Protecting Integrity of Infrastructure with Blockchain ...

June 24th, 2016

Scott Taggart, Santanu Das, Ulvi Kasapoglu, Clark Williams, David Mc Sweeney

Objectives of Cyber Security: Ensure CIA

- **Confidentiality**
- **Integrity**
- **Availability**

While much attention is given to compromises of *Confidentiality* (data breaches) and *Availability* (DoS), practically speaking all attacks require some a compromise of *System Integrity* in order to succeed

Cost of Compromise: Integrity versus Confidentiality

	Confidentiality Breach	Integrity Breach
Your Car	Your braking patterns are exposed.	Your braking system stops working.
Your Flight	Your flight plan is posted on the Internet. (note: it already is)	Your plane's instruments report that you are 1,000 feet higher than you actually are
Your Power Station	Your electricity bill is published online.	Critical systems compromised leading to shutdown or catastrophic failure
Your Pacemaker	Your heartbeat becomes public knowledge.	Shutdown and death
Your Home	The contents of your fridge are "leaked". You drink *how much* beer?	Your security system is remotely disabled

Source: https://guardtime.com/blog/blockchain-security-implications-for-the-industrial-internet

Example #0: Falsification of Aircraft Locational Information

Falsification of Aircraft Locational Information

What if you tricked a plane into thinking the ground isn't where it is?

This is actually based on a true story*...

* OK - maybe not a true story

Example #1: Maliciously Modified Ground Vehicle Firmware

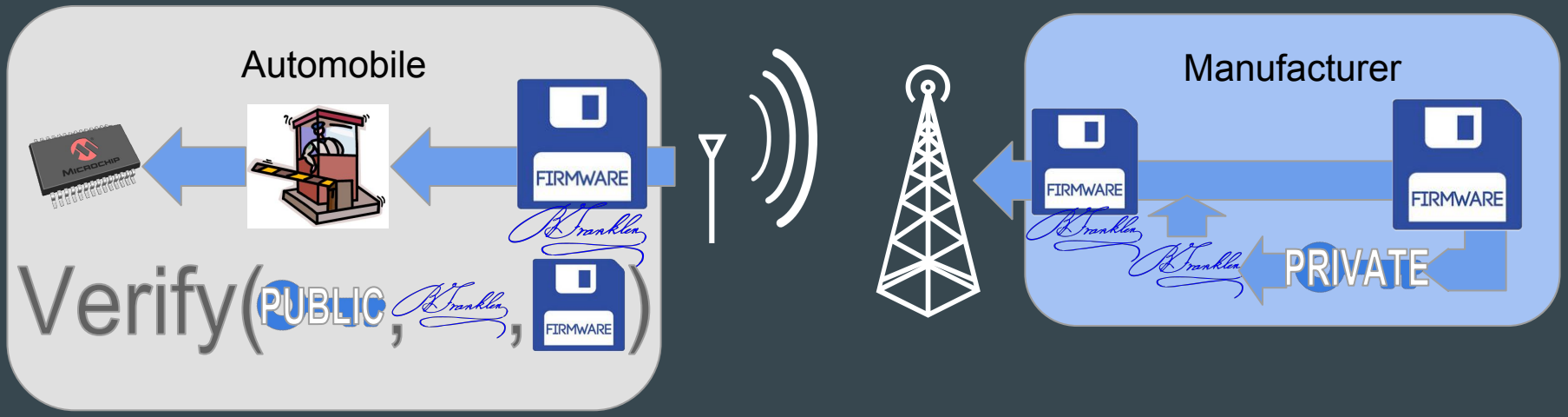
Compromise of Ground Vehicle Firmware

- Modern automobile contains upwards of 80 programmable Electronic Control Units (ECUs)[1] that manage practically every aspect of the vehicle's functionality
- Given the increasing complexity of this firmware and the incidence of bugs and new features there is great interest among automotive manufacturers in delivering Firmware Update Over The Air (FOTA)
- Who has interest in pushing illegitimate firmware to your automobile?
  - Car Thief
  - Competing Car Manufacturer
  - Terrorists

