APPLIED CRYPTOGRAPHY AND PRACTICAL EXAMPLES

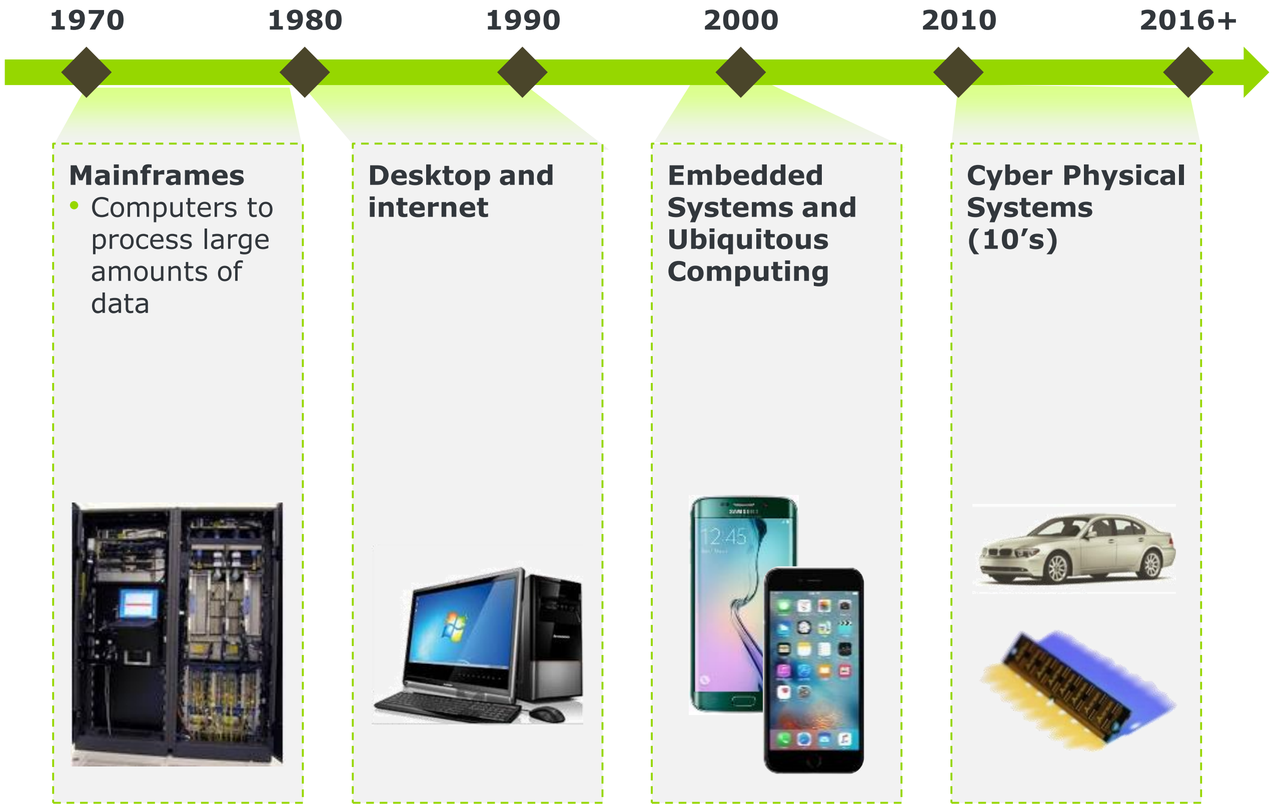
DR. NAJWA AARAJ

INTERNATIONAL CRYPTO MODULE CONFERENCE
17 MAY 2017

DARKMATTER

GUARDED BY GENIUS

COMPUTATIONAL SYSTEMS EVOLVED



1970 1980 1990 2000 2010 2016+

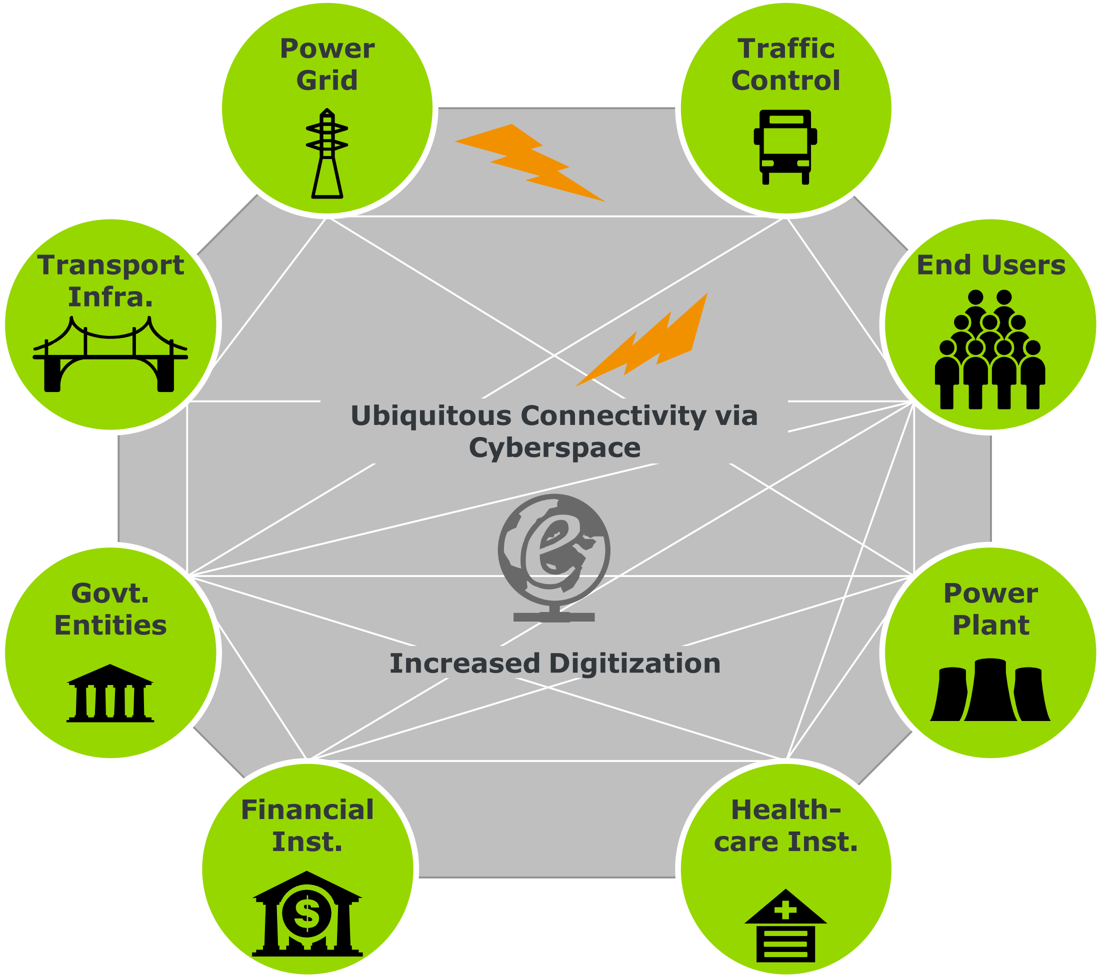
Mainframes

- Computers to process large amounts of data

Desktop and internet

Embedded Systems and Ubiquitous Computing

Cyber Physical Systems (10’s)



Power Grid

Traffic Control

Transport Infra.

End Users

Ubiquitous Connectivity via Cyberspace

Govt. Entities

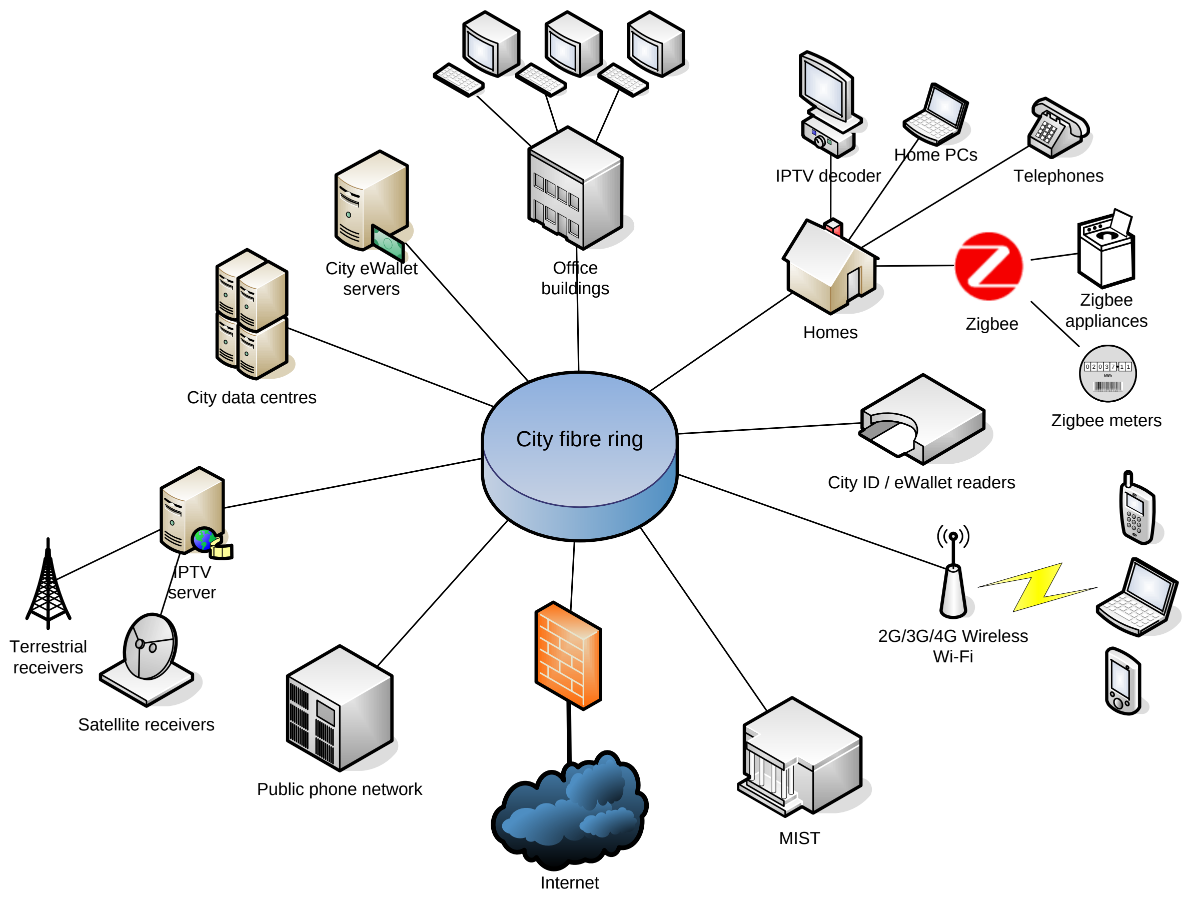
Power Plant

Increased Digitization

Financial Inst.

Health-care Inst.

SO DID THE COMPLEXITY OF ECOSYSTEMS



- City-wide ubiquitous data access across multiple devices types and technologies
- Should leverage Crypto for secure data handling in transit and at rest
- Can easily **leverage Crypto and BlockChain technologies** to enable efficient city-wide processes and transactions
  - G2G Transactions
  - C2G Transactions

APPLIED CRYPTO SOLUTIONS ARE REQUIRED

A Communication, OS and Kernel Security

- E2E Secure Communication transmitted over Voice, SMS, data, and Video Network
- Secure Cryptographic Algorithms
- Hardware Rooted Key Management
- Improved Random Number Generators
- Security Extensions – OS and kernel levels
- Integrity Monitoring
- Process Isolation and Type Enforcement
- Secure Boot and Hardware-based Root of Trust
- Full Encryption of Data at Rest

