Blockchain-based Cybersecurity Information Sharing for Improved Resiliency

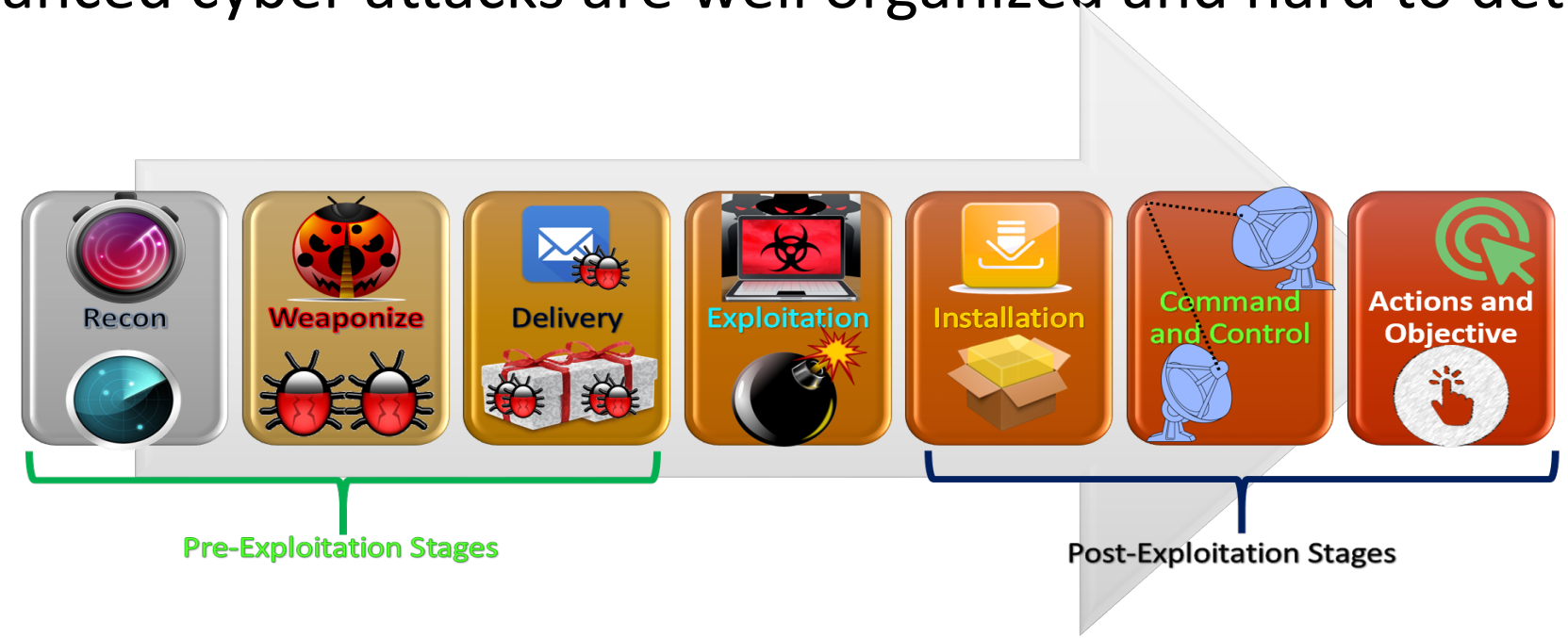
Dr. Deepak K. Tosh
Assistant Professor
Department of Computer Science
University of Texas at El Paso
Email: dktosh@utep.edu

Outline

- Motivation
- Cyber-Threat Information (CTI) sharing
- Current Efforts
- Modeling a “Specific” Problem: Sharing Participation
- Blockchain for Information Sharing
- Research Challenges
- Concluding Remarks

Growth of Cyber Threats

- Advanced cyber attacks are well organized and hard to detect



- Exploits are easily acquired and can be reused on multiple targets
- Reactive strategies are insufficient to deal with the threats

Need of Threat Intelligence

- Cyberattacks may not be prevented but their impacts can be reduced by
  - Improving cyber-awareness and understanding threat landscape
  - Collaborative effort from enterprises as well as government
  - Imposing security policies/laws (e.g. GDPR)
- Cyber-Threat Intelligence (CTI) can derive
  - Actionable information from various low level threat indicators (like IP, email, malicious URLs, domain names, attack pattern, geo-location info, malware hash)
  - Finding targeted resources, threat actors, methods/tools used, attack characteristics, IoC, etc.

