SECURING USER IDENTITY AND TRANSACTIONS SYMBIOTICALLY:

IOT MEETS BLOCKCHAIN

DAVID W. KRAVITZ, VICE PRESIDENT – CRYPTO SYSTEMS RESEARCH

JASON A. COOPER, EXECUTIVE DIRECTOR – EMBEDDED SYSTEMS SECURITY

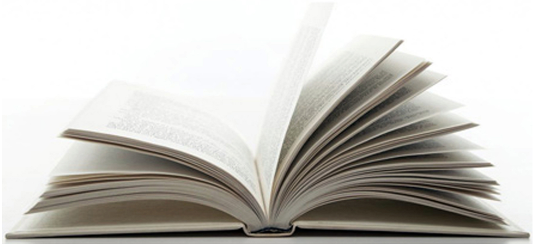
DARKMATTER

GUARDED BY GENIUS

CONCEPTS

- **Trust**
  - Between parties
  - Banks & Govt
  - Bitcoin?

- **Control**
  - Banks
  - Govt
  - Who says “Time Out!”?

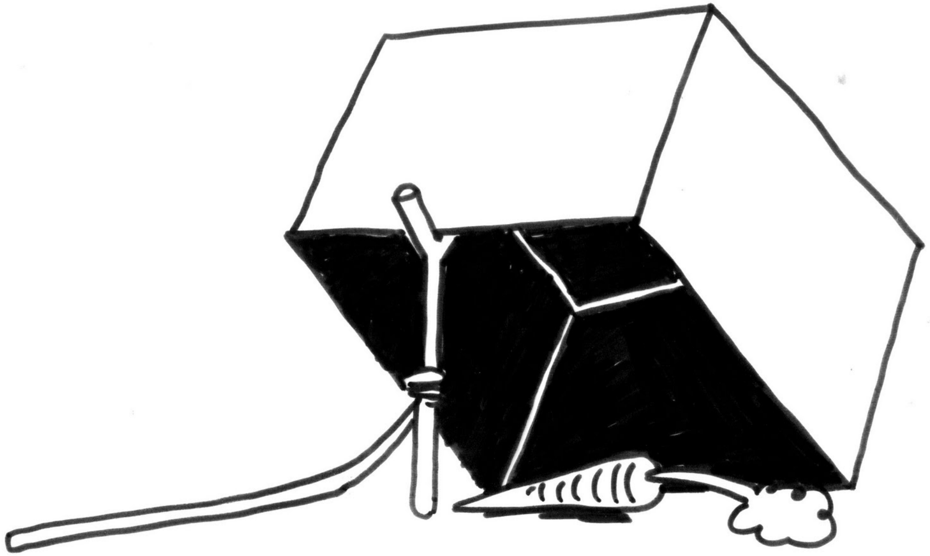


- **Data vs. Code**
  - Always Separate
  - Read one, Exec other

CRYPTO-CURRENCIES

- Distributed Data
- Currency not Issued by a Bank
- Regulated by Software
- Immutable History
- Reduced Correlation between TXNs