B BlockChain Security

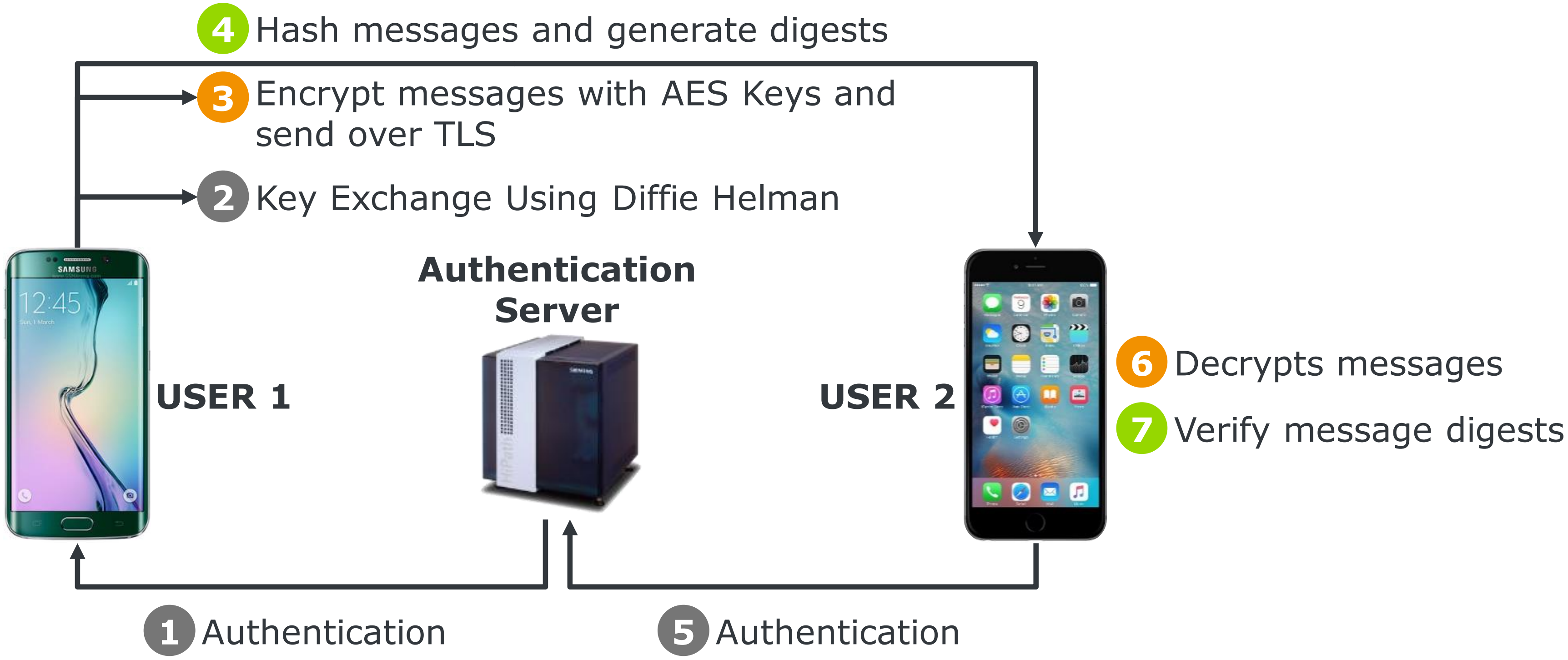
- Consolidated approach to IoT/supply chain and financial services/asset transfer: indispensable for suitably addressing smart city requirements
- Use of identity and attributes and multi-factor authentication
- Leverage immutable transaction history: references to previous transactions used to bolster against fraud beyond the limitations of traditional constructs of static identity

C Hardening of Crypto Implementations

- Vetted cryptographic components: combined, where appropriate, to prevent leakage; isolated, where appropriate, to manage fine-grained access control
- Algorithm and Protocol level countermeasures design and implementation

