RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: PDAC-F02

Blockchain Augmentation of the Trusted Supply Chain

Tom Dodson
Supply Chain Security Architect
Intel Corporation
@totommyd

Eduardo Cabre
Product Development Engineering Manager
Intel Corporation
@edcabre

Agenda

- Introduction
- Trusted Supply Chain on Blockchain
- Proof of Concept
- DEMO
- Conclusions and Summary
- Apply What You Learned

RSAConference2019

Trusted Supply Chain

An Introduction

Trusted Supply Chain - Introduction

- Problem
  - Assurance of a device's origin in today's diverse manufacturing, logistics, and just in time inventory.
  - Remote deployment and provisioning requires assurance in the Supply Chain.
- Solution
  - Use a Root of Trust to provide assurance of a device's origin
  - This Root of Trust establishes the foundation for a Trusted Supply Chain (TSC)
  - Blockchain adds an additional layer of trust in the overall system supply chain
- We will show how we augmented the existing hardware root of trust with the implementation of a blockchain to establish a TSC.

Trusting the Supply Chain – Problem

Military Warns Chinese Computer Gear Poses Cyber Spy Threat

Lenovo seeking access to classified Pentagon networks, J-2 report says

SHARE TWEET EMAIL

BY: Bill Gertz Follow @BillGertz

October 24, 2016 5:00 am

The Pentagon's Joint Staff recently warned against using equipment made by China's Lenovo computer manufacturer amid concerns about cyber spying against Pentagon networks, according to defense officials.

A recent internal report produced by the J-2 intelligence directorate stated that cyber security officials are concerned that Lenovo computers and handheld devices could introduce compromised hardware into the Defense Department supply chain, posing cyber espionage risks, said officials familiar with the report. The "supply chain" is how the Pentagon refers to its global network of suppliers that provide key components for weapons and other military systems.

The J-2 report was sent Sept. 28, and also contained a warning that Lenovo was seeking to purchase American information technology companies in a bid to gain access to classified Pentagon and military information networks.

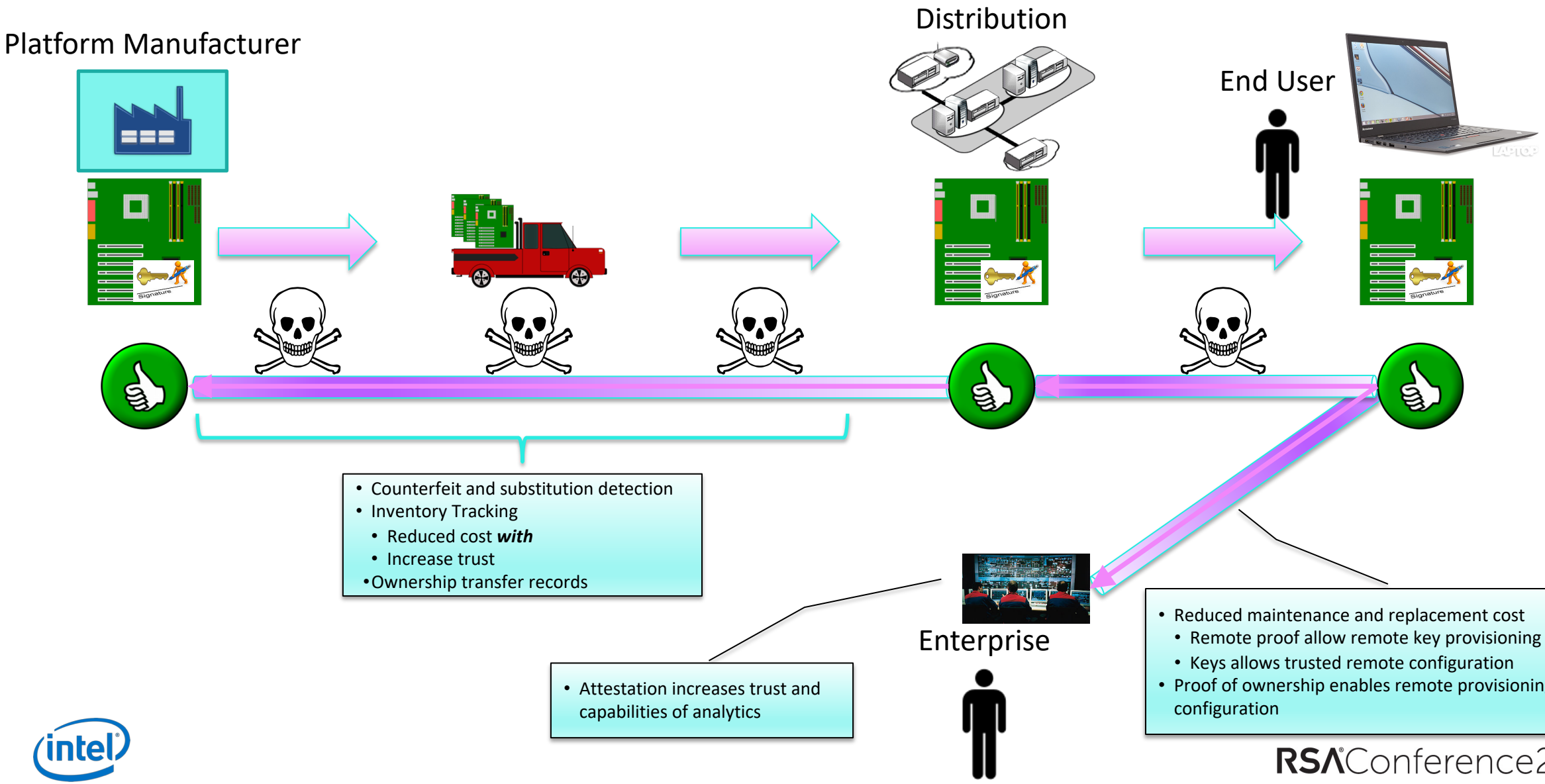
"cyber security officials are concerned that computers and handheld devices could introduce compromised hardware into the Defense Department **supply chain**, posing cyber espionage risks, said officials familiar with the report."