Handling Cybersecurity Threats

- Security investment helps in
  - Discovering system loopholes, bugs, vulnerabilities
  - Identify malicious activities
  - Developing anti-threat strategies

Improves defenders' ability to **predict attacker behavior and create more dynamic defenses**

- Demerits:
  - Costly
  - Time consuming

Cybersecurity Information Sharing

- An ecosystem where actionable cyber-threat intelligence is shared automatically across verticals and public / private sectors in near real-time to combat cyber threat landscape
- Benefits
  - Access to Indicators, Tactics, techniques, and procedures (TTPs), Security alerts, Threat intelligence reports, Tool configurations
  - Enhance operational understanding of cyber threats
  - Proactive Defense
  - Reduce Cyber Risk
  - Prioritized Mitigation Plan
  - Cost effective defense strategy

Limitations of Information Sharing

- Something stops organizations from sharing!!!
  - Jeopardize the security posture of the sharing organization
  - External impacts such as market value, reputation, etc.
  - Information free-riding
  - Spurious information and processing overheads

How did we get here?

Following 9-11 Federal Information Sharing grows- failure to connect the dots

In **2007**, President Bush creates **Comprehensive National Cyber Initiative (CNCI)**- Connect the Fed Cyber Centers in order to address cyber threat landscape

In **2013**, **Enhance Shared Situation Awareness Project (ESSA)** created to automate cyber threat information sharing between Fed Cyber Centers.

-Standard sharing languages STIX/TAXII, shared capability providers, and common sharing agreement (MISA).

In **2015**, **Cybersecurity Information Sharing Act (CISA)** passed.

-Establishes the **DHS Automated Indicator Sharing (AIS)** Program for sharing cyber threat indicators and defensive measures between the Federal Government and Non-Federal Entities.

In **2016** the **legacy of ESSA is leveraged by DHS** for continuation of Federal Cyber Threat Information Sharing and coordination through the Federal Cybersecurity Interagency Group (FCIG).

Cybersecurity Information Sharing Today

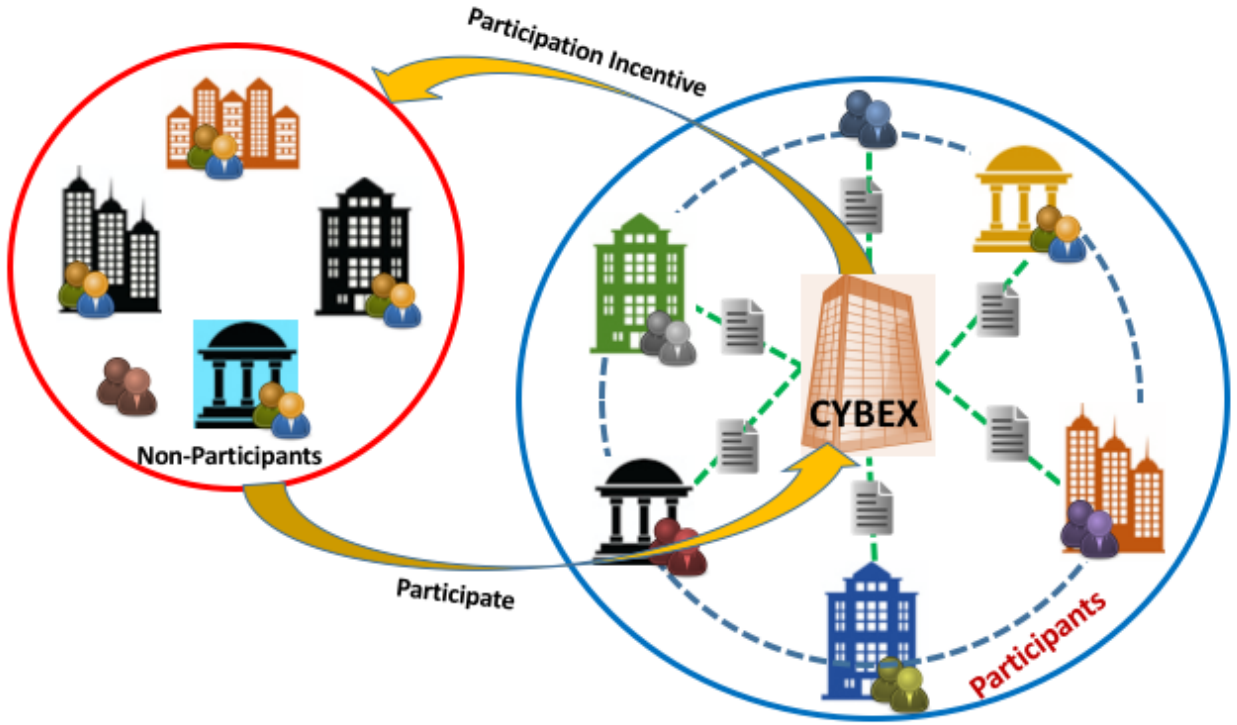
- Cybersecurity Information sharing has been going on through ISACs, ISAOs, eco-systems, open source, and commercial offerings
- Limitations
  - Generally unstructured data
  - Ad-hoc manual communications such as email / IM / IRC / paper
  - Few automated tools
  - Lack of incentive model for voluntary participation