SECURE PROTOCOLS ARE NEEDED …

X Public Key Crypto   X Private Key Crypto   X Hashing



4 Hash messages and generate digests

3 Encrypt messages with AES Keys and send over TLS

2 Key Exchange Using Diffie Helman

6 Decrypts messages

7 Verify message digests

1 Authentication

5 Authentication

Secure Cryptographic Algorithms

Hardened Cryptographic Library/ EMM/ RNG

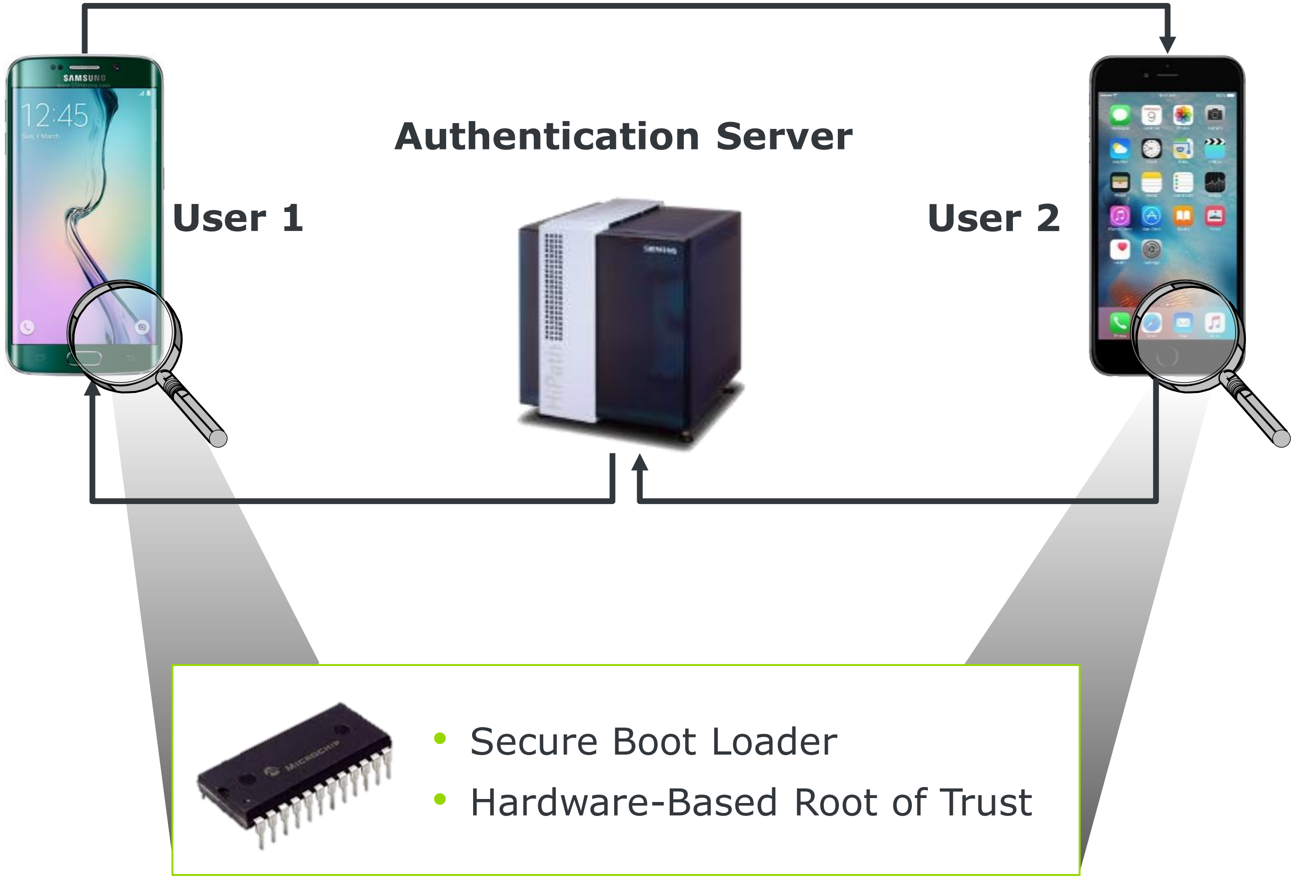
Robust Authentication and Localized PKI

Perfect Forward and Future Secrecy

Anonymity vs. Non-Repudiation

A

… SO IS KERNEL AND HARDWARE LEVEL SECURITY



- Secure Boot Loader
- Hardware-Based Root of Trust

Data at Rest Encryption

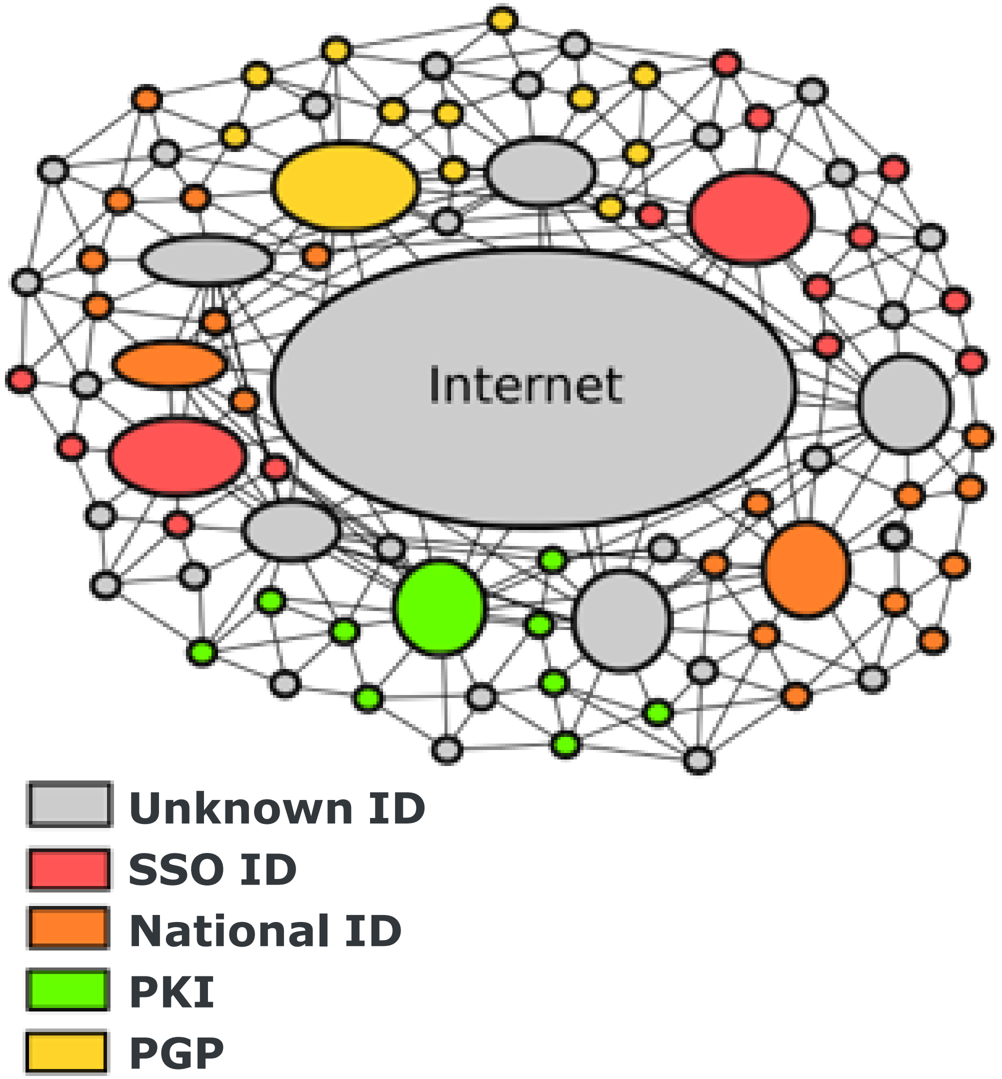
Real-time Integrity Monitor

Hardened Cryptographic Library

Hardware-Rooted Key Management

Hardened OS and Kernel

TODAY’S CONNECTED ECOSYSTEMS ARE NOT SECURE

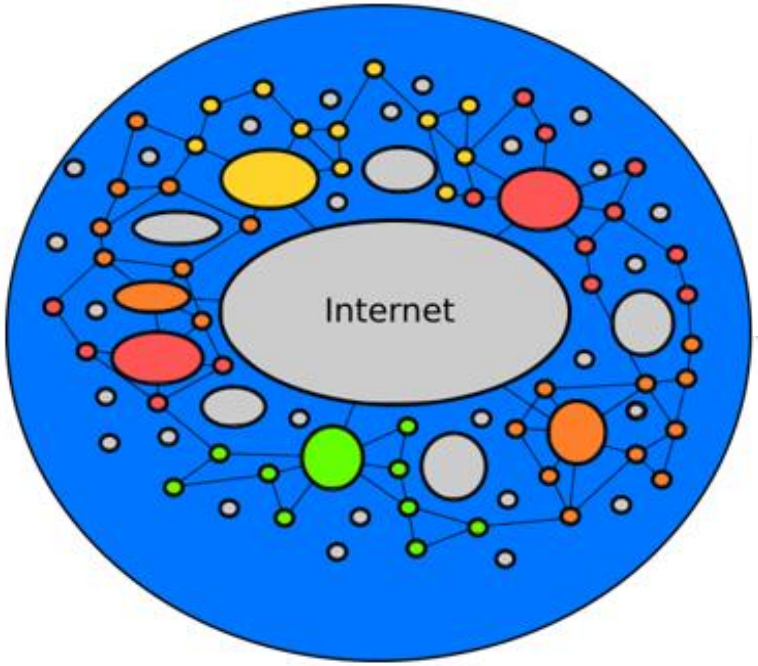


- Integrates different types of computing terminals and end points, covering large scale systems down to embedded systems such as IoT devices