500 Re-marked Engineering Samples crash Dublin, California school district network

Defense Federal Acquisition Regulation Supplement (DFARS) 252.246 - Contractor Counterfeit Electronic Part Detection and Avoidance System:

Design, operation, and maintenance of systems to detect and avoid *counterfeit* electronic parts and *suspect counterfeit* electronic parts.

Trusted Supply Chain – Value Proposition



Trusted Supply Chain Components

- Trusted Supply Chain (TSC) provides traceability for customer platforms
- The following are the traceability components

TSC COMPONENT	DETAILS
System-Level Traceability	• Supported by ***signed platform certificates*** • Linked to discrete ***Trusted Platform Module (TPM)*** on motherboard
Component-Level Traceability	• Supported by ***"as-built" report*** from Original Design Manufacturer (ODM) • ***ODM partnerships*** are vital to two-level traceability • ***Blockchain*** provides ***component supplier*** level traceability
Statement of Conformance	• Attests to ***authenticity of system*** • ***Signed by Platform Manufacturer*** • ***Blockchain*** provided ***statement of conformance***
Customer Web Portal	• Provides ***customer access*** to signed files • Files available for ***download***

Trusted Supply Chain Process – In Production

1 Component and Platform Data Captured at ODM

"As-Built" Data File

Component Data
(vendor, part #, serial #, validation history, ...)

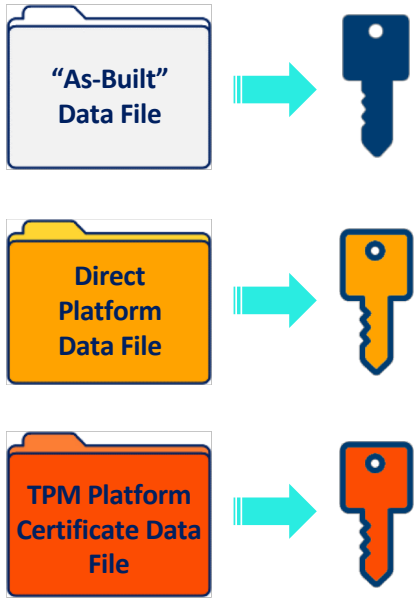
Direct Platform Data File

Platform Snapshot Data
(e.g., model #, PCR data, processor, memory, disk, …)

TPM Platform Certificate Data File

Certificate Data
(Endorsement Key, Endorsement Key serial #, ...)

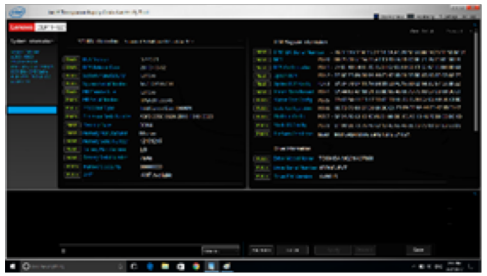
2 Data Transmitted to Intel Key Generation Services



3 Signed Certificates Created & Stored on Intel Database

4 Signed Certificates Available for Download, View, and Data Analytics

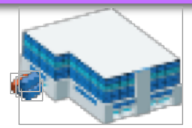
5 Auto Verify Tool (Web Download)



The TSC Supply Chain – Problem Statement

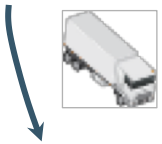
- The component information (e.g., manufacturer, part number, batch number, distributor) is provided by the ODM through the "Honor System"
- Moving the Trusted Supply Chain to a Blockchain will allow component suppliers to also participate in the supply chain at the component level.
- Component Supplier participation will allow for the verification of the components used by the ODM factory to manufacture the system.
- VARs, Distributors, Resellers can now use the Distributed Application (DAPP) on the blockchain to establish the root of trust for each system.