1) https://en.wikipedia.org/wiki/Electronic_control_unit

Traditional Solution: Public Key Cryptography

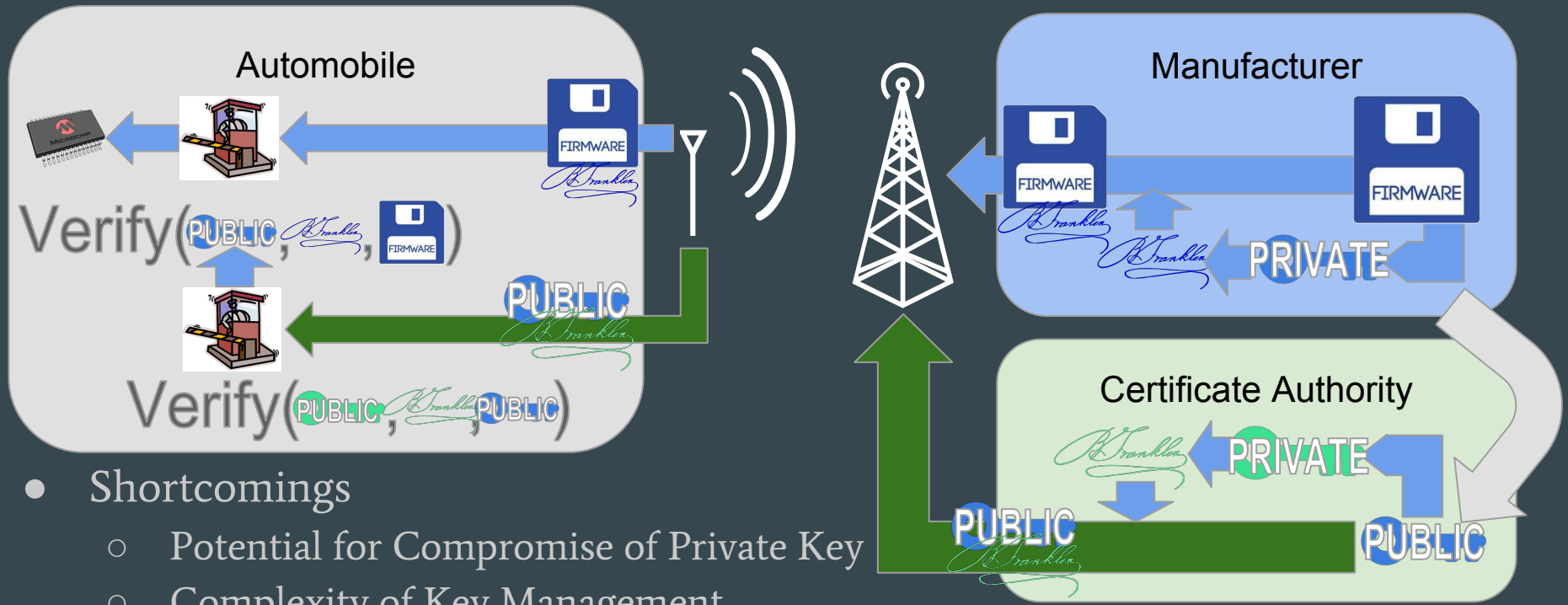
- Automobile rejects any firmware update that is not cryptographically signed with the automobile manufacturer's private key
- Need to revoke keys (effective after some date) when they are stolen



- Shortcomings
  - Potential for Compromise of Private Key
  - Complexity of Key Management
  - Signature Verification Computationally Expensive
- What if history of allowed firmware was universally visible?

