingly challenging to secure
- Cyber-physical foot print growing.
- A number of precedents where cyber/digital attack caused physical damage

"The pipeline software that was to run the pumps, turbines and valves was programmed to go haywire, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to the pipeline joints and welds. The result was the most monumental non-nuclear explosion and fire ever seen from space."

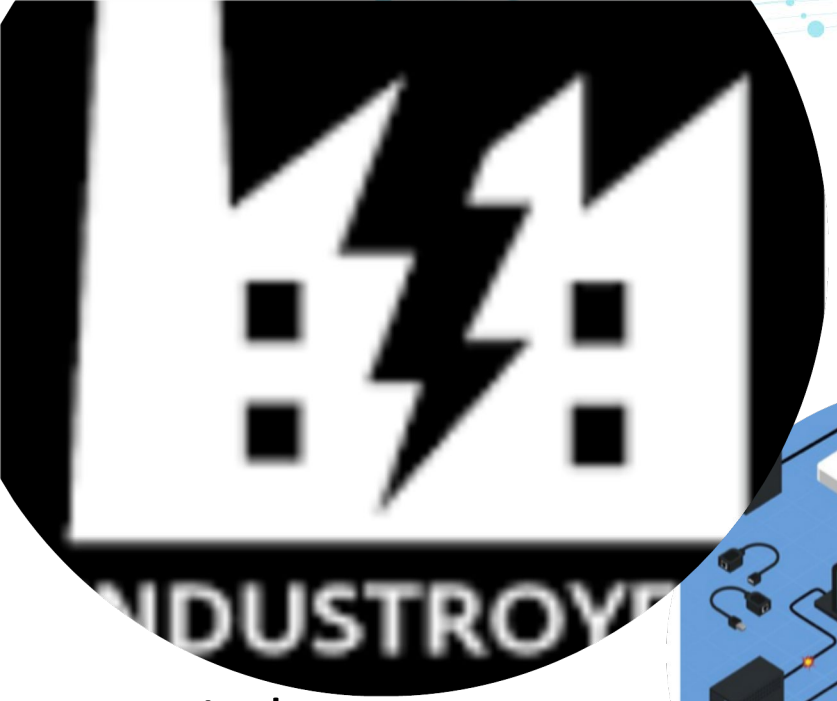
Use Cases & Lessons Learned

Lessons Learned & Recommendations

- Know and Monitor Your Critical Cyber Assets
- Do Not Run A Flat Network - Segregate & Secure Critical IT & OT Networks
- Cyber Policies Should Help Protect Us From Ourselves
- Hackers Often Use Very Basic Tactics to Hack Very Vulnerable Systems
- Implement Password Management Controls, Firewalls, Encryption & Configuration Policies



Use Cases & Lessons Learned



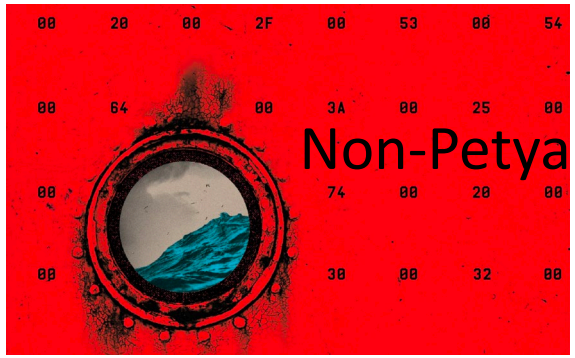
Industroyer

Wanna Cry

Devil's Ivy

Hack Brief: 'Devil's Ivy' Vulnerability Could Afflict Millions of IoT ...
apple.news