- Major questions:
  - ➢ Weak identity management amongst devices, especially, IoT devices
    - ❖ **Issue 1:** Identity Management amongst connected devices
  - ➢ Most connected devices do not authenticate to server or other Peers on the Network
    - ❖ **Issue 2:** Authentication of connected devices
  - ➢ Data-in-Transit is not protected for Confidentiality and Integrity
    - ❖ **Issue 3:** Data-in-transit / Communications Security [Encryption]

B

BLOCKCHAIN CAN HELP THE ECOSYSTEM TODAY



- ⬜ **Unknown ID**
- 🟥 **SSO ID**
- 🟧 **National ID**
- 🟩 **PKI**
- 🟨 **PGP**

BLOCK CHAIN SOLUTIONS

Smart Cities Ecosystem Issues	How Can BlockChain help?
❖ **Issue 1:** Identity Management amongst connected devices	♪ Manages proofs of identity and possession of entitlements and other attributes
❖ **Issue 2:** Authentication of connected devices	♪ Manages risk by meeting requirements for audit and regulatory compliance
❖ **Issue 3:** Data-in-transit / Communications Security [Encryption]	♪ Basic Crypto Layer
	General: ♪ Operates across Private entities (such as hotels) and Public/governmental entities (such as customs & immigration)

REAL ESTATE TRANSACTIONS EXAMPLE

Alice

1) Real estate agent Alice enrolls and receives **transaction certificates:** _embedded identity, real estate license, and current rating_

3) Alice submits a **transaction** that includes a **link to listing data**, **hash(listing data),** and **minimum buyer criteria**; this transaction or follow-up transactions can include available / unavailable date-time appointment slots

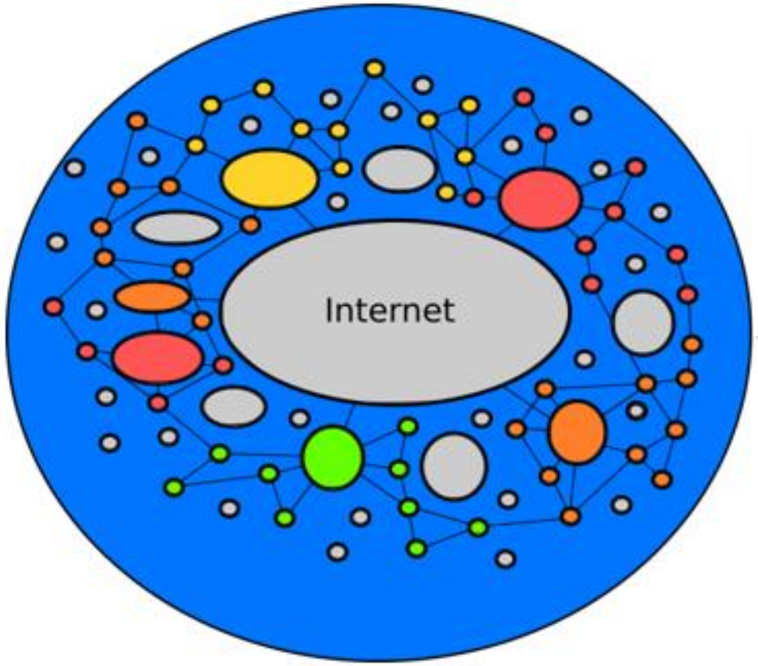
Bob

2) Potential buyer Bob enrolls and receives **transaction certificates:** _pre-qualification / pre-approval plus price level, and photo ID_

4) If Bob **is interested in** Alice**'s listing**, he submits a transaction to set up an appointment to review the property; his photo and appointment request are selectively released to Alice within the transaction –if Bob's transaction is accepted for inclusion in the blockchain

At the appointment date-time: if Bob**'s photo on the blockchain matches the image from the property's camera,** Alice **remotely activates the door unlock and video-calls** Bob **to begin the property tour**

BLOCKCHAIN CAN HELP THE ECOSYSTEM TODAY… BUT



⬜ Unknown ID

🟥 SSO ID

🟧 National ID

🟩 PKI

🟨 PGP

BLOCK CHAIN SOLUTIONS

Issues with Smart Cities Ecosystem	How Can BlockChain help?	Still … What are weaknesses of current Public / Private BlockChain?
❖ **Issue 1:** Identity Management amongst connected devices	♪ Manages proofs of identity and possession of entitlements and other attributes	« Weak identity / attribute management
❖ **Issue 2:** Authentication of connected devices	♪ Manages risk by meeting requirements for audit and regulatory compliance	« Weak authentication « Transactions authenticity based on (non-authenticated) public / private miners
❖ **Issue 3:** Data-in-transit / Communications Security [Encryption]	♪ Basic Crypto Layer	« Naïve: chained to its native crypto
	General: ♪ Operates across Private entities (such as hotels) and Public/governmental entities (such as customs & immigration)	General Weakness: 1. Unfriendly to the resource-constrained 2. Totally decentralized and loss of control [Public Blockchain mainly]

