Blockchain for Internet of Things Security and Privacy

Prof Raja Jurdak
Senior Principal Research Scientist
Research Group Leader, Distributed Sensing Systems

www.data61.csiro.au
Distributed Sensing Systems Group

- 45 researchers, postdocs, engineers, and students
IoT security and privacy is challenging
IoT Privacy and Security Challenges

• Heterogeneity in device resources
• Multiple attack surfaces
• Centralization
• Scale
• Context specific risks
• Poor implementation of security/privacy mechanisms in off-the-shelf products
IoT Privacy and Security Challenges

- Heterogeneity in device resources
- Multiple attack surfaces
- Centralization
- Scale
- Context specific risks
- Poor implementation of security/privacy mechanisms in off-the-shelf products

Blockchain for Internet of Things Security and Privacy

a possible solution
Blockchain Features

- A distributed *immutable* time-stamped ledger
- Creates a *secure* network over untrusted users
- Changeable PKs as users identity introduce high level *privacy*
- Demands for solving a puzzle to append blocks to the BlockChain (mining)
## Blockchain challenges in IoT

<table>
<thead>
<tr>
<th>BlockChain</th>
<th>IoT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Consuming</td>
<td>Mostly devices are resource restricted</td>
</tr>
<tr>
<td>Block mining is time consuming</td>
<td>Demands low latency</td>
</tr>
<tr>
<td>BlockChain scale poorly with large networks</td>
<td>IoT is expected to contain a large number of nodes</td>
</tr>
<tr>
<td>BlockChain has high bandwidth consumption</td>
<td>IoT devices have limited bandwidth and resources</td>
</tr>
</tbody>
</table>
Blockchain for IoT

- **Hierarchical structure:** resource optimization, scalability
- **Limited nodes process BlockChain:** processing overhead

Dorri, Kanhere, Jurdak, IOTDI, 2017
Blockchain for IoT Features

Data and transactions flow separation: decrease delay, resource optimization

Reduce processing: Distributed trust between CHs

Two tiers of BlockChain: linked for further applications
Smart Home Transactions

Indirectly accessible IoT devices: security, resource optimization

Dorri, Kanhere, Jurdak, Percom, 2017
Transactions handling
Transactions handling

Cloud Storage

Transaction to be stored

CHs

LBM

Data to be stored

Smart home thermostat

Requester

Local Storage

Authorization

Store data

Policy Checking

Local IL

Policy

Previous T

Next T

T(A)

T(B)

T(C)

T(Policy)

T(A)

T(B)

SenSig

RecSig

Transactions handling

Blockchain for Internet of Things Security and Privacy

Raja Jurdak
Comparison with Classical Blockchain

Our BlockChain Vs Bitcoin BlockChain

<table>
<thead>
<tr>
<th>Feature</th>
<th>Bitcoin BlockChain</th>
<th>Immutable Ledger</th>
<th>Public BlockChain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mining requirement</td>
<td>POW</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Forking</td>
<td>Not allowed</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Double spending</td>
<td>Not acceptable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Encryption</td>
<td>Asymmetric</td>
<td>Symmetric</td>
<td>Asymmetric</td>
</tr>
<tr>
<td>BlockChain visibility</td>
<td>Public</td>
<td>Private</td>
<td>Public</td>
</tr>
<tr>
<td>Transaction dissemination</td>
<td>Broadcast</td>
<td>Unicast</td>
<td>Unicast/Multicast</td>
</tr>
</tbody>
</table>
Security and privacy analysis

Accessibility threats

- **DDOS attack**
  - Devices are not directly accessible
  - Home manager controls all incoming and outgoing transactions
  - Keylists on CHs
  - Target threshold of received transactions
Security and privacy analysis

Accessibility threats

Dropping attack

Appending attack
Security and privacy analysis

Anonymity threats

• Linking attack

Video Intercom: PK = ksnaig1203ac
Smart phone Location: PK = ksnaig1203ac
Social Media

"ksnaig1203ac" is Alice!!!
Performance evaluation

We conduct simulation using NS3 to study the trust method

50 nodes in which 13 are CHs
Other IoT Applications

- Future connected and autonomous vehicles
- Smart grids
- ...

• Blockchain architecture for IoT security and privacy
• Maintains blockchain benefits with lightweight design
• Uses distributed trust to reduce block validation load
• Broadly applicable to other IoT applications

• Future work
  • Implement and evaluate architecture empirically
  • Methods for further scalability across network size and duration
Thank you

Raja Jurdak, PhD
Senior Principal Research Scientist
& Research Group Leader, Distributed Sensing Systems
Cyberphysical Systems Program

t  +61 7 3327 4355
e  raja.jurdak@csiro.au
w  http://research.csiro.au/dss

www.data61.csiro.au
References


Our other publications