HACK BRIEF: 'DEVIL'S IVY' VULNERABILITY COULD



Non-Petya

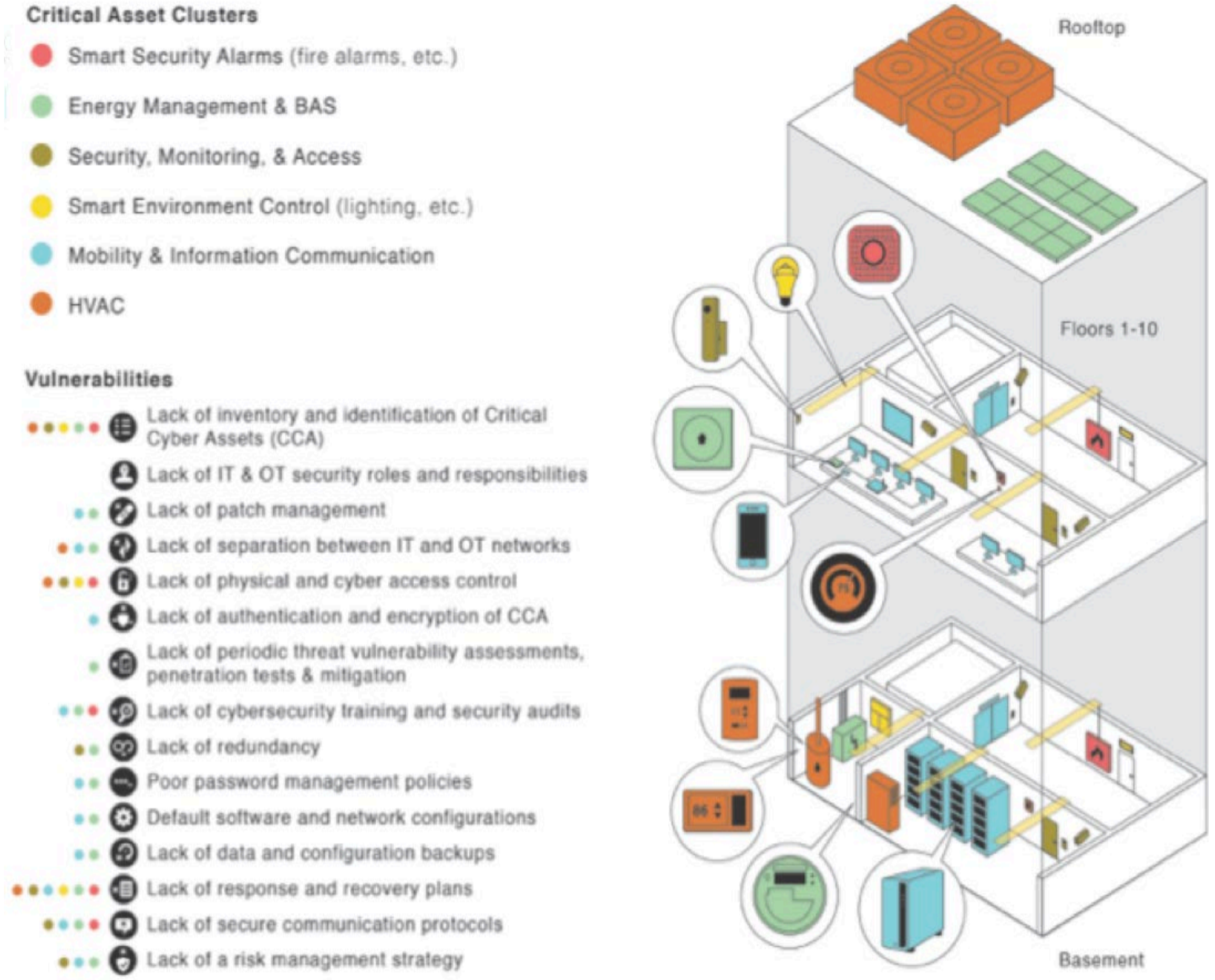
Lessons Learned & Recommendations

- Cyber threats are evolving faster than control system defenses
- Cyber security starts with smart supply chain security, smart procurement and provisioning of devices
- Though it is easy to find vulnerabilities, you can make it tough to exploit them
- Patch early, Patch often, Patch Smart
- Security is a continuous process that requires active management of cyber risk

Use Cases & Lessons Learned

Lessons Learned & Recommendations

- **Get the basics right:** Critical facilities lack basic cybersecurity risk management
- **Inventory:** If don't know your critical cyber assets you can't protect them
- **Trust the process:** Cybersecurity is a continuous process, not an end state.
- **Culture:** A holistic response is required to mitigate a complex, evolving and non-linear threat.



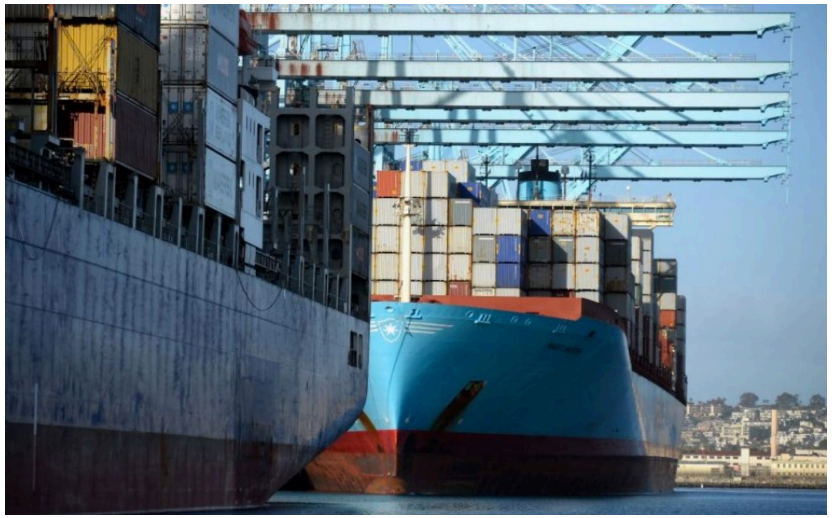
Pacific Northwest NATIONAL LABORATORY

Technical Specification Requirements to Use Blockchain

Pacific Northwest
NATIONAL LABORATORY

RSAConference2019

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

Avoiding The Vulnerabilities of Centralized Single Points of Failure for Critical Defense and Weapons Systems