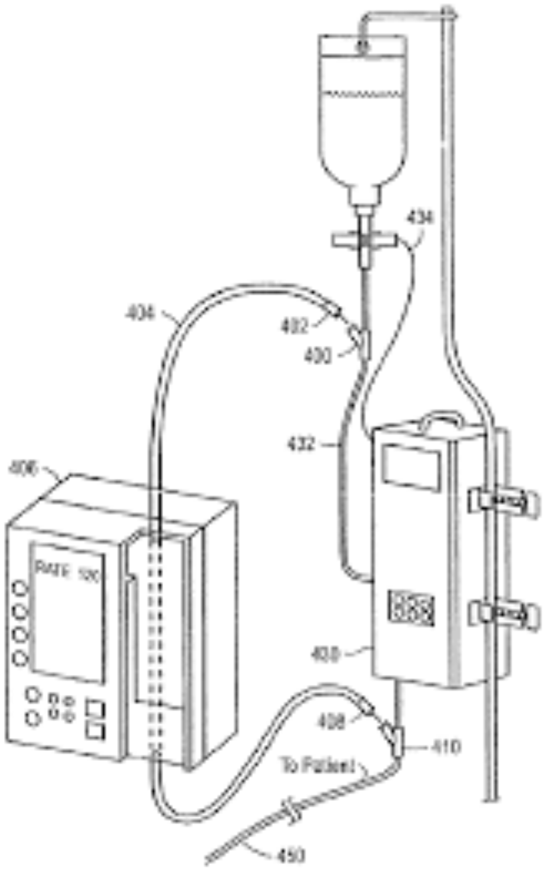
SMART CONTRACTS / CHAIN CODE



- Replace Legal Documents with Code
- Recorded on the Blockchain
- Executed by Blockchain Infrastructure
- Turing Complete & Rigid ?!
- No Failure Handling

LEDGER ACTIONS

- Augment Contracts with Code
- Executed by a Party to the TXN
- Errors can be Handled Locally
- Any Language or Subset thereof Party will Accept
- Asynchronous, Off-Chain Execution



OUR PROPOSED LEDGER

- IoT-Focused
  - Asynchronous Reporting
  - Off-Chain Auth/Attr/Exec
  - Auth Constrained Devices
- Distributed Data
- Immutable History <-> PKI
- No Correlation of TXNs
- Separate Validation & Consensus
- Shared / Single Histories

PUTTING CRYPTO TO WORK (CORRECTLY)

- Database management: immutable sequenced records support IoT ops tracking with need-to-know access
- Identity & attributes management: context-based

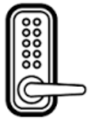
Attribute Certificate ⊃ Bob’s attribs || Bob’s public key cert ID

TCert ⊃ Bob’s attribs [encrypted*] || Bob’s one-time-use pub key

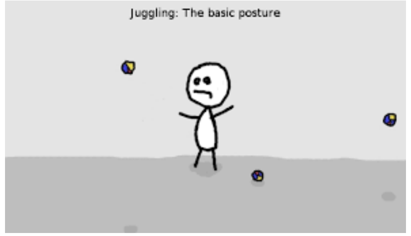
[Later: *TXN metadata includes selectively released keys]

- Risk management: constrained

But I’m Bob



OK, I’ve been expecting you:



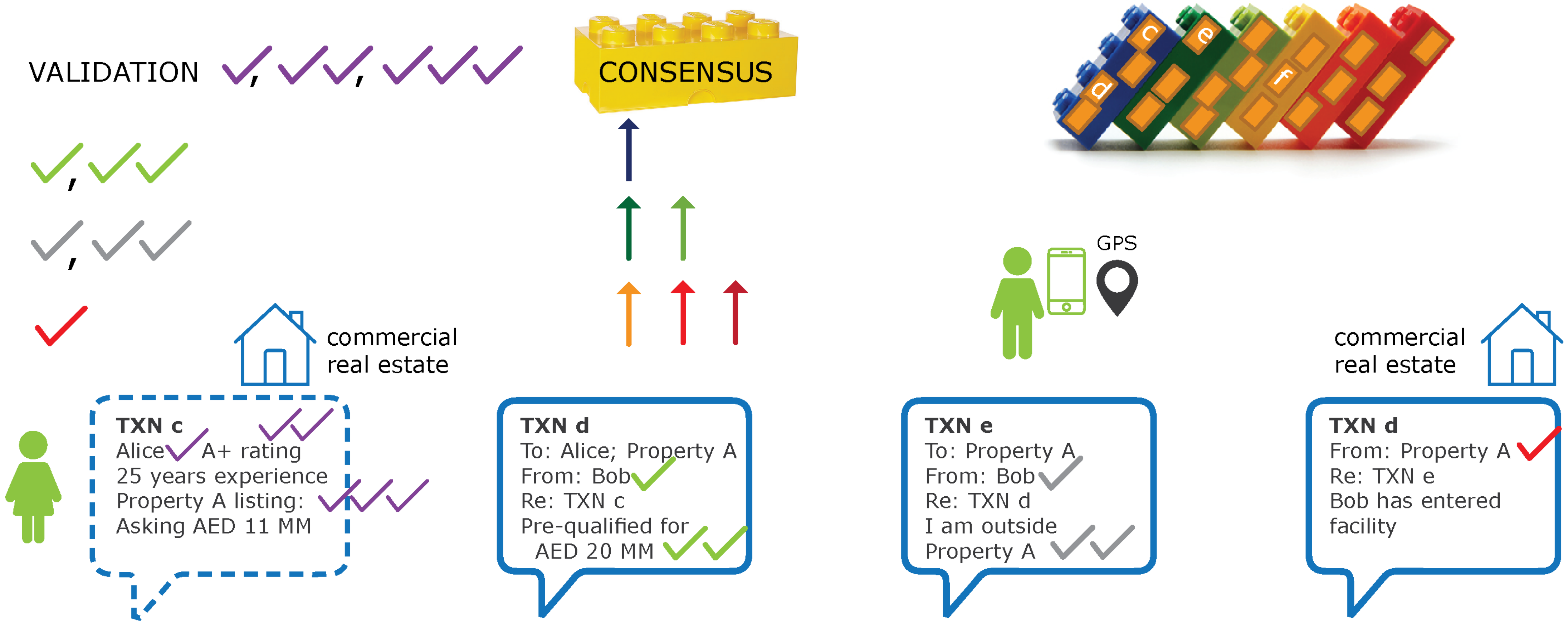
Unintended linkage

□

Privacy-preserving

☑

REAL-ESTATE LOCK BOX MEETS BLOCKCHAIN



TXN c
Alice ✓ A+ rating ✓✓
25 years experience
Property A listing: ✓✓✓
Asking AED 11 MM

TXN d
To: Alice; Property A
From: Bob ✓
Re: TXN c
Pre-qualified for
AED 20 MM ✓✓

TXN e
To: Property A
From: Bob ✓
Re: TXN d
I am outside
Property A ✓✓

TXN d
From: Property A ✓
Re: TXN e
Bob has entered
facility

Involves IoT: Property A (door lock, cameras, heat/AC, lighting, etc.)
Agent-less tour possible: immutable record of before-Bob / after-Bob condition of Property A

STANDARDS-BASED WITH A V2V ORIGIN

- Draft NIST Special Pub 800-63B **Authentication & Lifecycle Management**: “The verifier SHALL NOT store the identifying key itself, but SHALL use a verification method such as use of an approved hash function or proof of possession (PoP) of the identifying key to uniquely identify the authenticator.”
- Draft NIST Special Pub 800-63-3 **Digital Identity Guidelines** : “A digital identity is always unique in the context of a digital service, but does not necessarily need to uniquely identify the subject.”

CAMP LLC

Vehicle Safety Communications 5 (VSC5)

HONDA
Honda R&D Americas

Ford

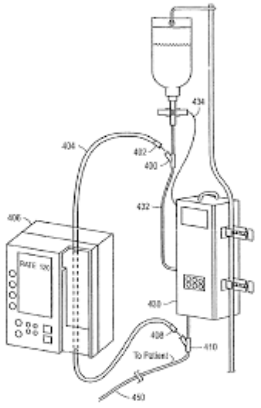
mazda

HYUNDAI·KIA MOTORS
Hyundai·Kia America Technical Center, Inc.