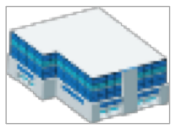
Suppliers



Suppliers

- Component Inventory
- Ship components

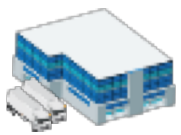




Manufacturing

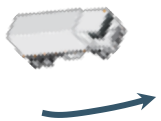
- Builds Base Assemblies
- Work In Process (WIP)
- Creates Shipment

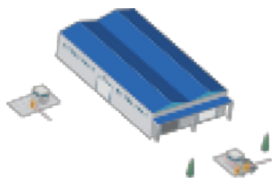
Manufacturer In or Out-Source

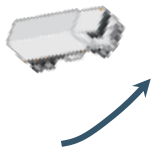


3rd Party Logistics

- Freight Forwarding
- Customs Clearance
- Consolidation
- FG Inventory







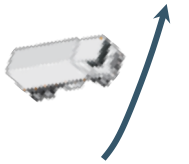
Distributors

- Break Bulk
- Cross Dock
- FG Inventory
- Kit

Distributor

Customer/ Retailer

- Point of Sale, Sell-thru
- Inventory
- Returns, Post-Sales



Customer Data Centers

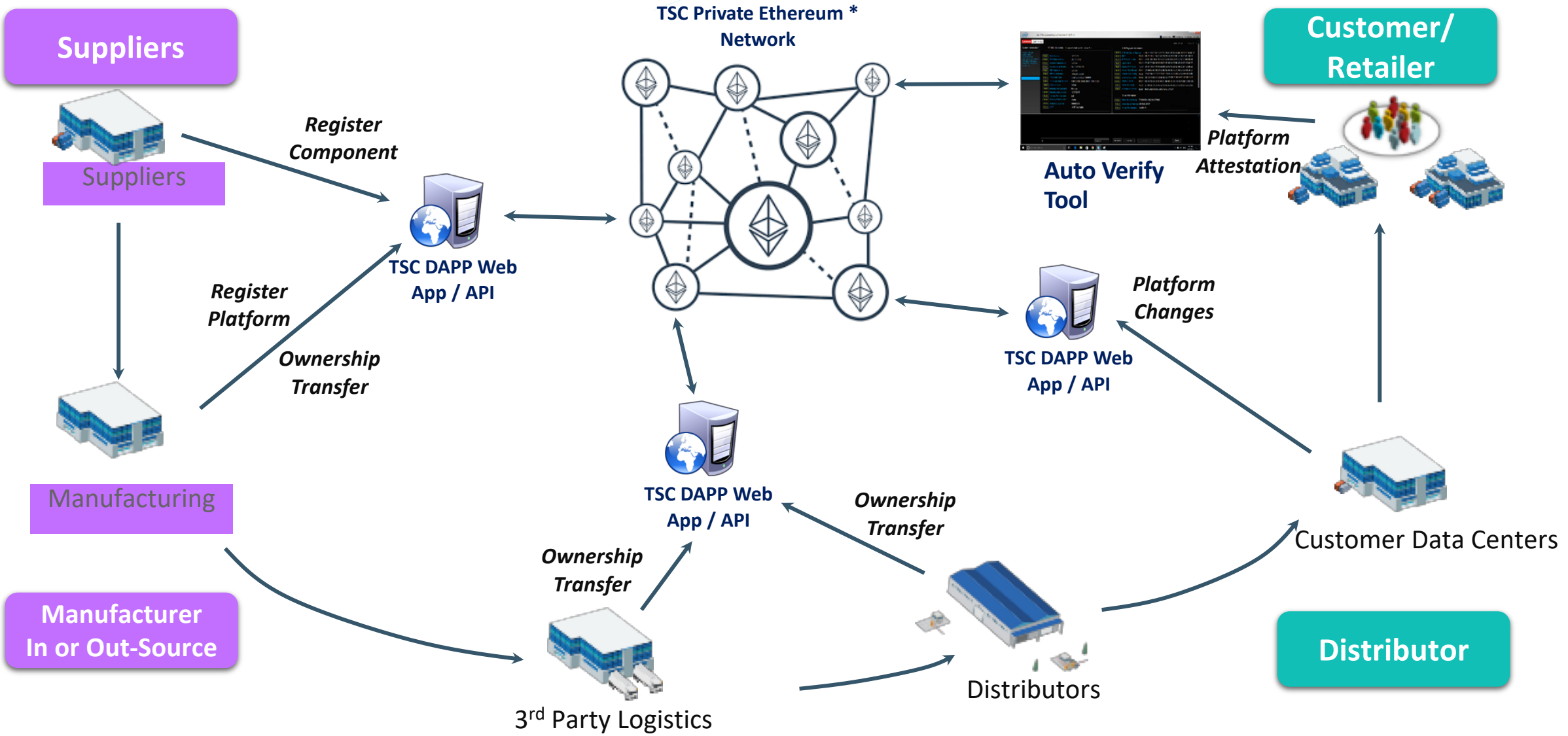
- Forecast, Sales Orders
- Goods Receipts
- Inventory of New & Returned Goods