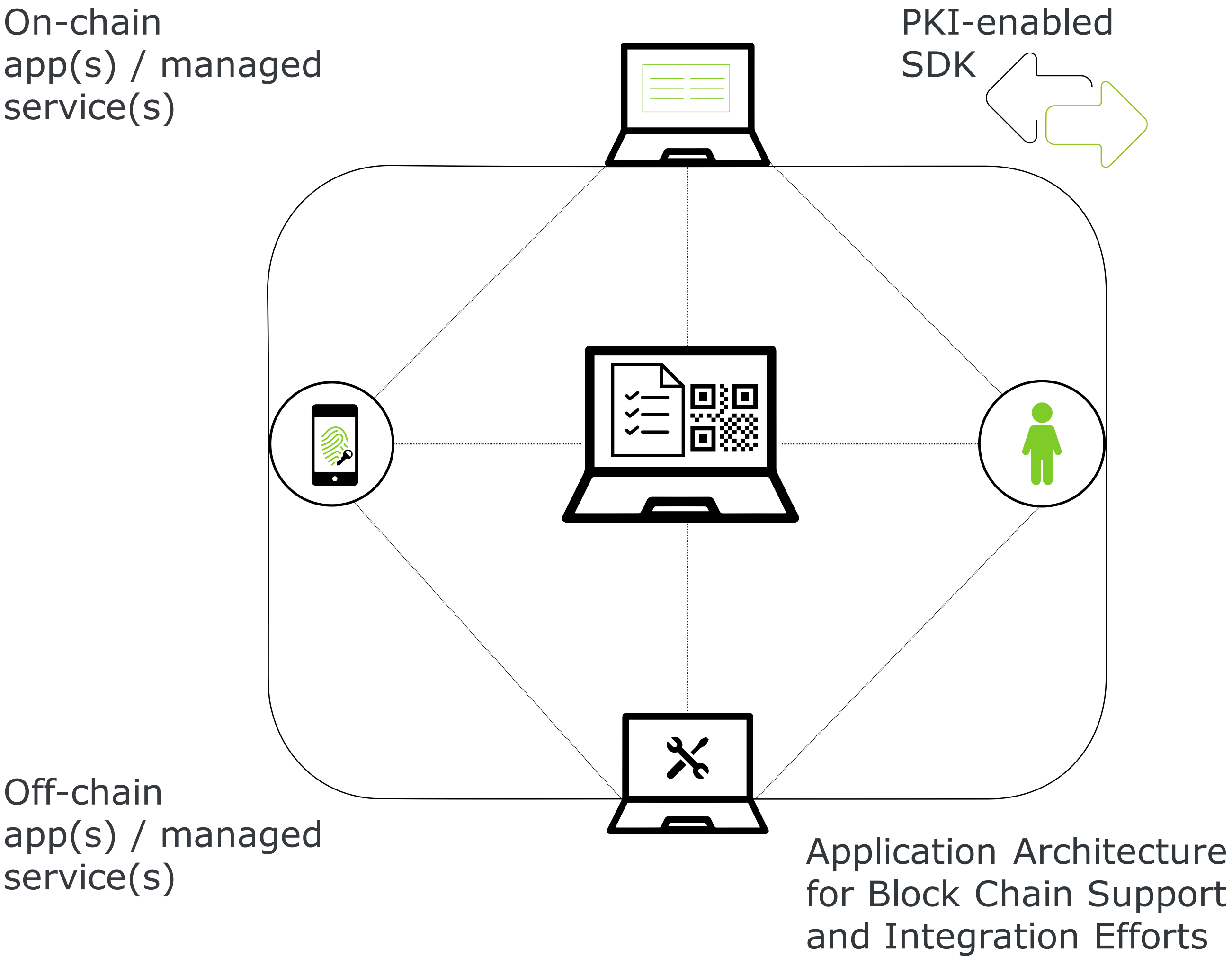
Current BlockChain suffers from Security and Scalability Issues

HOW DID WE IMPROVE UPON EXISTING SOLUTIONS?

Ledger
Blockchain
World State

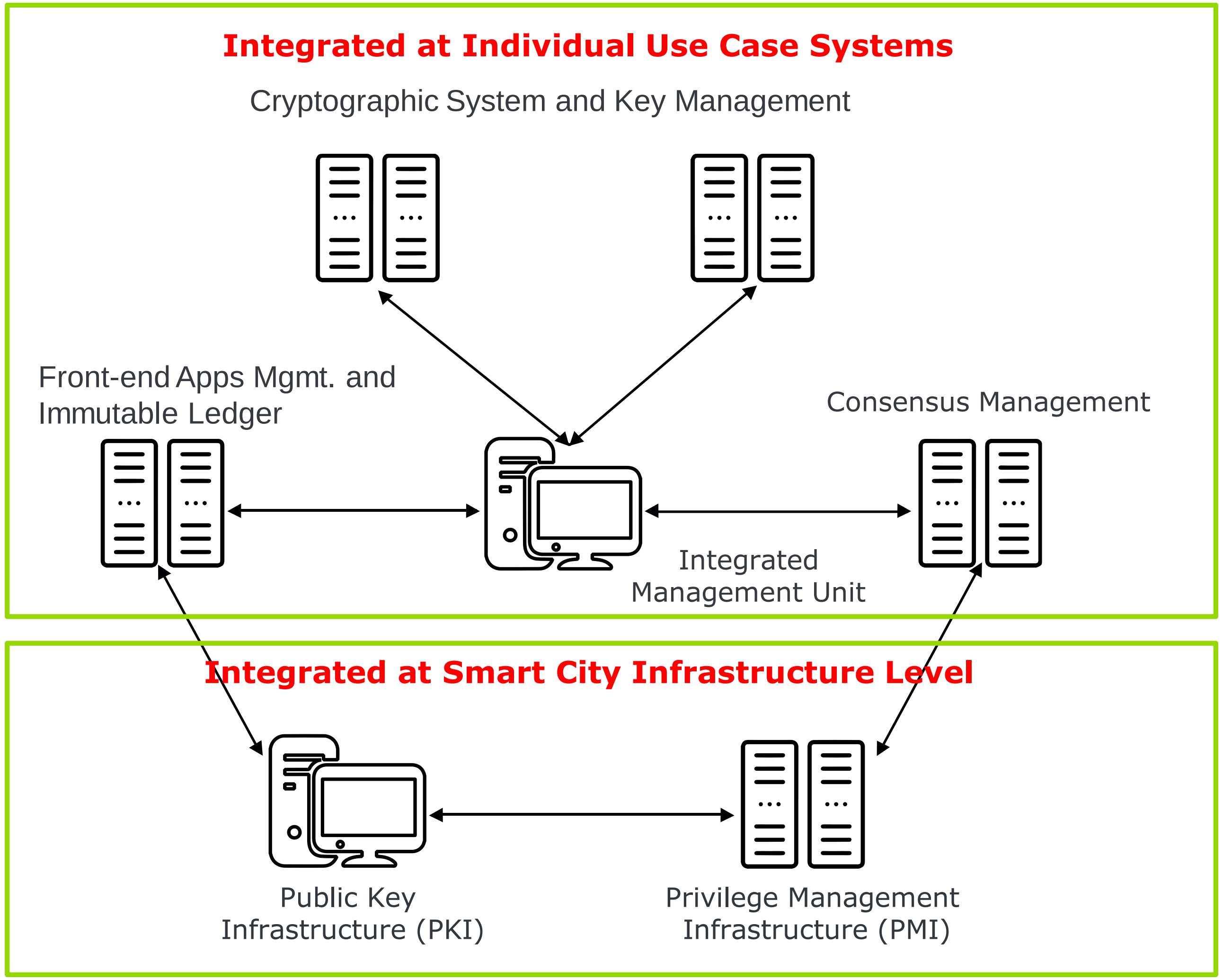
- identity
- authorization
- integrity
- confidentiality
- auditability