GM

NISSAN

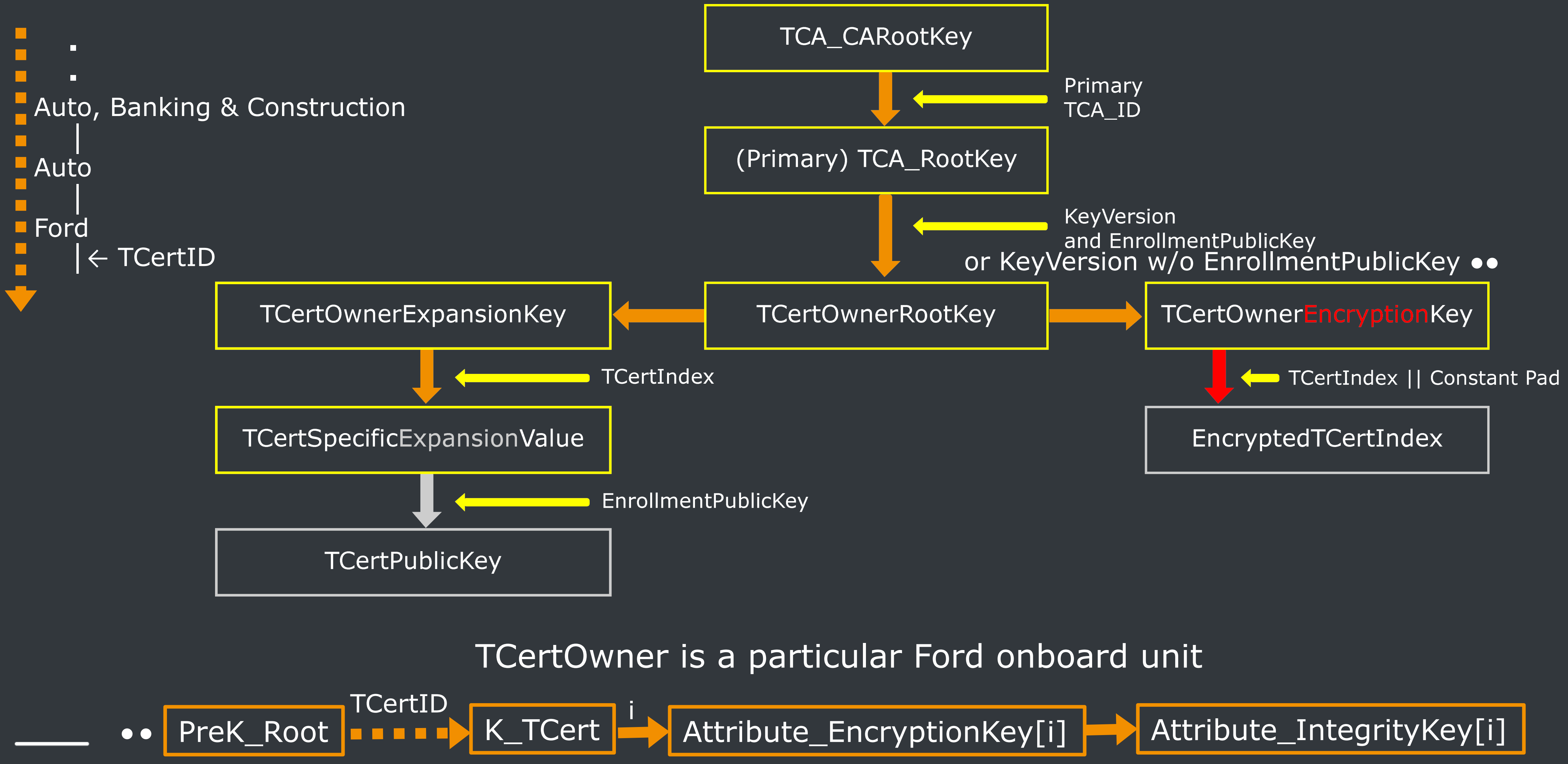
VOLKSWAGEN
GROUP OF AMERICA



MAKING THE BLOCKCHAIN ACCESSIBLE

- Signature TCert- owner:
  - key expansion to recover TCert private keys (sig; key agreement)
  - selective disclosure keys for TCert attributes PoP
- Key agreement TCert- requestor: certain of its PoP keys
- Primary TCA: threshold-/multi- sig generation of TemplateTCerts
- Subordinate TCA: generation of TCerts (redundant & restricted ops)
- Audit$_1$: capability to cluster TXNs for subset of TCert owners
- Audit$_2$: passively access PoP keys for subclasses of users/devices
- Audit$_{3pre}$: payloads via Validator-enforced TXN-creator audit granting
- Audit$_{3post}$: payloads via key agreement TCerts or authorized queries