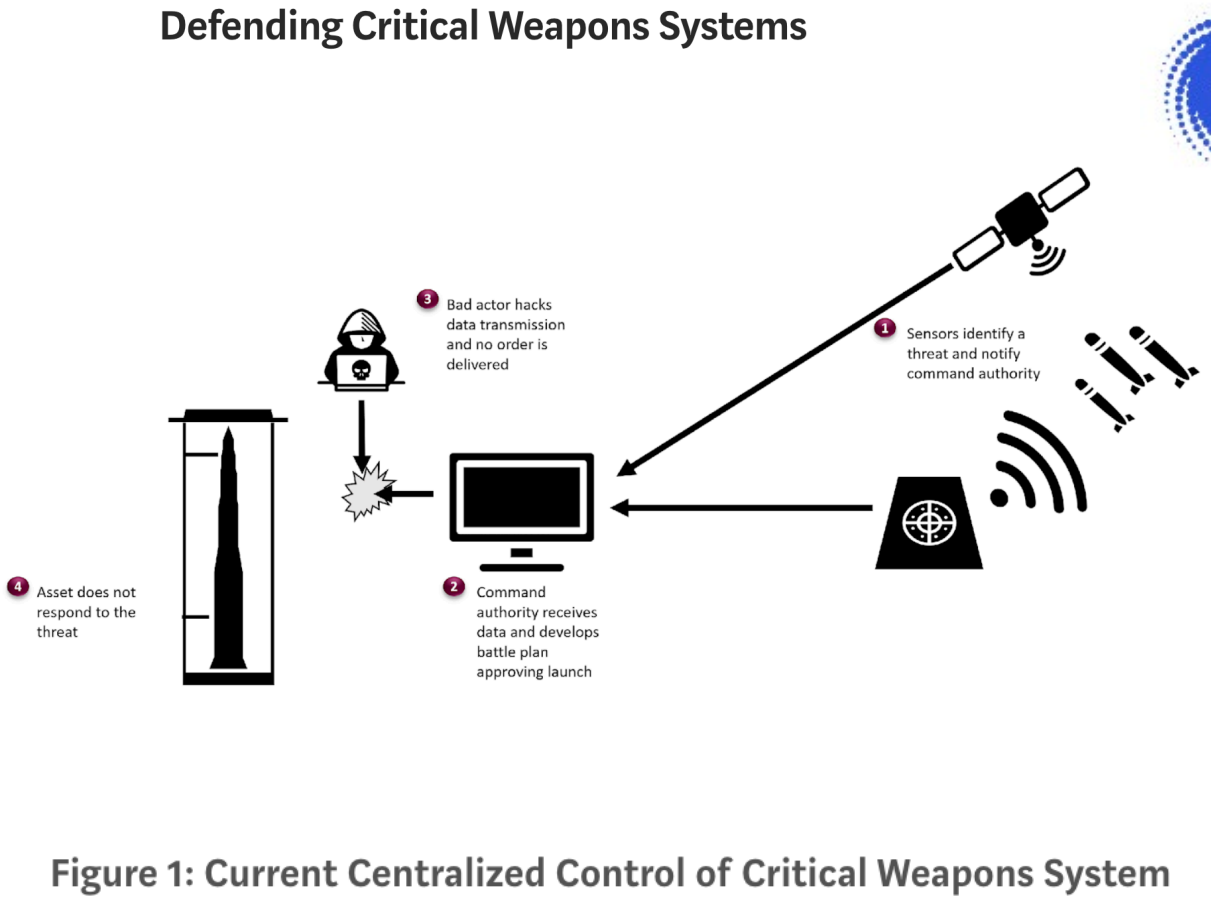


Figure 1: Current Centralized Control of Critical Weapons System

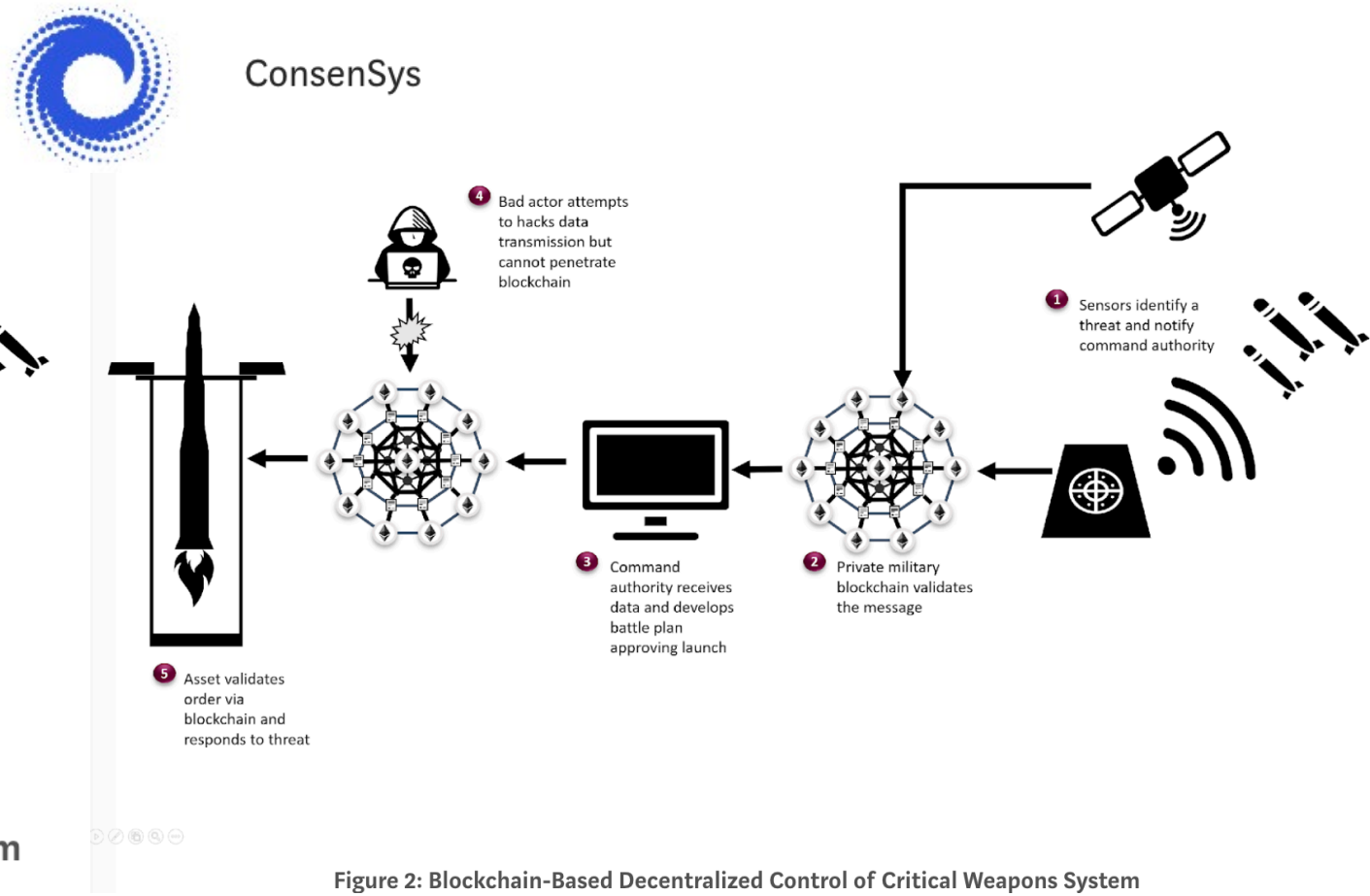