RSAConference2019

Trusted Supply Chain on the Blockchain

A decentralized model

TSC on Blockchain



* *"Ethereum is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract functionality."* – Ethereum Foundation

System-Level Traceability

- Supply chain level traceability based upon the Blockchain
  - Platform provenance starting at the component level
  - Extending into system level root of trust based upon Trusted Platform
- System level traceability based on a hardware root of trust:
  - For example Trusted Platform Module (TPM) 2.0 on motherboard, or silicon traceability using Physical unclonable function (PUF)
  - Associates platform serial number with TPM serial number and public Endorsement Key (EK)
- Software tools deployed during the manufacturing flow at the ODM:
  - Capture system information
  - Capture TPM Certificate (Including public EK)

RSAConference2019

TSC on Blockchain Proof of Concept

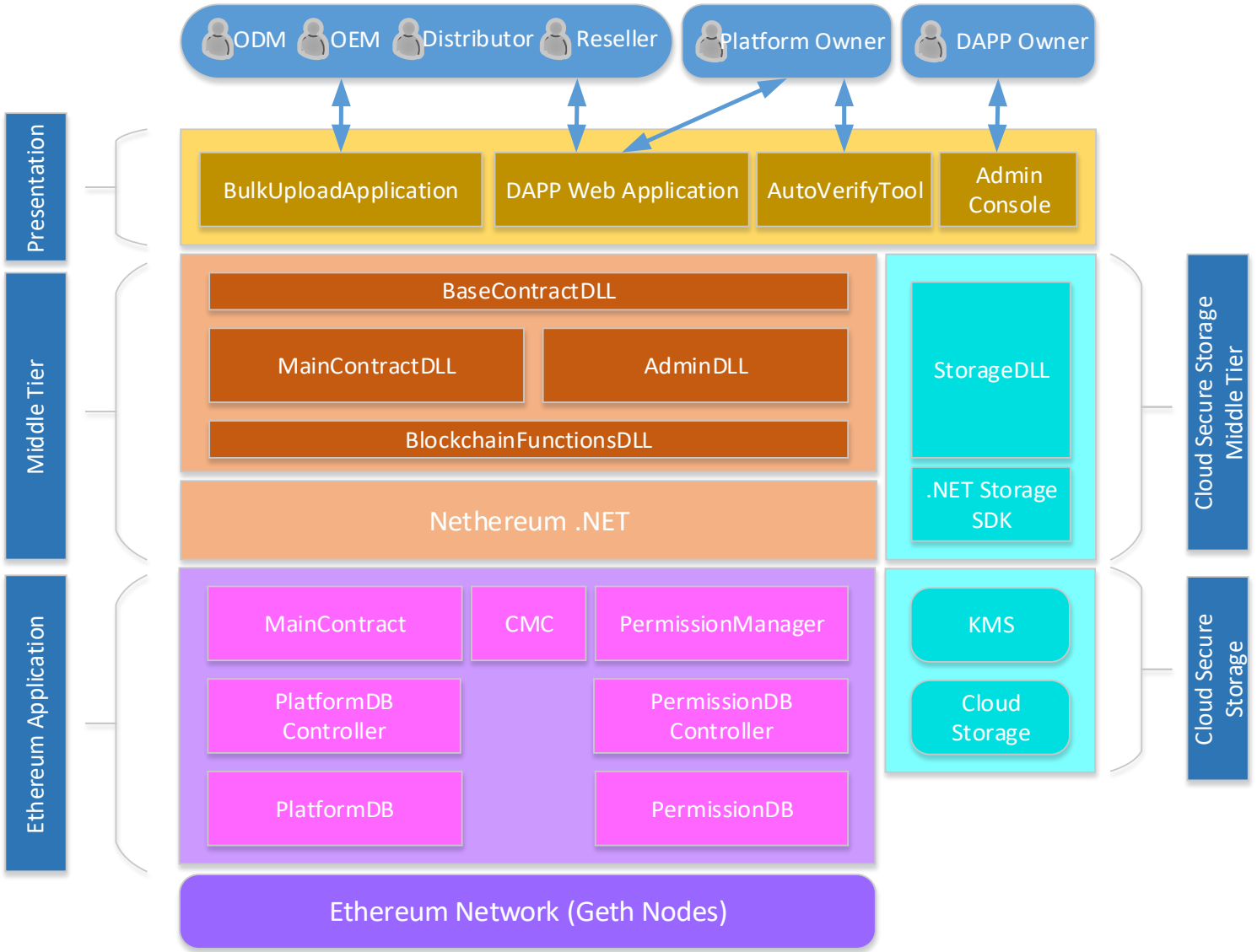
Architectural details

Proof of Concept (POC) Goals and Objectives

- Conducted a proof of concept to determine the feasibility of productizing TSC on Blockchain
- Objectives:
  - Evaluate cost, performance, and security tradeoffs
  - Compare public versus private blockchain options
  - Evaluate extending TSC to additional participants (component suppliers, distributors, resellers)
  - Gather expertise to develop Distributed Applications (DAPPs)
  - Develop designs for scalability and maintainability
  - Grow understanding of blockchain development ecosystem