Traditional Solution: Public Key Cryptography

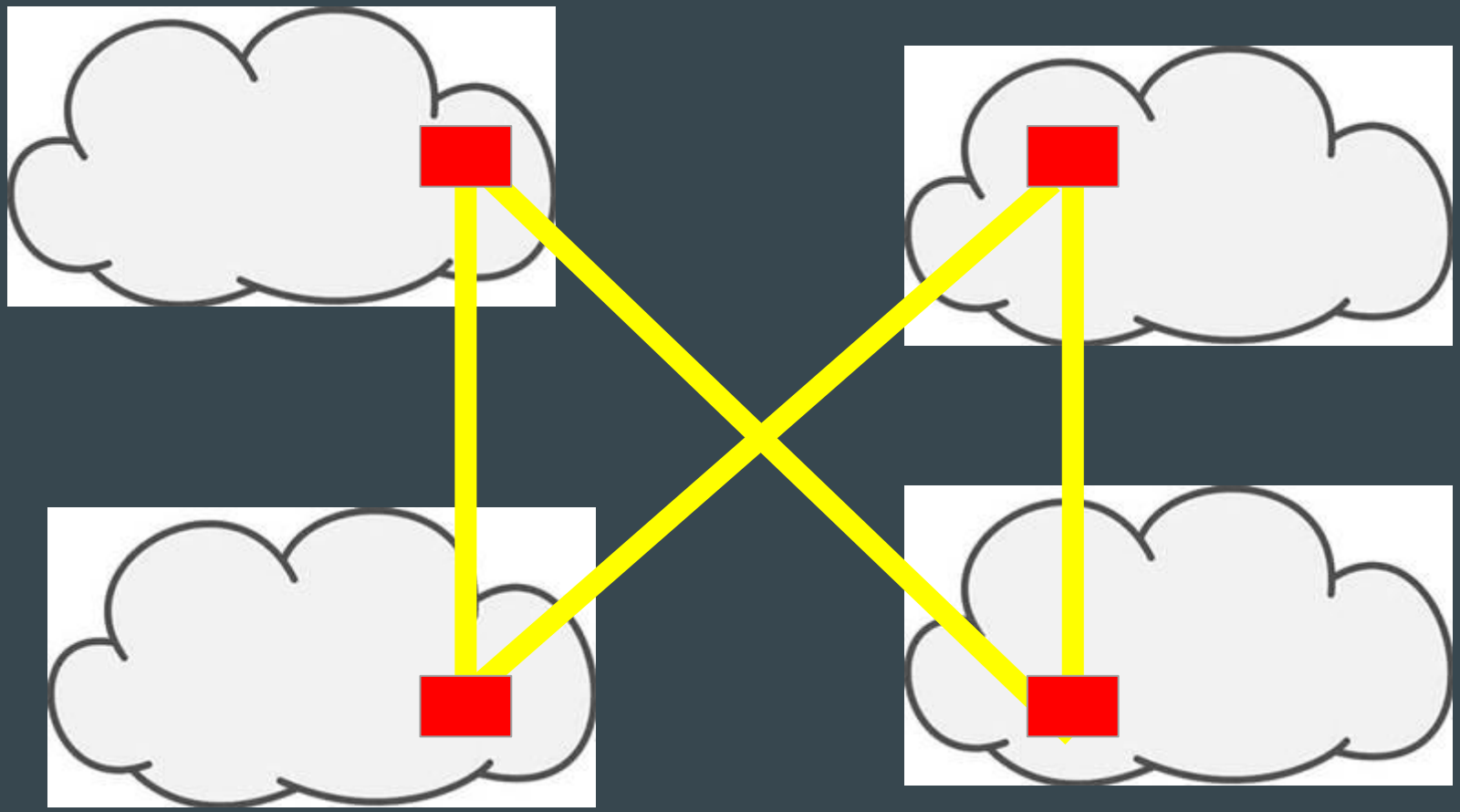
- Automobile rejects any firmware update that is not cryptographically signed with the automobile manufacturer's private key
- Need to revoke keys (effective after some date) when they are stolen



- Shortcomings
  - Potential for Compromise of Private Key
  - Complexity of Key Management
  - Signature Verification Computationally Expensive
- What if history of allowed firmware was universally visible?

Example #2: Coordinated update of Network Policy in a Distributed Ad-Hoc Tactical Network

Current methods for network management and control across nodes include protocols like SNMP that is susceptible to data tampering and DoS