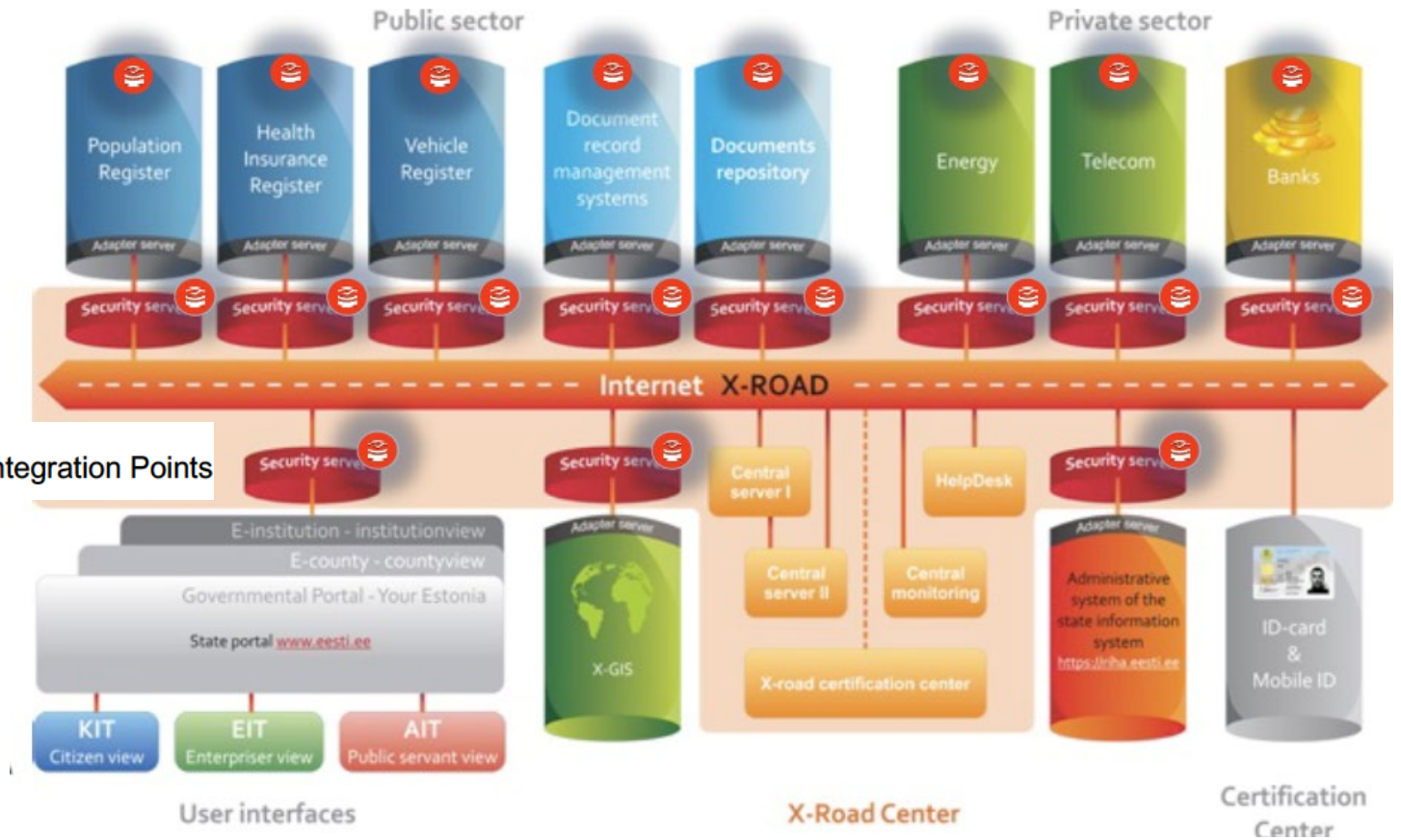
Figure 2: Blockchain-Based Decentralized Control of Critical Weapons System