TSC on Blockchain DAPP Architecture

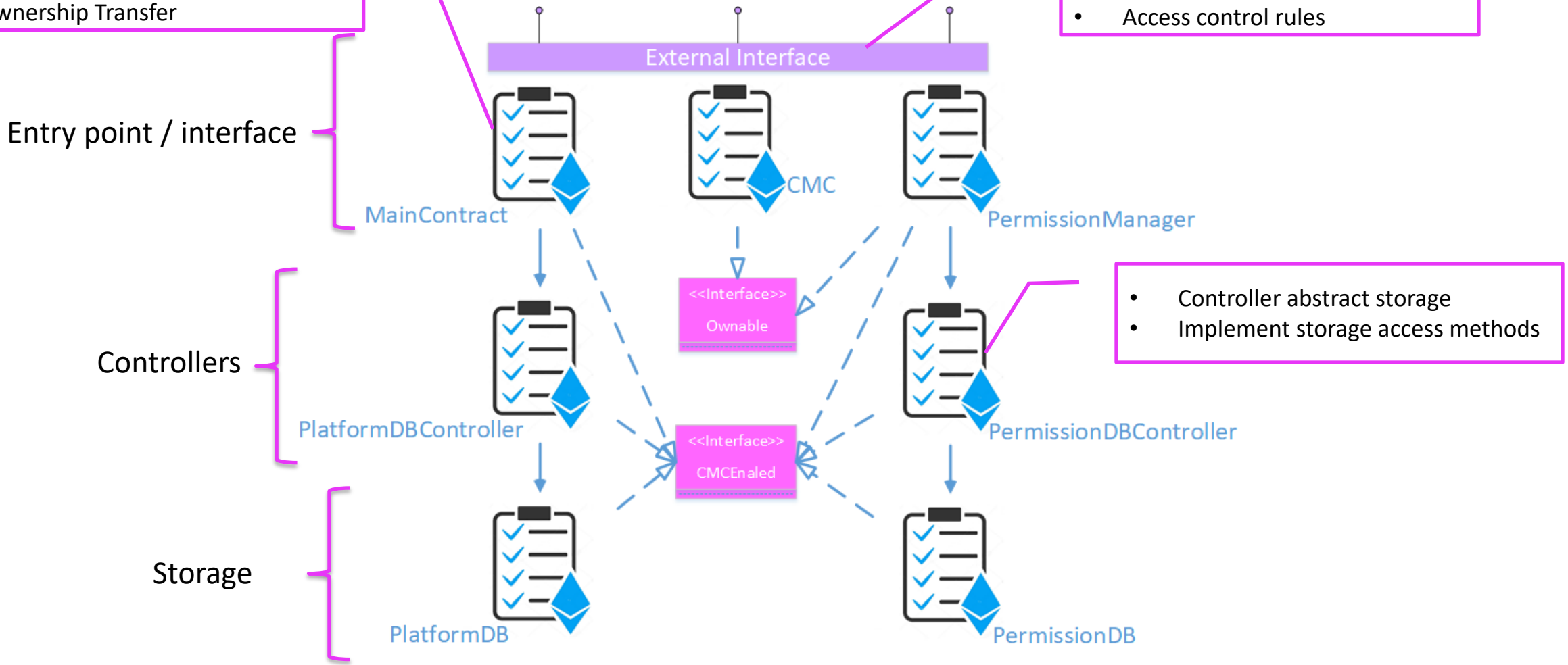
- Four tier architecture
  - Presentation: Web application, Bulk Upload Tool, AutoVerify Tool
  - Middle Tier: C#.NET libraries implement integration with Ethereum Application
  - Ethereum Application: Solidity Smart Contracts implement blockchain business logic
  - Ethereum Network: Set of nodes running private Ethereum blockchain.
- Cloud Secure Storage
  - Middle Tier: provide integration with cloud storage
  - Secure Storage: Key Management Service, cloud storage



TSC on Blockchain Architecture – Ethereum Application

- Method allows platform registration
- File upload
- Ownership Transfer

- Methods expose functionality
- Access to middle tier
- Access control rules

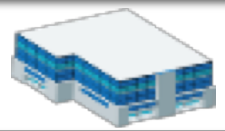
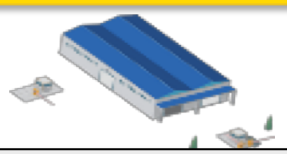


- Controller abstract storage
- Implement storage access methods

* Five Type Model developed by Monax [1]