A recent Case Study with my Dark Matter team: **Hyperledger Project**


On-chain app(s) / managed service(s)
PKI-enabled SDK
Off-chain app(s) / managed service(s)

Application Architecture for Block Chain Support and Integration Efforts

DMLEDGER SDK TO RESOLVE ISSUES… ITS COMPONENTS



Integrated at Individual Use Case Systems

Cryptographic System and Key Management

Front-end Apps Mgmt. and Immutable Ledger

Consensus Management

Integrated Management Unit

Integrated at Smart City Infrastructure Level

Public Key Infrastructure (PKI)

Privilege Management Infrastructure (PMI)

A. Which parts of the BlockChain are provided by DM SDK?

- SDK written in C; scales down to smallest devices
- API can be called from many popular languages.
- Provides all functionality necessary for interacting with DM Ledgers in a secure manner
- Suite of example code for common applications. Android App, iOS App, Python web server, Java server, Go client, etc.
- Examples and the API documentation used to integrate quickly

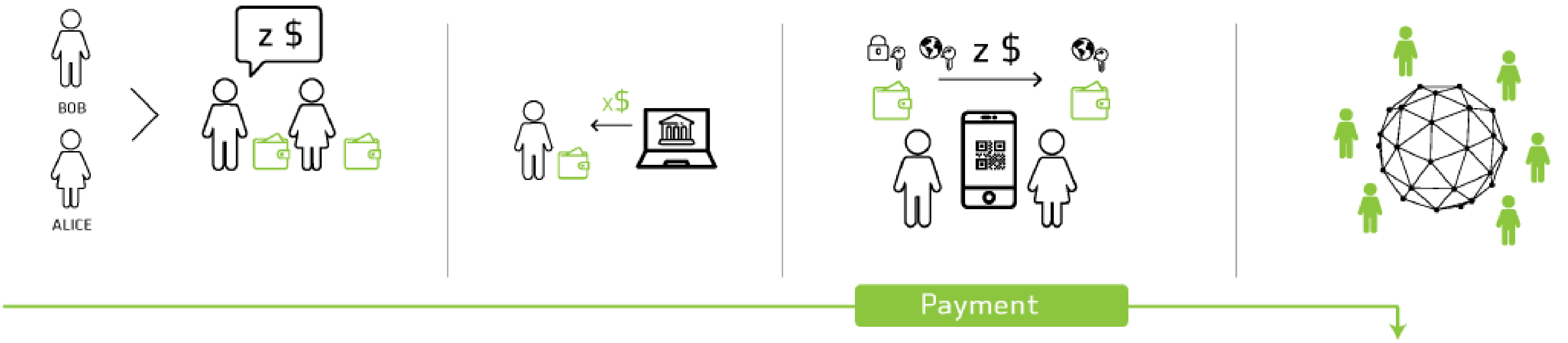
B. What other components from BlockChain technologies would still be missing that our SDK does not have?

None.

- We provide immutable ledger, validation, consensus, and decentralization
- Additionally, we provide Identity and Attribute Management and integration with existing implementations of the same.

B

PERMISSIONED BLOCKCHAIN IS USED (1/2)



Bob and Alice both have blockchain wallets on their mobile devices. Bob owes Alice z dollars

Bob's bank has deposited x dollars into Bob's blockchain accountID B from an off-chain bank account

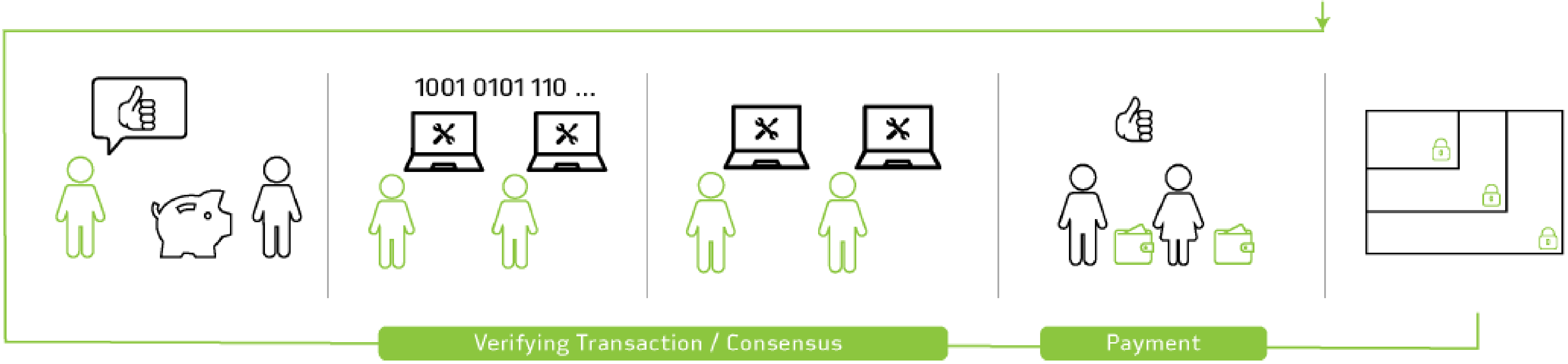
Bob gets a key agreement transaction certificate for Alice's accountID A, and extracts a transaction certificate and coresponding private key from his wallet in order to sign a transaction that transfers z dollars from accountID B to accountID A

(secured using the public key from Alice's key agreement transaction certificate and public key for Validator group)

Bob sends the transaction to a trusted Validating Peer (VP) that broadcasts the transaction to all other VPs