Source: ConsenSys

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

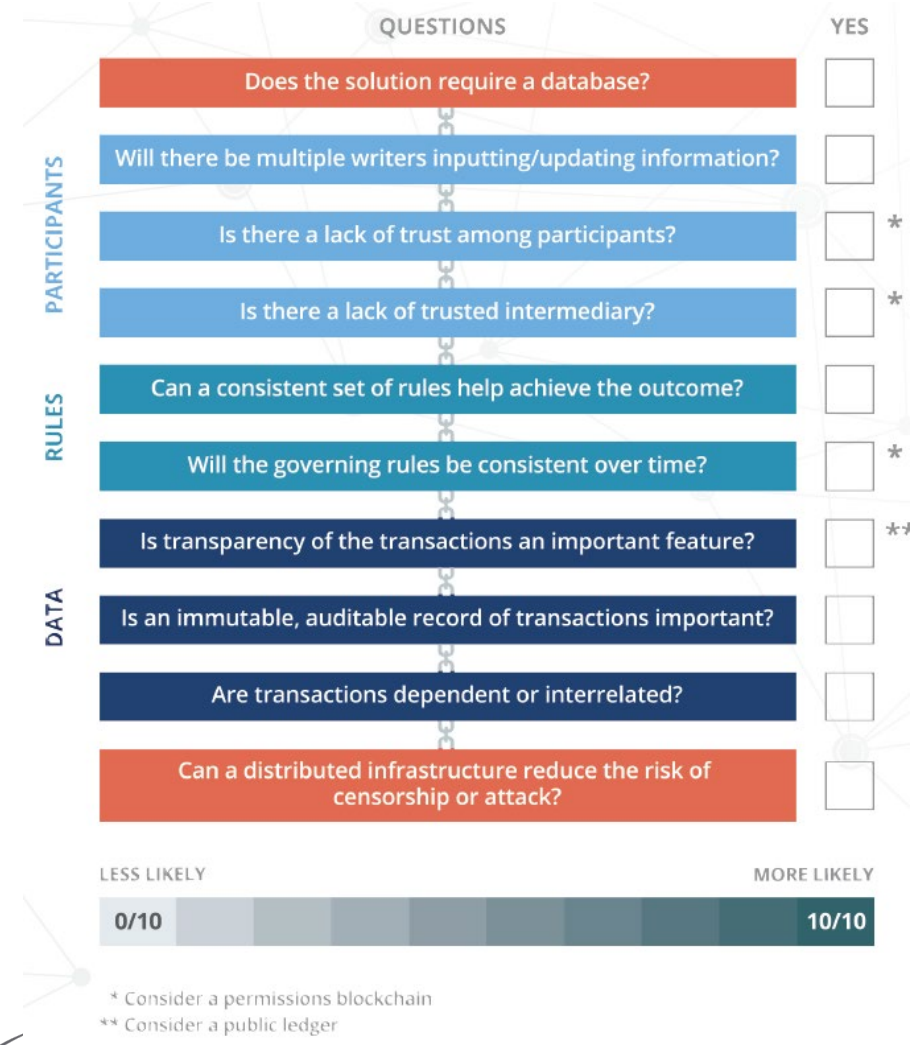
guardtime

RSAConference2019

Technical Specification Requirements to Use Blockchain

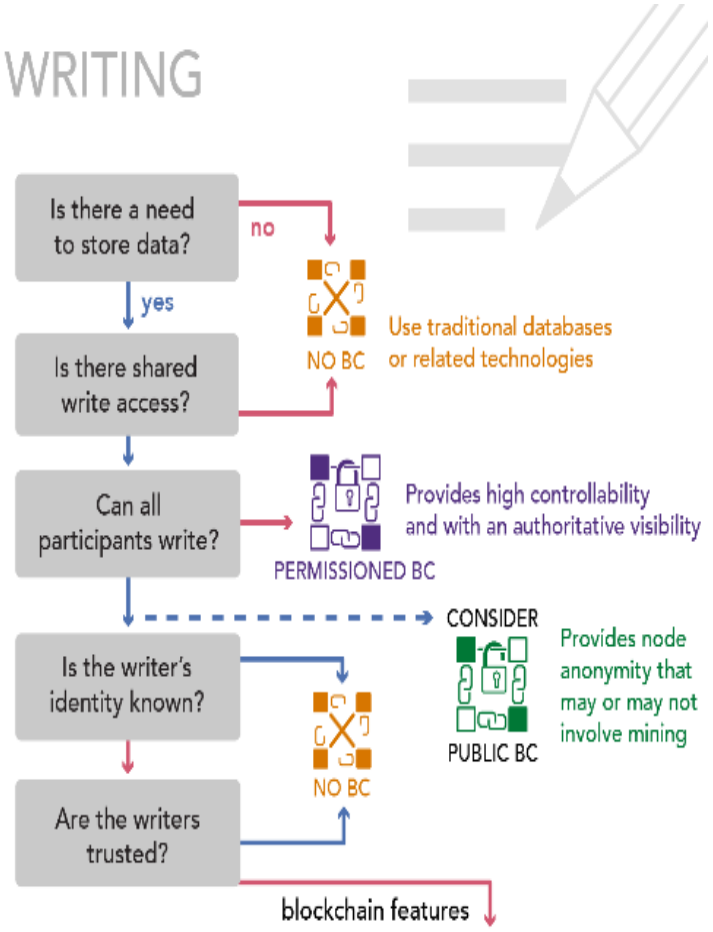
Lessons Learned

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



Source: CARA LAPOINTE AND LARA FISHBANE 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.