Outline

- ✓Motivation
- ✓Cyber-Threat Information (CTI) sharing
- ✓Current Efforts
- **Modeling a "Specific" Problem: Sharing Participation**
- Blockchain for Information Sharing
- Research Challenges
- Concluding Remarks

CYBEX Self-Coexistence Game

- *N*-firms play independently to figure out whether to participate in the CTI sharing or not



CYBEX Self-Coexistence Game

Conflict:

- Firms' participation depend on participation cost charged by CYBEX
  - If CYBEX charges too high, low participation might be resulted
  - If CYBEX charges too low, CYBEX might not be profitable

- Firm's net payoff depends two major factors:
  - Sharing and Investment Gain
  - Participation cost and cost of information shared

CYBEX Self-Coexistence Game

- The strategic form can be

	Participate & Share	Not Participate
Participate & Share	$Sa\log(1+I)-x-c$, $Sa\log(1+I)-x-c$	$a\log(1+I)-x-c$, $a\log(1+I)$
Not Participate	$a\log(1+I)$, $a\log(1+I)-x-c$	$a\log(1+I)$, $a\log(1+I)$

- If *S* is low, then pure strategy Nash equilibrium for the single stage game is: (*Not Participate, Not Participate*)
  - CYBEX cannot survive in this case
- **Multi-stage evolutionary analysis** is important

Evolutionary Game Analysis

Goal: Find evolutionary stable strategy (ESS) that cannot be invaded by any other strategy

Replicator Dynamics:

Assume, $\alpha =$ Proportion of population who participate and share in CYBEX, the transformation rate ($g(\alpha)$) is

- Proportional to difference of expected individual utility for that strategy ($E{\downarrow}sh\ (u)$) and expected utility of the population
  - $g(\alpha)=\alpha[E{\downarrow}sh\ (u)-E(u)]$

Where, $E(u)$ is average utility of the whole population

Solving the Game

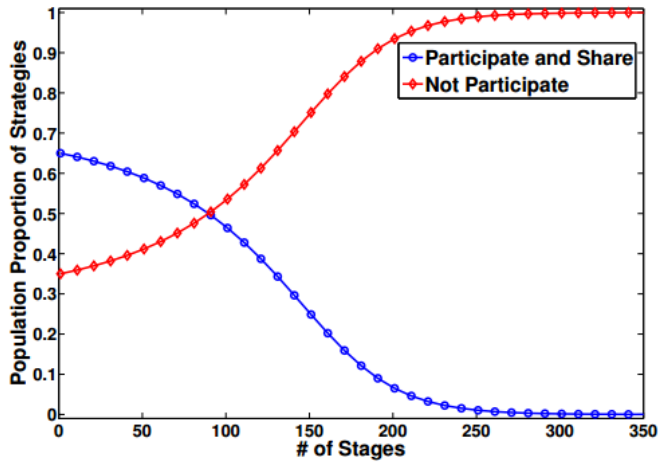
- Solving for $g(\alpha)=0$, we find

$$\alpha_{sol_1} = 0$$
$$\alpha_{sol_2} = 1$$
$$\alpha_{sol_3} = \frac{x+c}{(S-1)a\log(1+I)}$$