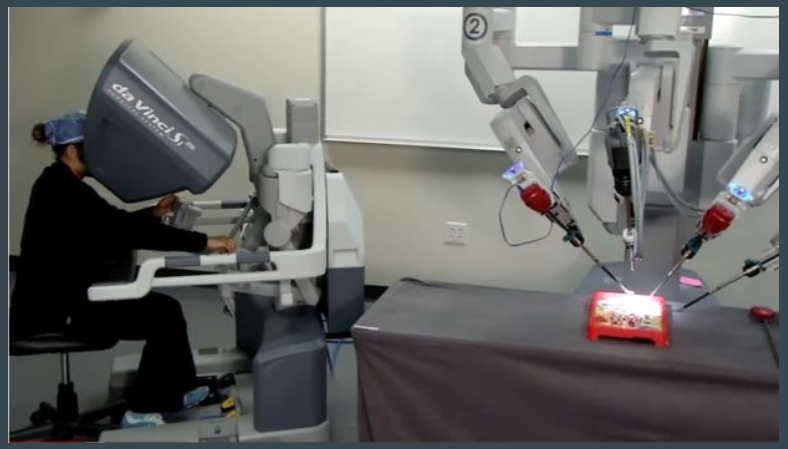


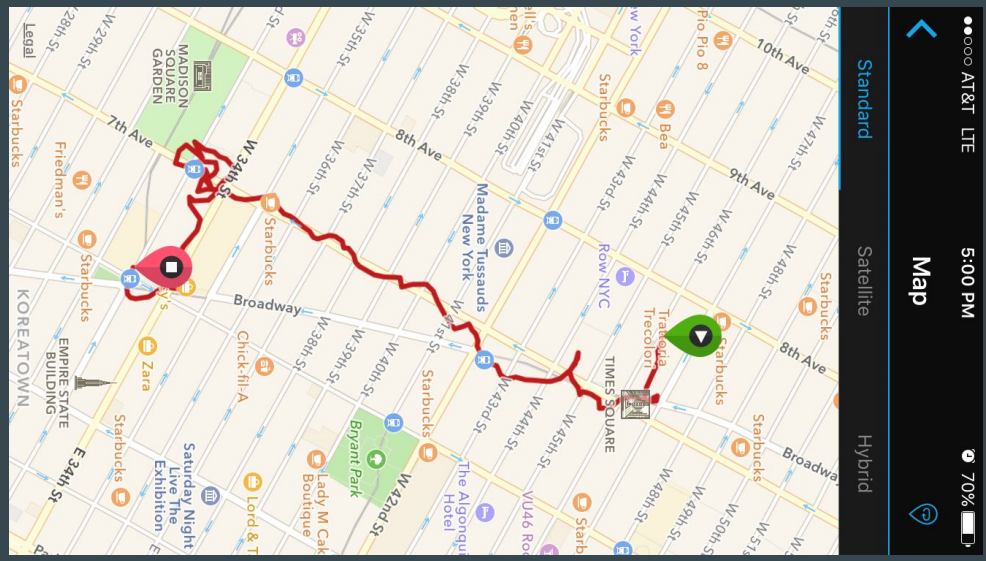
Secure Deconflicted Update of Policy Database (such as message prioritization) using Blockchain

Example #3: Breach of Health Data and Compromise of Medical Equipment

IoT for Health Data & Equipment

- Number and variety of network-connected devices that function in the context of health rapidly increasing:
  - **Remote Surgery Robots** (via Interoperable Telesurgery Protocol)
  - **Wearables** - Collecting personal health and spatio-temporal data
  - **Professional Monitoring Devices**





http://www.computerworld.com/article/2927471/healthcare-it/robot-performs-test-surgery-1200-miles-away-from-doctor.html

Compromise of Health Data & Equipment

- Connectivity introduces vulnerability in medical equipment:
  - Sensitive HIPAA data can be compromised.
  - Transactions can be manipulated.

- Possible Adversary / Motivation:
  - Monitoring Devices → Health data can be manipulated → Insurance Fraud
  - Wearables → Geolocation data coupled with social media → Marketing Value
  - Remote Surgery → Healthcare Instruments may be intercepted [1] → Sabotage / Assassinations

https://www.technologyreview.com/s/537001/security-experts-hack-teleoperated-surgical-robot/

Example #4: Data Integrity for Law Enforcement

What can Keyless Signature Infrastructure (KSI) do?

