Blockchain for Cyber-Physical Systems

Sabah Suhail

University of Tartu
Information Security Research Group

September 29, 2021
Outline

1 Introduction
   - IoT Challenges
   - Role of blockchain-based technology for IoT

2 Blockchain-based architectures for solving IoT challenges
   - Types of blockchains: Access Mechanism
   - Types of blockchains: Control Mechanism
   - Types of blockchains: Structure
   - Consensus Mechanisms
   - Architectures for IoT

3 Blockchain-based IoT Application
   - Examples
     - Supply Chain
     - Digital Twins

4 Open Issues
Table of Contents

1 Introduction
   • IoT Challenges
   • Role of blockchain-based technology for IoT

2 Blockchain-based architectures for solving IoT challenges
   • Types of blockchains: Access Mechanism
   • Types of blockchains: Control Mechanism
   • Types of blockchains: Structure
   • Consensus Mechanisms
   • Architectures for IoT

3 Blockchain-based IoT Application
   • Examples
     • Supply Chain
     • Digital Twins

4 Open Issues
Introduction

Figure: CPSs: Connecting physical and digital worlds
IoT Challenges

- Centralized security
- Communication architectures
- Resource constraints
- User privacy
Role of blockchain-based technology for IoT

- Distributed architecture
- Tamper-proof recording
- Transparency
- Trustless consensus
- Privacy
- Smart contracts
Summary

Blockchain for IoT

- Distributed architecture
- Tamper-proof recording
- Secure Data
- Traceability
- Transparency
- Trustless consensus
- Access Privileges
- Privacy
- Smart contracts
- Privacy
Table of Contents

1 Introduction
   ■ IoT Challenges
   ■ Role of blockchain-based technology for IoT

2 Blockchain-based architectures for solving IoT challenges
   ■ Types of blockchains: Access Mechanism
   ■ Types of blockchains: Control Mechanism
   ■ Types of blockchains: Structure
   ■ Consensus Mechanisms
   ■ Architectures for IoT

3 Blockchain-based IoT Application
   ■ Examples
     ■ Supply Chain
     ■ Digital Twins

4 Open Issues
## Types of blockchains: Access Mechanism

<table>
<thead>
<tr>
<th></th>
<th>Public</th>
<th>Private</th>
<th>Consortium</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Structure</strong></td>
<td>Decentralized</td>
<td>Centralized</td>
<td>Partially decentralized</td>
</tr>
<tr>
<td><strong>Governed by</strong></td>
<td>All</td>
<td>Trusted entity</td>
<td>Predefined group</td>
</tr>
<tr>
<td><strong>Efficiency</strong></td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Higher</td>
<td>Lower</td>
<td>Average</td>
</tr>
<tr>
<td><strong>Privacy</strong></td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
</tr>
</tbody>
</table>

## Types of blockchains: Control Mechanism

<table>
<thead>
<tr>
<th></th>
<th>Permissionless</th>
<th>Permissioned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>Write</td>
<td>Join</td>
</tr>
<tr>
<td>Public</td>
<td>Any</td>
<td>Any Authorized</td>
</tr>
<tr>
<td>Public</td>
<td>Any</td>
<td>Authorized</td>
</tr>
<tr>
<td>Private</td>
<td>Authorized</td>
<td>Operator</td>
</tr>
<tr>
<td>Private</td>
<td>Authorized</td>
<td>Authorized</td>
</tr>
<tr>
<td>Consortium</td>
<td>Authorized</td>
<td>Validators</td>
</tr>
<tr>
<td>Consortium</td>
<td>Authorized</td>
<td>Authorized</td>
</tr>
</tbody>
</table>

Types of blockchains: Structure (1/2)

Chain-structured blockchains

DAG-structured blockchains (Scalability, Quantum-Resistant, No miners)

Figure: Tangle (Source [7]).