KEY MANAGEMENT



:

Auto, Banking & Construction

Auto

Ford

← TCertID

TCA_CARootKey

Primary TCA_ID

(Primary) TCA_RootKey

KeyVersion and EnrollmentPublicKey or KeyVersion w/o EnrollmentPublicKey ●●

TCertOwnerExpansionKey

TCertOwnerRootKey

TCertOwnerEncryptionKey

TCertIndex

TCertIndex || Constant Pad

TCertSpecificExpansionValue

EncryptedTCertIndex

EnrollmentPublicKey

TCertPublicKey

TCertOwner is a particular Ford onboard unit

●● PreK_Root

TCertID

K_TCert

i

Attribute_EncryptionKey[i]

Attribute_IntegrityKey[i]

SUPPLY CHAIN PROVENANCE: PSEUDONYMS

Device Manufacturer $\xrightarrow[\text{TXN A}]{}$ Distributor $\xrightarrow[\text{TXN B}]{}$ Consumer i $\xrightarrow[\text{TXN C}]{}$ Consumer j

Device Creation (TXN A): payload ⊃ Device Serial Number(s); metadata ⊃ Device Manufacturer signature TCert with "selectively released" attribute(s) key(s) + Device Manufacturer-acquired Distributor- owned key agreement TCert with Distributor attribute key

First Sale (TXN B): payload ⊃ specific Device Serial Number and decryption key for payload of TXN A; metadata ⊃ Distributor signature TCert with attribute(s) key(s) + Distributor-acquired Consumer i-owned key agreement TCert with pseudonym attribute key

eBay (TXN C): payload ⊃ decryption key for payload of TXN B; metadata ⊃ Consumer i signature TCert with pseudonym attribute key (with pseudonym matching TXN B) + Consumer i- acquired Consumer j- owned key agreement TCert with pseudonym attribute key

AN M2M USE CASE

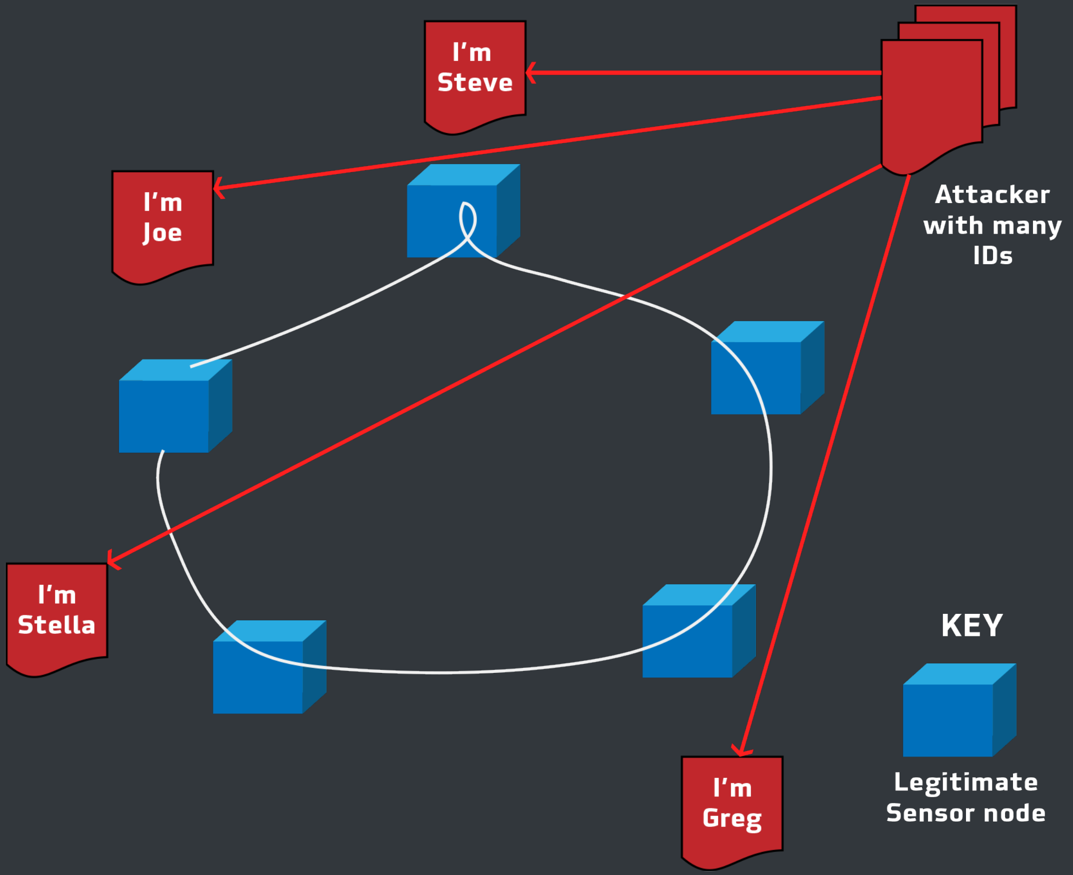
External Attribute Authority (AA)
Internal Attribute Certificate Authority (ACA)