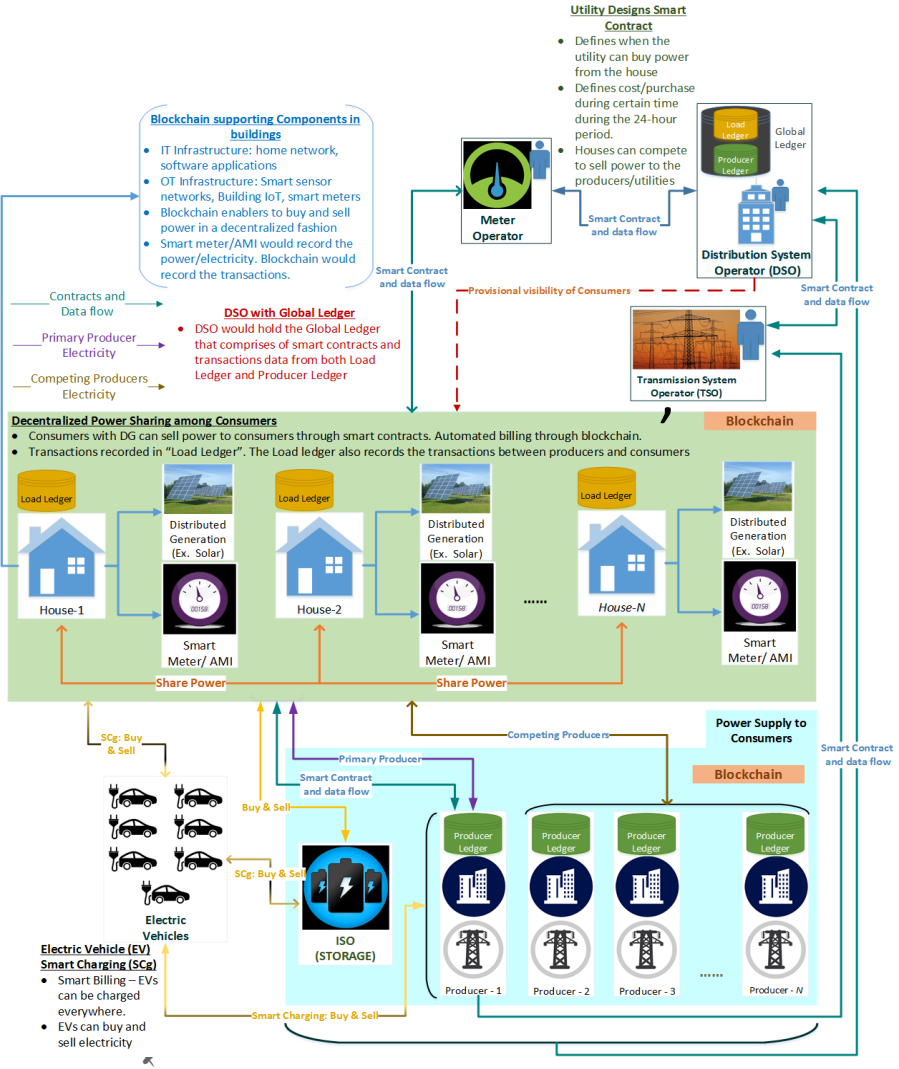
Source: Mylrea & Gourisetti, 2019

RSAConference2019

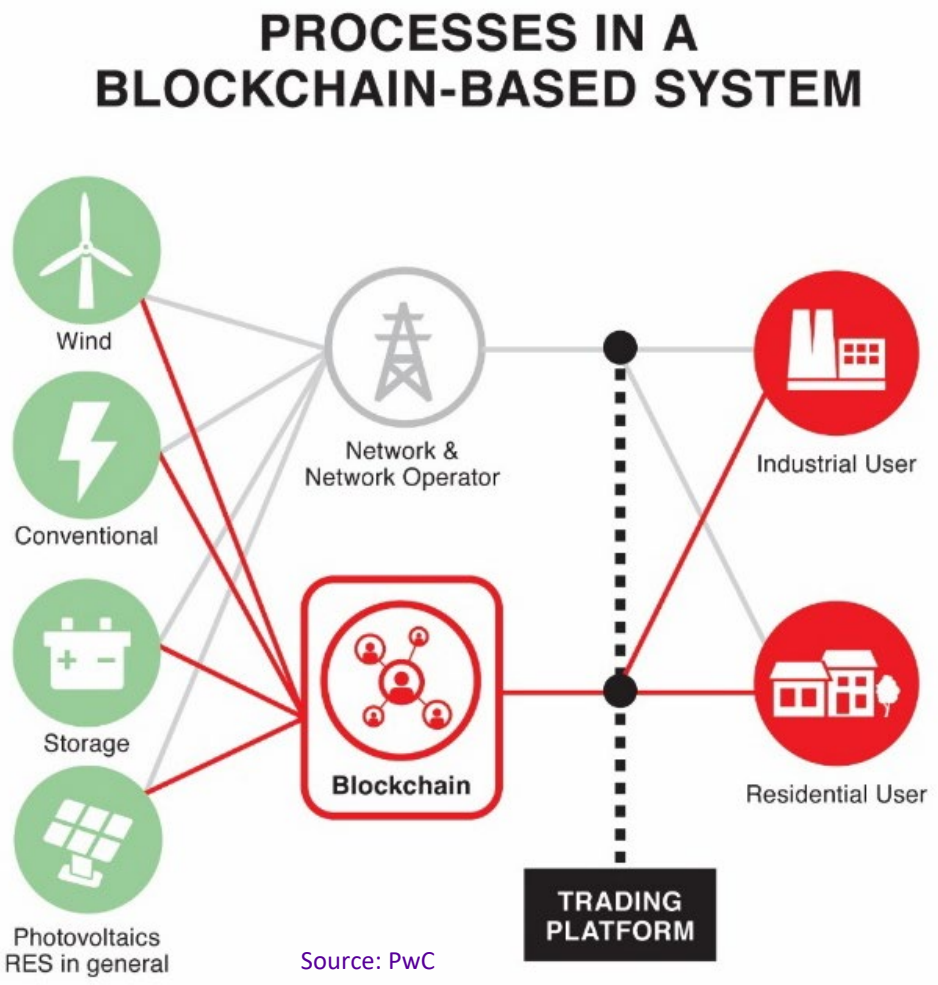
Real World Blockchain Use Cases

Lessons Learned

Secure Ledger of Things for Internet of Things: blockchain peer-to-peer (P2P) distributed ledger for secure energy exchange



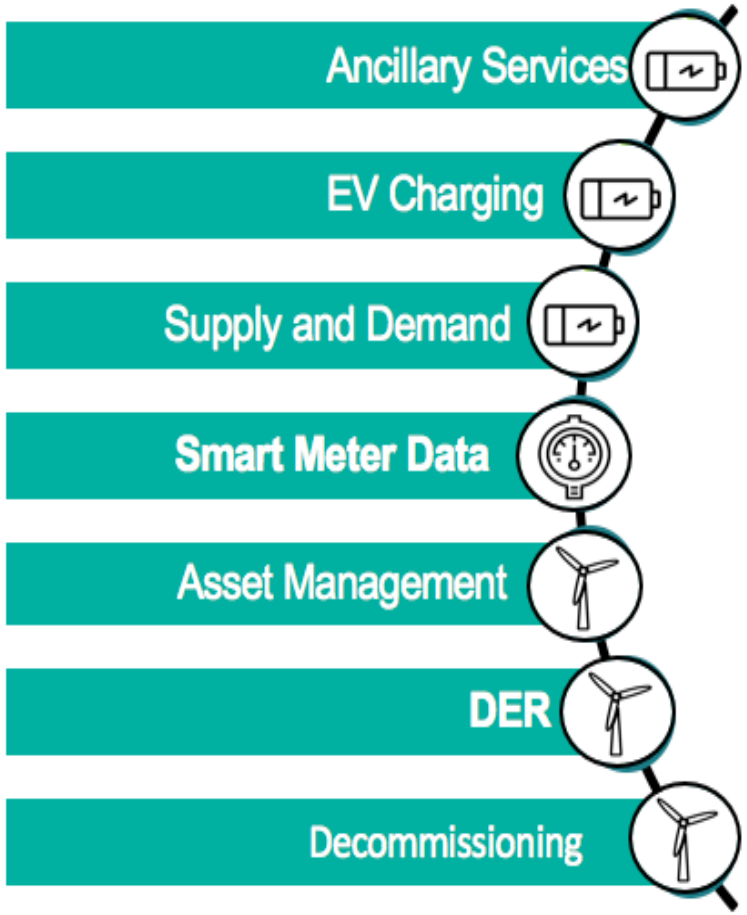
Increase trustworthiness and integrity of data, while accelerating grid modernization and energy decarbonization, decentralization and digitization