- Digital data is signed by cryptographically linking a signature tag to the data. Any data can be signed
- Verifying the signature allows assertion of:
  - **Signing time:** When the data was signed
  - **Signing entity:** Which network node signed the data
  - **Data integrity:** The data has not been changed since signing

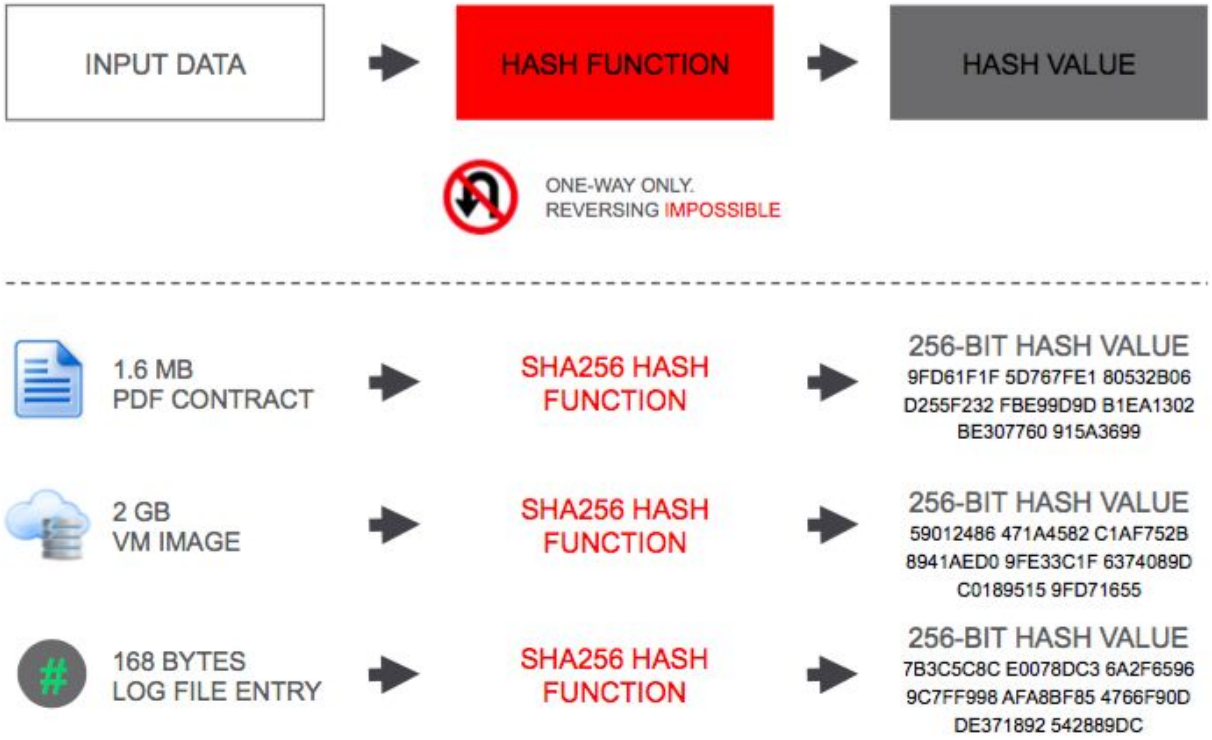
KSI Benefits

- Proof
  - Proof of time and integrity of electronic data as well as attribution of origin
- Massively scalable
  - System performance is practically independent of the number of clients
- Open verification
  - One needs to trust publicly available information only
- Portable
  - Data can be verified even after that has crossed organizational boundaries
- Long term validity
  - Proof is based only on the properties of hash functions
- Supports near real-time protection
  - KSI verifications require only milliseconds which allows clients to perform continuous monitoring and tamper detection
- Offline
  - The system does not require network connectivity for verification
- Post-Quantum
  - The proof stays valid even assuming functioning quantum computers, i.e. does not rely on traditional asymmetric or elliptic curve cryptography