B

PERMISSIONED BLOCKCHAIN IS USED (2/2)



Each VP checks in state table that z ≤ accountID B balance

All VPs reach consensus (using PBFT algorithm) on the order to follow to execute the transactions

Each VP independently executes the transactions and incorporates them (as well as the state values that result from execution) into a new block - and the state table is updated

Bob and Alice receive confirmation that their transaction has been executed

Bob and Alice's transaction is added to the Blockchain. Every subsequent block added further increases the security of the previous blocks

BLOCKCHAIN & REAL-ESTATE; WHAT CAN GO WRONG

1

- Alice provides an A+ rating for herself and 25 years of experience; Alice submits a transaction **TXN s** **[TXN stands for Transaction]** with Property A listing asking AED 11Mn

Attack Vector: Alice lies about her experience / rating

Re: TXN s

2

- **Potential buyer** Bob enrolls**;** Bob **is interested in** Alice**'s listing**, he submits a transaction **TXN t** to set up an appointment to review the property; Bob is pre-qualified for AED 20Mn

Attack Vectors: (1) Bob lies about his identity and (2) mining process is not cryptographically validated; **mining process could be fraud**

Re: TXN t

3 4

- Alice submits a transaction **TXN u** that includes acceptance of Bob as a potential buy and schedules an appointment
- At the appointment time, Bob submits a transaction **TXN v** in which he announces his attendance and location

Attack Vectors: Bob Lies about his location

Re: TXN(s) u and v

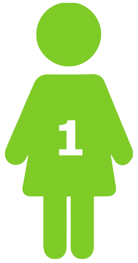
5,7 6,8

- Bob decides to buy and submits **TXN w** [Offer]
- Upon mining, Alice submits **TXN x** [Accept Offer]
- Bob submits transaction **TXN _y** [payment]
- Alice submits **TXN _z** [deed transfer]

Attack Vectors: (1) Crypto and original listing hash (TXN_s) are outdated; (2) mining could be fraudulent

While todays' BlockChain largely improves the process, it introduces critical vulnerabilities which may lead to: (1) seller's or buyer's **time waste**; (2) **Identity Fraud**; and (3) most critically (with lower probability) **fraud transactions** because of malicious or compromised miners

BLOCKCHAIN & REAL-ESTATE; DMLEDGER SDK MITIGATION

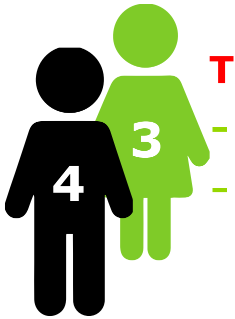


TXN_s Attack Vector: DMLedger SDK mitigation

- PKI-based authentication of Alice
- Enrollment Certificate issued for Alice [ECA]
- Transaction Certificated issued for TXN_s [TCA]
- Circumvention-proof cumulative rating associated to Alice transactions via auditable and immutable history

TXN_t Attack Vectors: DMLedger SDK mitigation

- PKI-based authentication of Bob
- Enrollment Certificate issued for Bob [ECA]
- Transaction Certificated issued for TXN_t [TCA]
- Consensus based on existing trust models through Validating Peers (PKI-authenticated)



TXN_{u,v} Attack Vector: DMLedger SDK mitigation

- Transaction Certificate issued for TXN_{u,v} [TCA]
- Through additional features, mobile devices and known stationary infrastructure units attest on BlockChain to their location while within spoof-proof communications range of Bob's phone

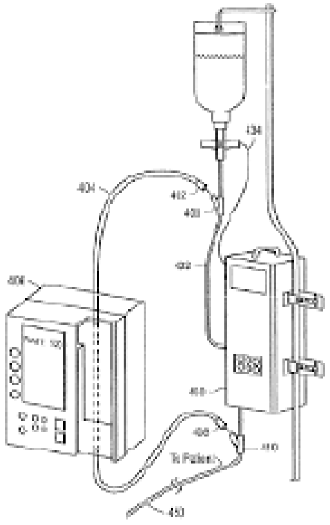
TXN_{w,x,y,z} Attack Vectors: DMLedger SDK mitigation

- Trans. Certificate issued for TXN_{w,x,y,x}
- Hash Agility enables data to outlive current crypto
- In-house developed crypto
- Consensus based on existing trust models through Validating Peers (PKI-enrolled and authenticated)

DMLedger SDK addresses vulnerabilities and ensures: (1) **authenticated transactions**; (2) transactions through **authenticated consensus** [**no fraudulent mining**]; (3) **immutable transactions history**; and (4) **hardened cryptography**

SMARTER CONTRACTS

- Our model is extensible to securing off-chain processes: communications and code execution
- Enables compatibility with existing IoT devices, independently of blockchain consensus
- Suitable for time-critical operations
  - Dispensing of prescribed pharmaceuticals via IV drips



- Suitable for periodically scheduled financial services execution
  - LIBOR rates- based payment calculation and funds transfer

- Distributed system intelligence ⇒ autonomous decision-making for access control
- Can split attribute proof-of-possession from enrollment private key usage

CRYPTO STRUCTURE

- **(A) Asymmetric crypto:** role-independent unlinkable public key expansion for transaction validation and directed data disclosure

Combined with

- **(B) Symmetric crypto**: uniquely encrypted & selectively-releasable proofs of ownership of roles/attributes

- **(A) And (B)** are incorporated into transaction certificates

- Enables: (1) controlled transaction clustering & graduated access by authorized auditors, and (2) Recovery by transaction certificate owners of expanded private keys

COUNTERMEASURES

Algorithm-level Countermeasures

- Randomness (masking / blinding)
- Constant Time implementations
- Pre-computations and Leak Reduction
- Noise based countermeasures
- Increase dependencies on Boolean ops (e.g. keccak)
- Randomize in-algorithm structures between rounds

PROTOCOL LEVEL COUNTERMEASURES

Protocol-level Countermeasures:

- Reduce the amount of leakage to less than the minimum required for key(s) recovery using SPA / DPA / EM-based leakage
- Reduce interim states that could lead to leakage
- Key Agility (per session / per call / per message)
- Layered Security
- Increased Overall bit level security
- Redundant crypto operations to reduce leakage and temp values
- Smart choice of the cryptosystem

THANK YOU

DARKMATTER