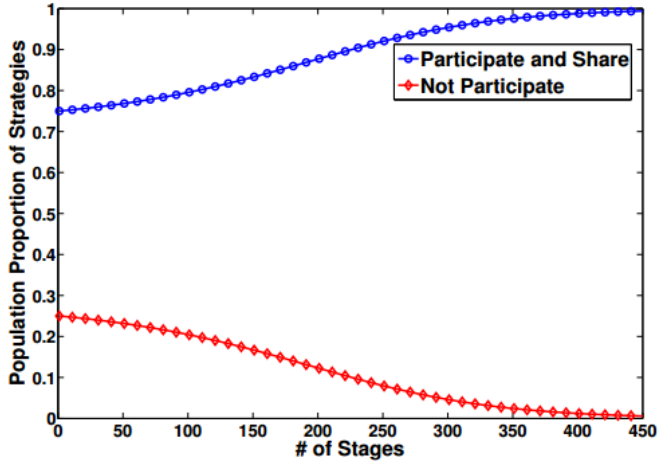
- To have stable neighborhood, $g'(\alpha)<0$
- Wise choice of incentive or participation cost (c) is needed to motivate the socially optimal behavior

Interesting Evolutionary Strategy

- Exact ESS is decided depending on initial sharing strategy population (α)
  - $\alpha \downarrow sol \downarrow 1$ (No Sharing) is ESS, if $0 < \alpha < c + x/(S-1)a\log(1+I)$
  - $\alpha \downarrow sol \downarrow 2$ (Share & Participate) is ESS, if $c + x/(S-1)a\log(1+I) < \alpha < 1$



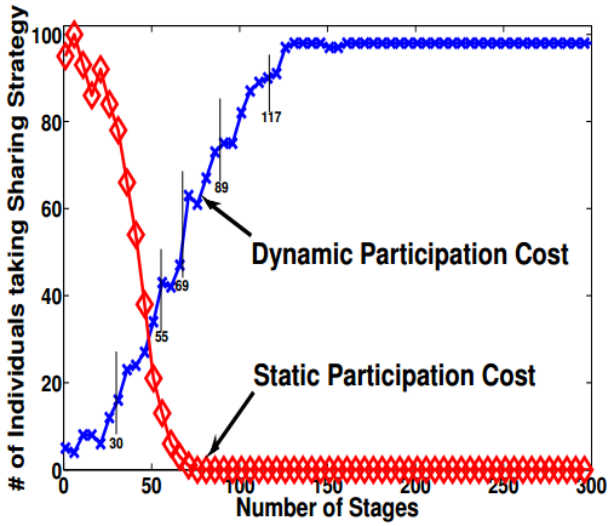
(a) $\alpha^*_{sol_3} < \alpha_{thres}$



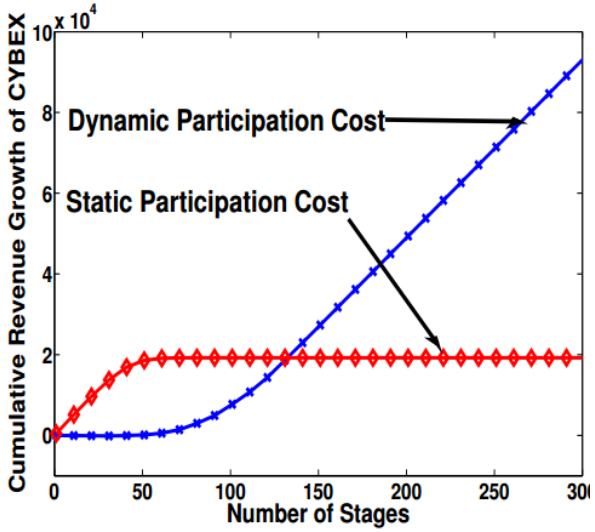
(b) $\alpha^*_{sol_3} > \alpha_{thres}$

Incentivization through Participation Cost

- Dynamic incentive/participation cost exploits the ESS conditions
  - Revenue of CYBEX grows periodically
- Static cost demotivates firms from participation