Source: PwC

Source: Mylrea & Gourisetti, 2019

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

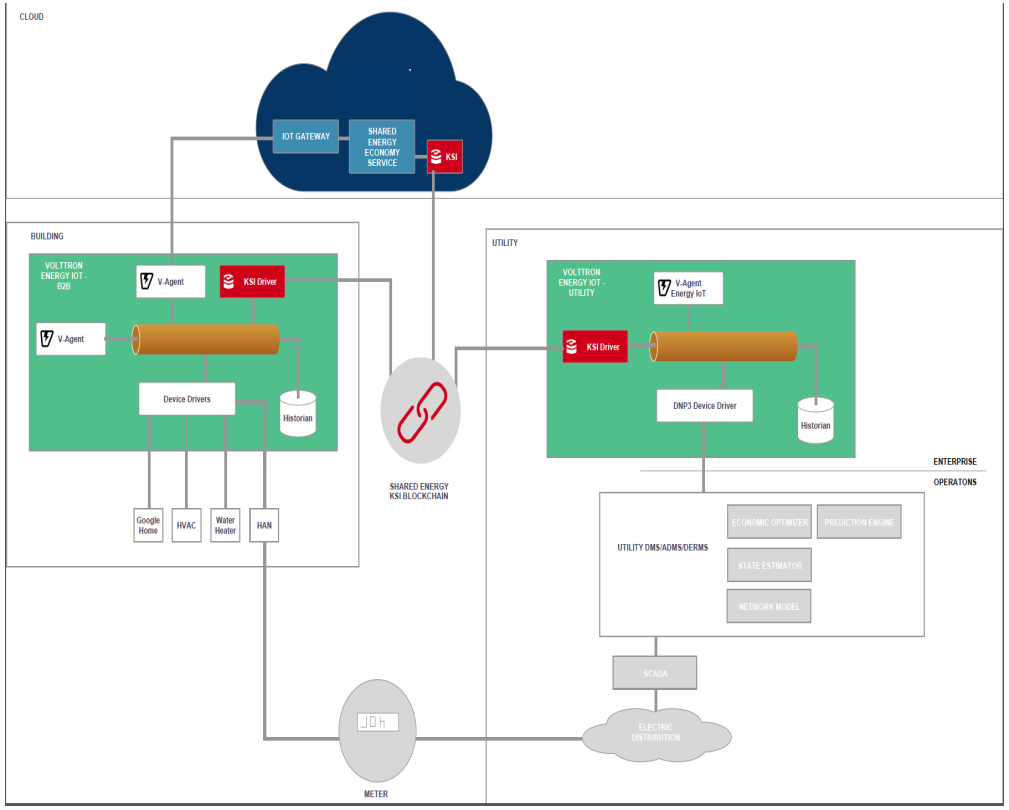


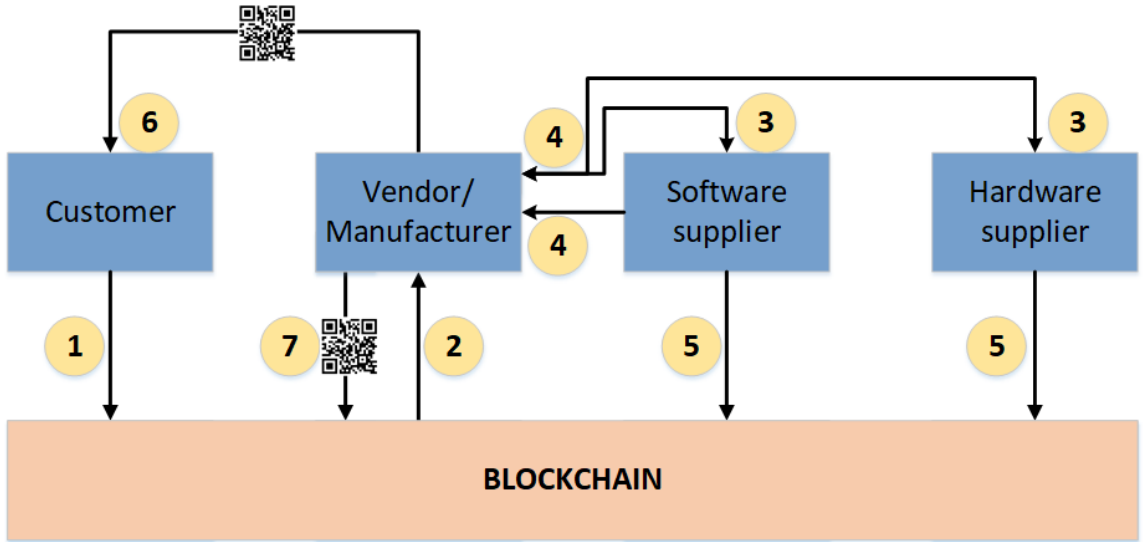
Source: Neil Gerber, IBM Hyperledger

Blockchain 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 Guardtime	• 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

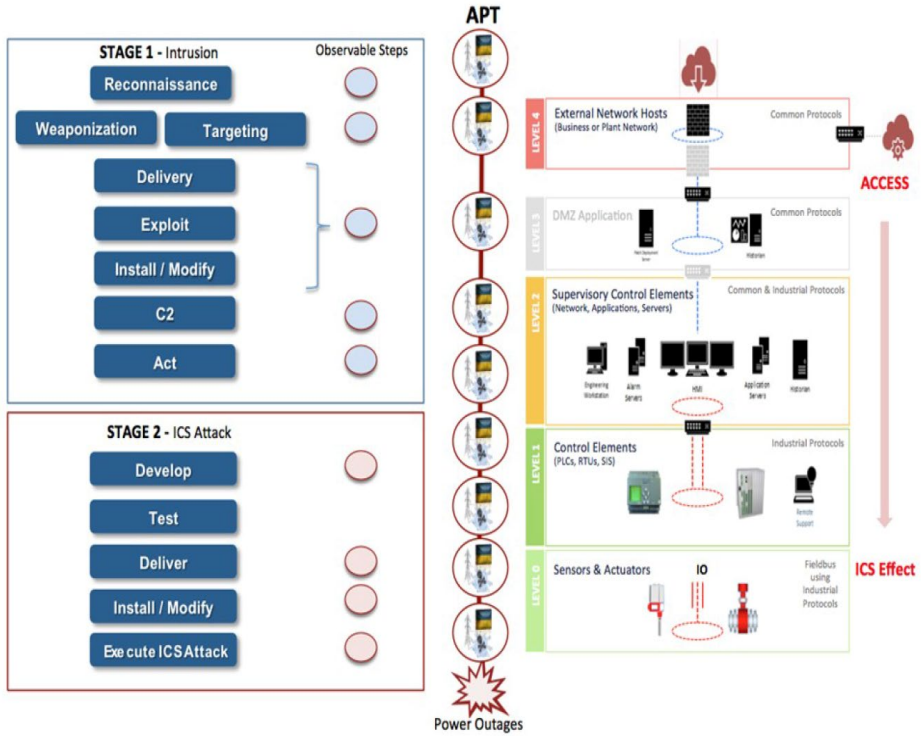
Use Case 1: Supply Chain Security





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

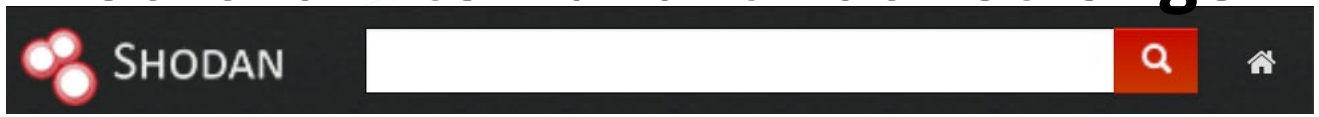
How Hacked Water Heaters Could Trigger Mass Blackouts