TSC on Blockchain – Supply Chain Flows

Trusted Supply Chain Flow

ODM	OEM	Dist/Reseller	Platform Owner
			
• Platform Manufactured • Register Platform • Upload Platform Files • Transfers Ownership to OEM	• Retrieve platform data file • Verify Platforms • Transfer ownership to distributor	• Retrieve Platform Files • Modify platform • Generate platform files • Transfer ownership to end customer	• Retrieve platform data files • Platform attestation w/ AutoVerify Tool • Configure platform • Generate new platform Data Files w/ AutoVerify

DAPP Web Application

AutoVerify

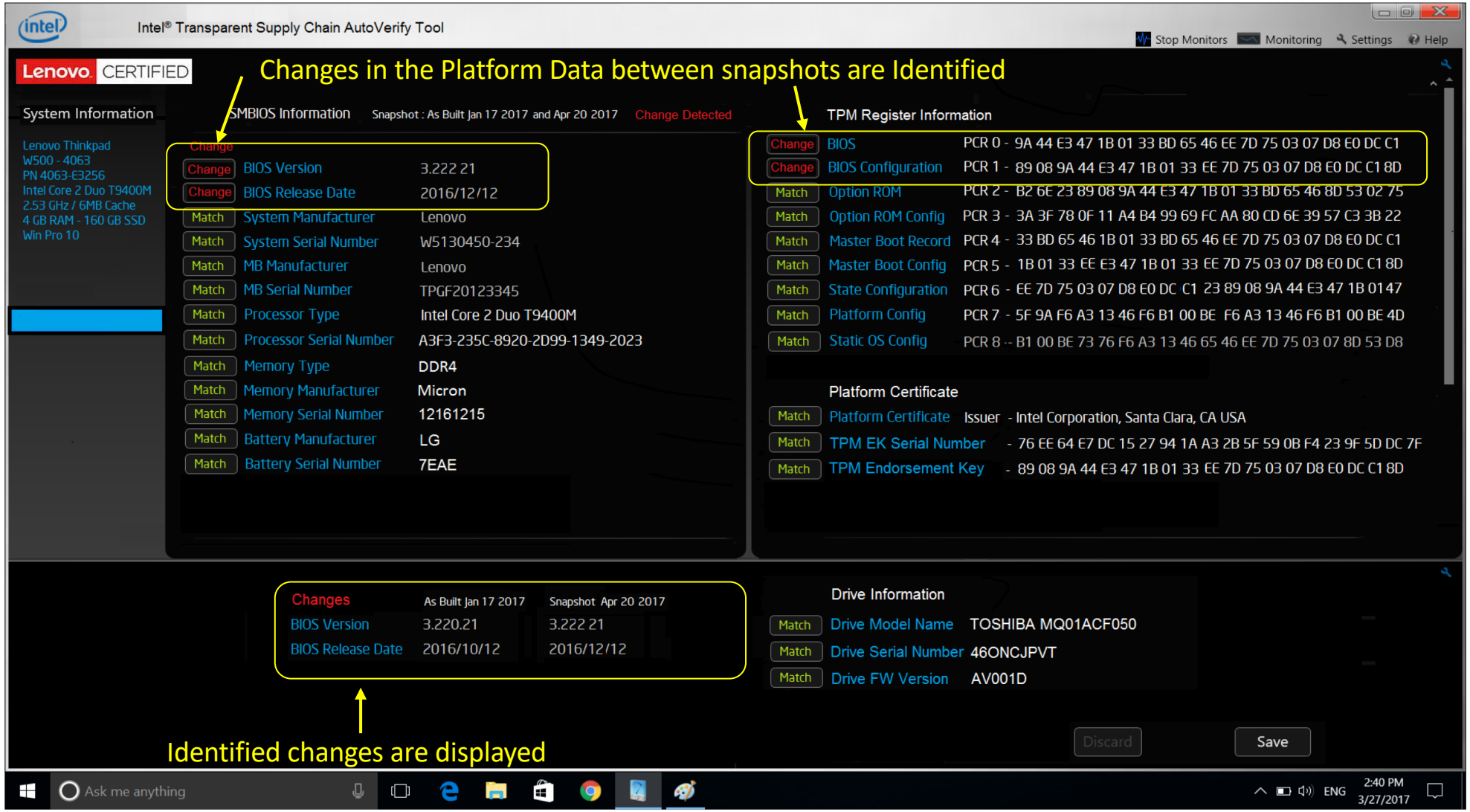
Ethereum Blockchain

Cloud Secure Storage

Auto Verify Tool

- Blockchain Platform Validation:
  - Verifies that the platform TPM matches the platform certificate data file from the DAPP
  - Platform Attestation is confirmed by comparing the TPM module's Endorsement Key against the Endorsement Key stored in the platform certificate data file
  - Platform data file integrity provided by the blockchain
- Direct Platform Components Validation:
  - The Auto Verify tool compares the "snapshot" of the platform component data taken during manufacturing and stored in the DAPP with a "snapshot" of the platform components taken at first boot
  - Any changes in system will be flagged and reported out to the customer in the tool
  - Additional platform "snapshots" can be generated and stored in the DAPP throughout the Platform life cycle