Blockchain Technology

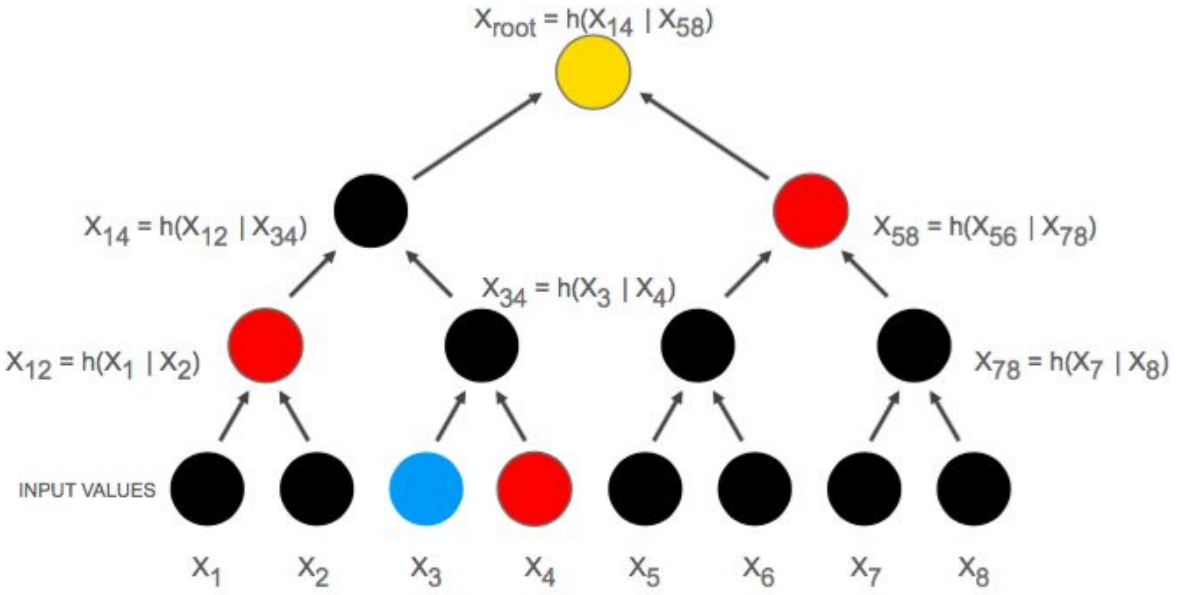
KSI is Based on Cryptographic Hash Functions

- A Hash Function takes arbitrarily-sized data as input and generates a unique fixed-size bit sequence as output.
  - The output is known as the Hash Value, message digest, or digital fingerprint of the input.
  - A cryptographically secure hash function is one-way.



Aggregating Individual Hash Values into a Tree

- A Hash Tree takes hash values as inputs and, via repeated hash function application, generates a single root hash value.
- On the figure:
  - x_1 to x_8 are the input hash values
  - h() represents hashing (hash function application)
  - | represents concatenation



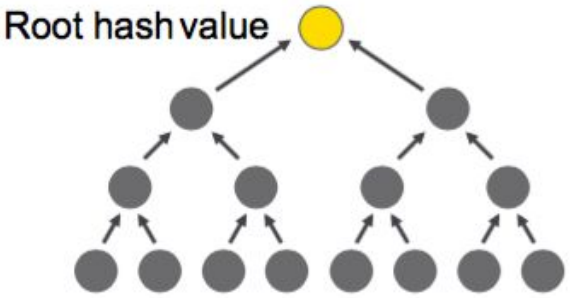
EXAMPLE: A HASH TREE WITH 8 LEAVES CONTAINING THE INPUT HASH VALUES

Add Root Hashes to the Calendar Blockchain

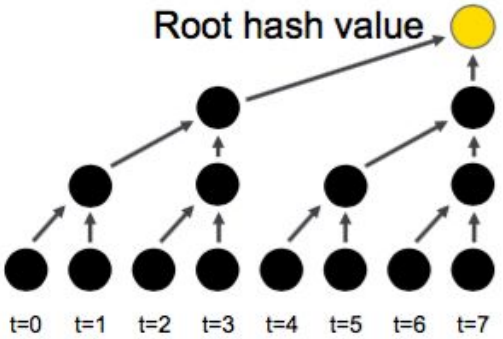
- The Calendar Blockchain is a special kind of hash tree that contains a time element.
- The Calendar Blockchain, unlike the aggregation tree, is perpetual: data is only appended to it, never removed.

- Each aggregation tree root value becomes a leaf node in the hash calendar. A new leaf is added each second and linked to previous entries.
- This extends the hash chain from the aggregation tree, through the hash calendar, to the calendar root hash value which can later be used to prove the time of signing.

HASH TREE



CALENDAR BLOCKCHAIN



Questions?

Your presenters

Scott Taggart - scott.taggart@qiotec.com
Santanu Das - santanu.das@navy.mil
Ulvi Kasapoglu - ali.ulvi.kasapoglu@oracle.com
Clark Williams - rwilliams@ll.mit.edu
David Mc Sweeney - dave.mcsweeny@state.ma.us