- **APPLICABLE TO AD HOC COLONIES OF DEVICES ORGANIZED FOR TASK FULFILLMENT**
- **CALLS FOR DEVICE PARTICIPATION AS BLOCKCHAIN TRANSACTIONS**
  - May specify acceptance criteria: minimum attribute rating scores
  - Responses by qualified devices incorporated into blockchain
- **DEVICES CAN USE FACTORY-PROVISIONED CERTIFICATES**
  - Prove attributes to ACA via AA-issued assertions
- **OFF-CHAIN FULFILLMENT: RESPONSE TRANSACTION TCERTS MAY BE USED FOR AUTHENTICATED-TLS COMMUNICATIONS**
- **ON-CHAIN MUTUAL RATING OF DEVICES: REFERENCE RATED DEVICE’S TCERT**
  - Ratings encrypted for access by Analytics Processor (AP)
  - AP clusters individual ratings according to deviceID
  - AP acting as AA issues (cumulative) attribute rating assertions

AN H2M USE CASE

- USERS RATE EXPERIENCES WITH PHYSICAL ESTABLISHMENTS/VIRTUAL SERVICES
- ESTABLISHMENT/SERVICE PROVIDER AS OWNER OF TIME-LIMITED TCERTS EMBEDDED WITH RATING SCORES
- A RATING IS DISCARDED BY AP IF SUBMITTED BY A DEVICE THAT WAS NOT “PRESENT” AT ESTABLISHMENT OR SERVICE PROVIDER
    - As determined via TCert-based transactions submitted (a) during presence at establishment/use of service, and (b) later for rating
    - Recall AP can cluster TCerts according to their owners

THWARTS SYBIL ATTACKS



WRAP-UP

Consolidation: M2M, supply chain, financial services, asset transfer

- Mutually beneficial symbiosis
  - Use **identity**/attributes: secure **transaction** authentication/authorization
  - Reference immutable **transaction** history: counter fraud against static **identity**
- **Fortify multi-factor authentication** to resist hijacking
- **Extend multi-factor authentication** to “voting” by neighboring devices that are not within the control of the device being attested
- Extend from “device” to **groups of devices** for availability, while not falling prey to attacks against ill-advised key management
- Vetted crypto: **combined**, where appropriate, to prevent leakage; **isolated**, where appropriate, to manage fine-grained access control

QUESTIONS?