Auto Verify Tool



RSAConference2019

DEMO

Video


Transparent Supply Chain DAPP
localhost:56437/Login
Transparent Supply Chain - DAPP
Transfer Ownership
Login
Register
User Logged in as :
Login
Select a Role and Click Login
ODM User
OEM User
Reseller
Distributor
Platform Owner
Login
Login with Email
Enter the Registered Email and Click "Login with Email"
Enter Email Address
Login with Email
© 2018 - Transparent Supply Chain - DAPP
1:14 PM
1/16/2019

RSAConference2019

TSC on Blockchain Proof of Concept

Performance and Security

Performance and Throughput Comparison

Public Ethereum

Private Ethereum

	Public Ethereum	Private Ethereum
Block mining time	14.5 sec per block	14.5 sec per block
Confirmation time	10 confirmation blocks (145 sec confirmation)	10 confirmation blocks (145 sec confirmation)
Block Gas Limit	8,000,000 gas per block	**320,000,000 gas per block**
Theoretical Capacity	500,701 platforms / year	**188,208,579 platforms / year**

Security Comparison

Criteria	Public Ethereum	Private Ethereum
Confidentiality	• End to end file encryption in transit and storage. Uses cloud storage, based on KMS key. • Depending on storage key management, access can be controlled so that only the authorized users have access.	• End to end file encryption in transit and storage. Uses cloud storage, based on KMS key. • Depending on key management, access can be controlled so that only the authorized users have access. • Additionally, private blockchain limits on-blockchain data access to authorized parties
Privacy / Anonymity	• Worst of all, pseudonymous at best. Anonymity easy to compromise in public internet.	• Pseudonymous. Anonymity exposure limited only to network participants.
Trust	• Large decentralization. Massively distributed, allows independent confirmation, distributed trust among entire public networks (thousands of nodes)	• Limited decentralization. Small distribution, allows independent confirmation by individual participants.
Reliability	• Highly reliable and available	• Reliability based on underlying infrastructure.

RSAConference2019

TSC on Blockchain Proof of Concept

Findings and Observations

Development Ecosystem

- Access to development tools, documentation, and sample code is challenging.
- It is recommended to use patterns to enable scalability and maintenance.
- Difficult to integrate tools and programming languages to develop the Ethereum application.
- Recommended Tools:

Truffle	•Development framework •https://github.com/trufflesuite/truffle
Geth	•Ethereum node in Go •https://github.com/ethereum/go-ethereum/wiki/geth
Ganache	•Run simulated dev network •https://truffleframework.com/ganache
MIST Browser	•Ethereum web browser •https://github.com/ethereum/mist
Nethereum 3.0	•.NET DAPP integration library •https://nethereum.com/

Challenges and Learnings

- Little documentation available to address issues encountered during development.
- Nethereum is an excellent library for integrating C# code
- Research on blockchain security is limited. Few mathematical models exists to evaluate security of blockchain transactions.
- Transactional capacity on the Ethereum blockchain is limited. Private Ethereum configuration changes can be made to improve performance.

RSAConference2019

Conclusions and Summary

Conclusions and Recommendations

- Conclusions
  - Increased platform security can be achieved by using blockchain for platform attestation
  - Data storage is now decentralized, no central party has access or control
  - Privacy in the blockchain is always a concern, private blockchain reduces exposure.
  - Developing blockchain security models is imperative as future work
- Recommendations
  - Transfer supply chain management to the blockchain whenever possible
  - Private blockchain networks are better suited for supply chain solutions where privacy and performance are required
  - Use off-chain sensitive data storage such as Cloud storage
  - Use blockchain to maintain integrity of data records

Summary

- A Trusted Supply Chain is based on a hardware Root of Trust and the Blockchain
  - TPM provides hardware Root of Trust
  - Ethereum blockchain provides supply chain trust
- End-user verifiable component authenticity backs up the hardware Root of Trust
  - Auto-Verify tool validates the system component
  - Blockchain provides data integrity and verification
- Blockchain implementation of a Trusted Supply Chain is feasible

Apply What You Have Learned Today

- Next week you should:
  - Consider your companies IT Components supply chains
- In the first three months following this presentation you should:
  - Identify IT Components that have supply chain risk
  - Determine if there is an opportunity to incorporate TSC supply chain
- Within six months you should:
  - Implement a blockchain based secure supply chain solution
  - Consider platforms that incorporate TSC
  - Review the Trusted Supply Chain on Blockchain POC whitepaper (located here)