(a)



(b)

Other Challenges

- Cyber-investment
  - Optimal security investment while sharing is considered
- Information Ownership
- Integrity and Auditability of shared information

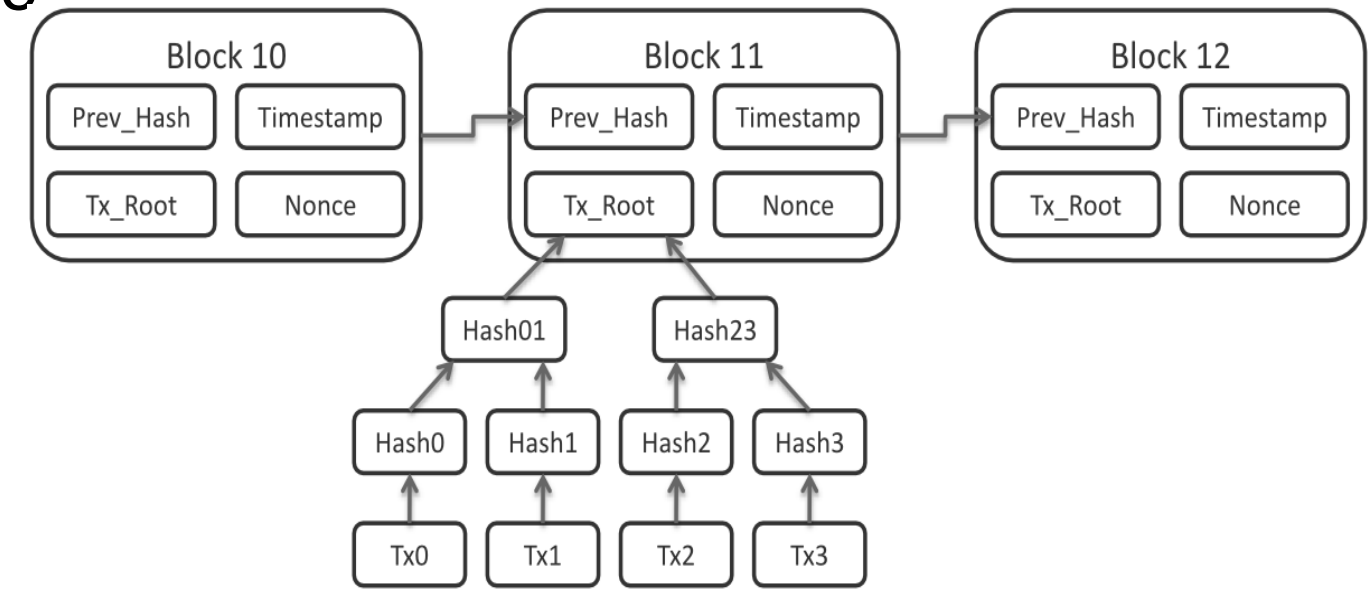
Outline

- ✓Motivation
- ✓Cyber-Threat Information (CTI) sharing
- ✓Current Efforts
- ✓ Modeling a “Specific” Problem: Sharing Participation
- **Blockchain for Information Sharing**
- Research Challenges
- Concluding Remarks

Blockchain for Information Sharing

Blockchain (Integral part of Bitcoin):

- An open distributed ledger to record transactions **immutably**
- **Cost-less verification** of transactions
- Fault-tolerant



Source: https://en.wikipedia.org/wiki/Blockchain

Blockchain-empowered Cybersecurity Information Sharing Goals

What?
Real-time dissemination of relevant and actionable cyber threat indicators and defensive measures