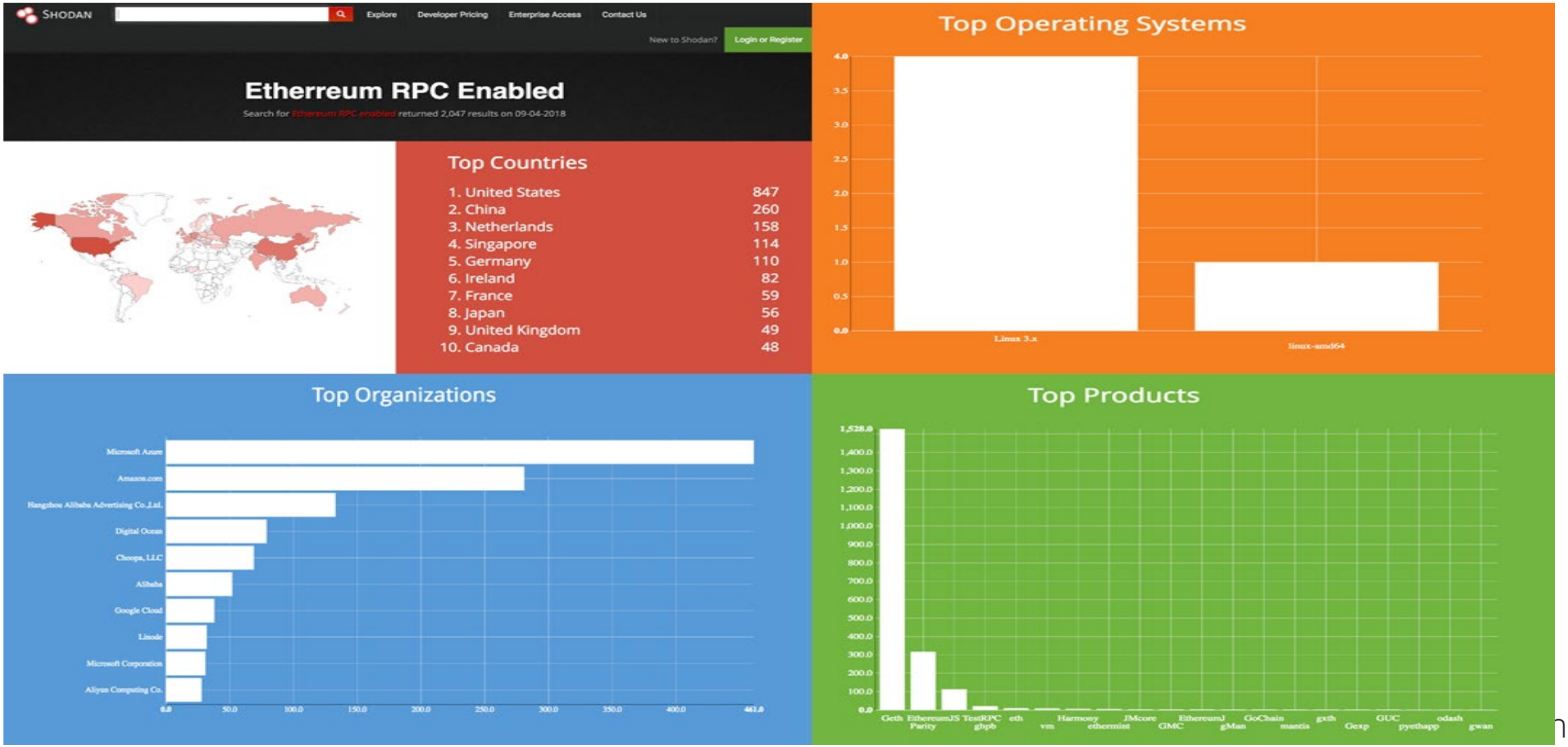
RSAConference2019

Blockchain Challenges

Lessons Learned

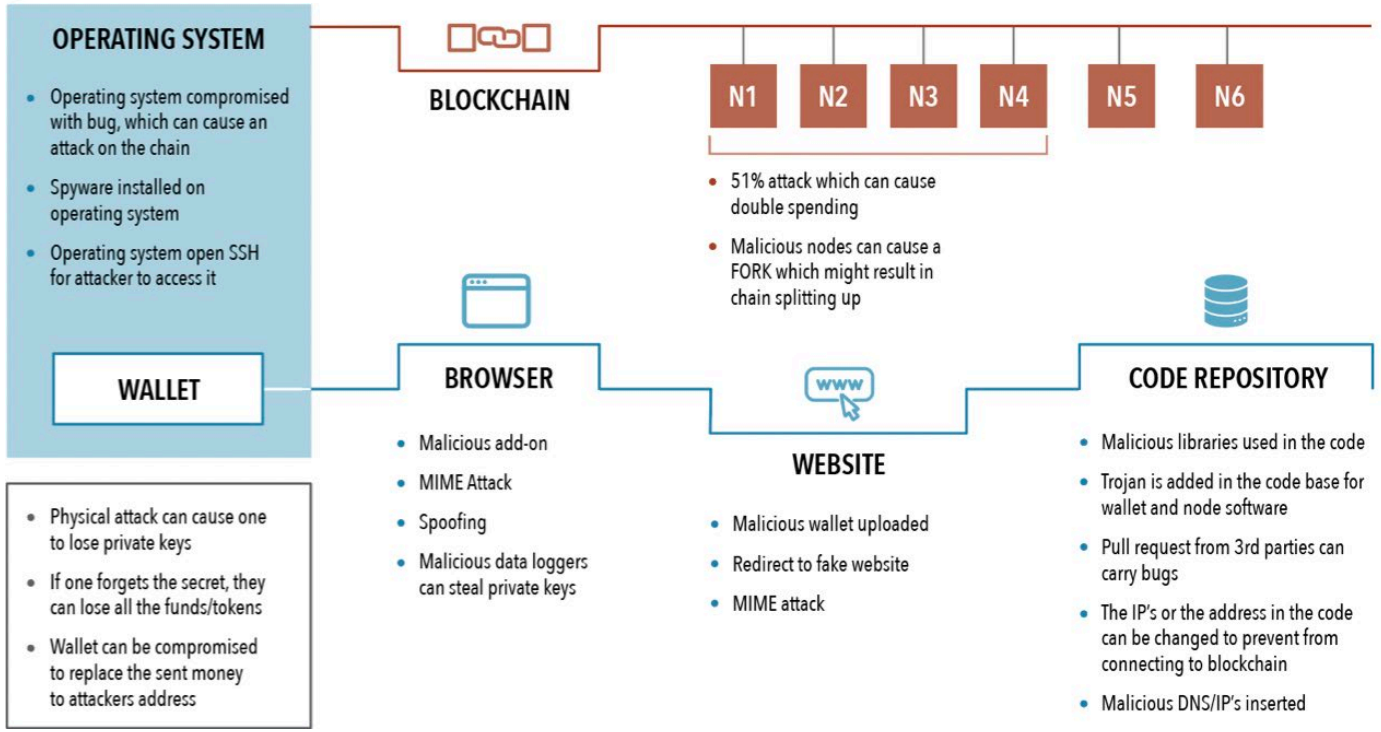
Breaking the Blockchain to Build it Back Stronger





Blockchain Challenges

- 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



Dr. Michael Mylrea

Senior Advisor, Cybersecurity & Energy Technology | Blockchain Lead

Pacific Northwest National Lab

michael.mylrea@pnnl.gov