Helpful Resources

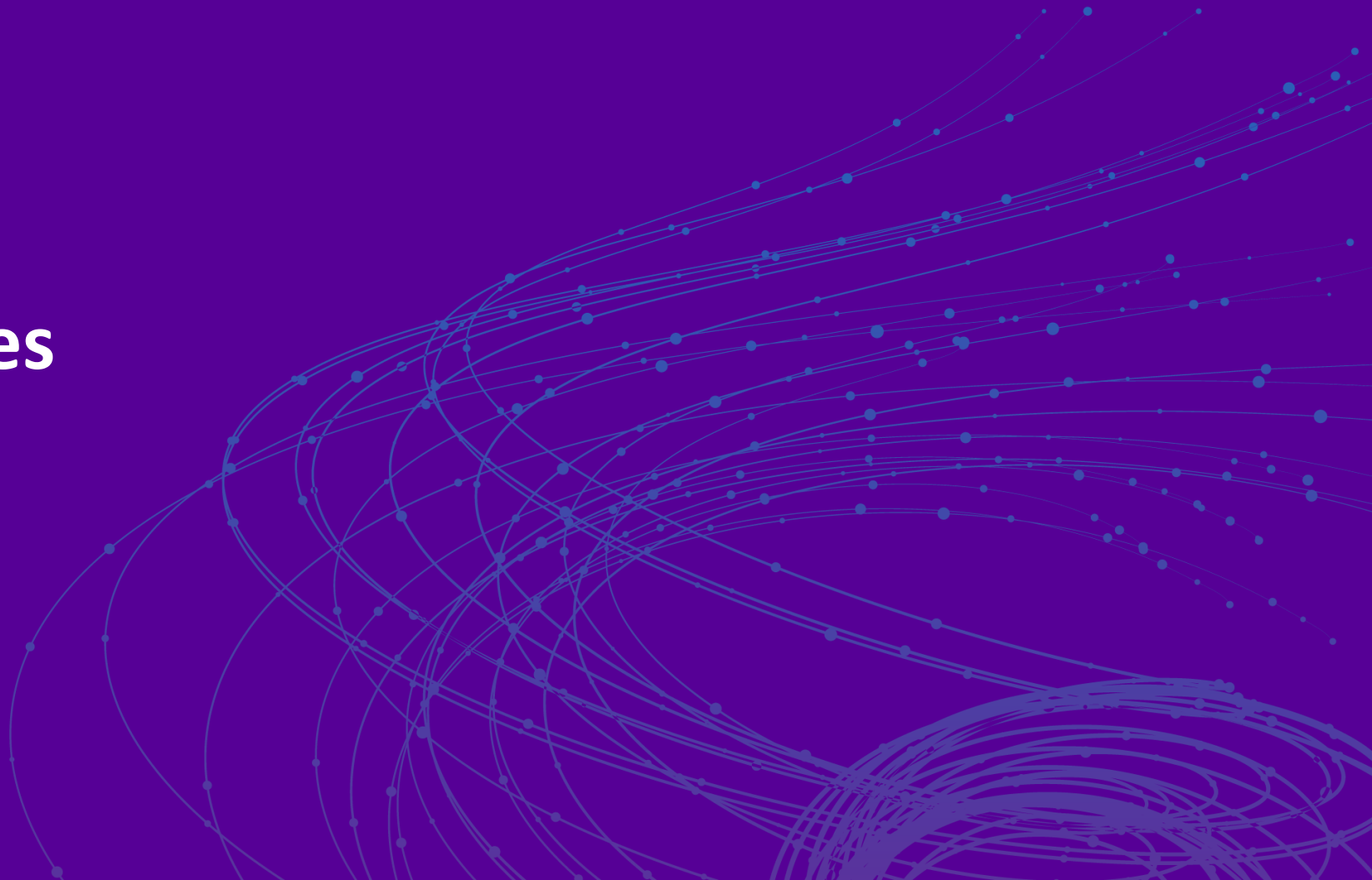
- The Ethereum project (https://www.ethereum.org/)
- The Five Types Model Sample Project (https://github.com/harshpokharna/The-5-Types-Model-Simple-Bank-System-Solidity)
- The Ethereum Blog (https://blog.ethereum.org/)
- Solidity Documentation (https://solidity.readthedocs.io/en/latest/index.html)
- Nethereum Documentation (https://nethereum.readthedocs.io/en/latest/)
- Smart Contract Programming Tutorial (https://medium.com/@ConsenSys/a-101-noob-intro-to-programming-smart-contracts-on-ethereum-695d15c1dab4)
- Ethereum and Solidity (https://www.udemy.com/ethereum-and-solidity-the-complete-developers-guide/)

References

- Contacts:
  - Tom Dodson: tom.dodson@intel.com
  - Eduardo Cabre: eduardo.cabre@intel.com
- Transparent Supply Chain
  - https://www.intel.com/content/www/us/en/servers/transparent-supply-chain.html
- Software Stacks
  - https://github.com/tpm2-software
  - https://sourceforge.net/projects/ibmtpm20tss/
- A Practical Guide to TPM 2.0
  - https://www.apress.com/us/book/9781430265832

RSAConference2019

Support Slides



TSC on Blockchain – Supply Chain Flows