Who?
Government, military and commercial sectors

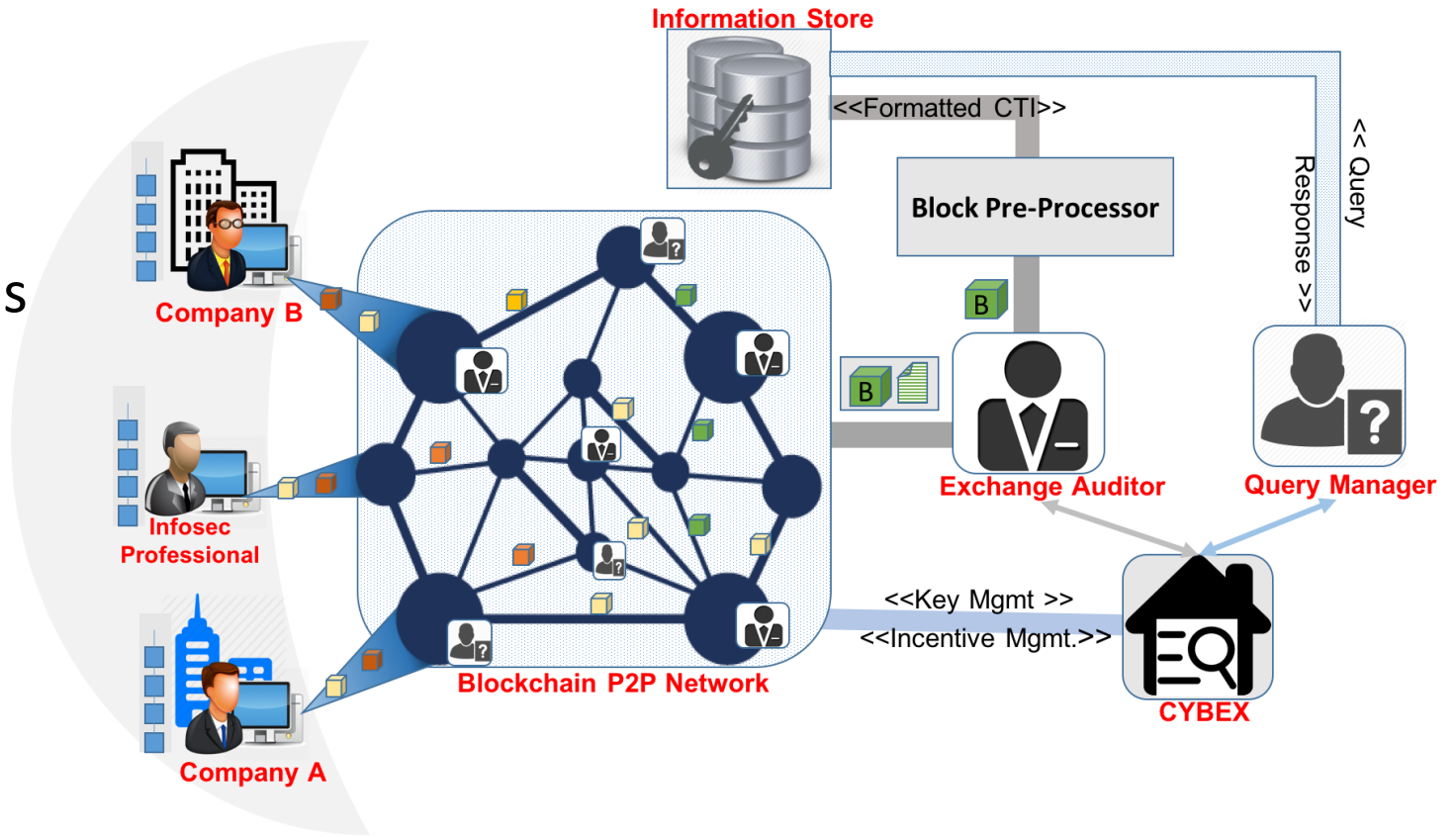
Why?
Proactive defense and reduce cyber risk

While?
Ensuring integrity, trust, and privacy

Blockchain-integrated Information Sharing

Provenance:

- Auditing process which maintains a record of all operations conducted on shared threat information
- Maintain Information Integrity



Research Challenges

- Ensuring information privacy
- Pruning redundant information
- Deriving actionable threat intelligence
- Quality vs. quantity
- Enabling sector-wise information sharing

Concluding Remarks

- Cybersecurity landscape is huge and there are a lot to explore
- Cyber-threat information sharing is one important initiative toward proactive defense
- Blockchain technology is a new frontier to design tamper-resistant systems
- A working platform that integrates both is yet to come

Thank You

Questions??