Suggested Reading [4]
Video link: How IOTA works?
### Types of blockchains: Structure (2/2)

<table>
<thead>
<tr>
<th></th>
<th>Chain-structured Blockchain</th>
<th>DAG-structured Blockchain</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Structure</strong></td>
<td>Linked list</td>
<td>Single transaction</td>
</tr>
<tr>
<td><strong>Consensus</strong></td>
<td>PoW, PoS</td>
<td>PoW</td>
</tr>
<tr>
<td><strong>Transaction</strong></td>
<td>Transactions as grouped blocks</td>
<td>Single transaction</td>
</tr>
<tr>
<td><strong>Scalability</strong></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Transaction Fee</strong></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Mining</strong></td>
<td>Involve miners</td>
<td>No miners</td>
</tr>
<tr>
<td><strong>Maturity</strong></td>
<td>Well-established</td>
<td>Experimental</td>
</tr>
<tr>
<td><strong>Quantum Resistant</strong></td>
<td>Not immune to quantum attacks</td>
<td>Use quantum-resistant cryptographic algorithms</td>
</tr>
<tr>
<td><strong>Platforms</strong></td>
<td>Ethereum, Hyperledger</td>
<td>IOTA, Byteball</td>
</tr>
</tbody>
</table>

**Review:** What are the Pros and Cons of chain- and DAG-structured blockchains?

---

1. Improved Scalability: increased block size, sharding, off-chain channels
Question

How the scalability problem associated with the chain-structured blockchains can reduce the adaptability of blockchain technologies for IoT applications?
Answer: Quiz

- Append-only ledger: blocks \(\uparrow\), \(\rightarrow\) size of blockchain at full nodes.
- \(\uparrow\) size of blockchain \(\rightarrow\) more resources
- Resource demand \(\uparrow\), \(\rightarrow\) nodes in consensus mechanism \(\downarrow\)
- **Result**: \(\uparrow\) blockchain size, \(\rightarrow\) centralized with only few nodes fully participating in the distributed consensus.
Consensus Mechanisms

- **Proof of Work (PoW)**
  - Few messages exchanged to achieve consensus
  - High energy and computing consumption

- **Proof of Stake (PoS)**
  - Scalable and consume low power
  - Easy to monopolize, threat to security

- **Practical Byzantine Fault Tolerance (pBFT)**
  - Less hardware/energy requirements
  - Not scalable
Architectures for IoT (1/4)

- Distributed architecture
- Hierarchical architecture
- Blockchain-as-a-service architecture
Distributed architecture

- Maximize trust
- DoS attacks, bandwidth overhead, less scalable
Hierarchical architecture

- Reduce traffic
- Eclipse attacks
Blockchain-as-a-service architecture

- Reduce hardware requirements
- Centralized trust
Summary

- Types of blockchain
  - Access Mechanism
  - Control Mechanism
  - Structure

- Consensus Mechanism
  - PoW, PoS, pBFT

- Architectures for IoT
  - Distributed architecture
  - Hierarchical architecture
  - Blockchain-as-a-service architecture
# Table of Contents

1. Introduction
   - IoT Challenges
   - Role of blockchain-based technology for IoT

2. Blockchain-based architectures for solving IoT challenges
   - Types of blockchains: Access Mechanism
   - Types of blockchains: Control Mechanism
   - Types of blockchains: Structure
   - Consensus Mechanisms
   - Architectures for IoT

3. Blockchain-based IoT Application
   - Examples
     - Supply Chain
     - Digital Twins

4. Open Issues
IoT Applications

- Control Unit
- Task offloading
- Delivering results
- Sensor node
- Gateway node
- UAV
- Smart Factory
- Industrial IoT
- Nuclear Reactor
- Control Unit
- Sensor node
- Gateway node
- Digital Twins
- Physical Entity
- Virtual Entity
- Connections
- Renewable Resources
- Grid Station
- Microgrid
- Smart Grid
- Consumers having smart meters
Figure: Supply chain (Source [7]).
1. How to resolve data silos issues?

- limited view of data
- threaten data integrity
- waste of resources
2. How to resolve **counterfeiting** issues in supply chain?

- Selling counterfeit ICs for military and commercial uses
- Coronavirus fuels a surge in fake medicines
- Horse-meat scandal

**Figure:** Product story (Source: [5]).
3 How to ensure confidential trade flows among competitors?

Video link: Why Apple needs Samsung?
How to ensure dissemination of **trustworthy data**?

⭐ **GIGO**\(^2\) Problem

---

2\(^{nd}\) Garbage-In Garbage-Out
Summary: Challenges in Supply Chain

Challenges

Data Management
- Disparate Data Sources
- Data Traceability
- Data Availability
- Fault Tolerance

Data Security
- Data Confidentiality
- Data Integrity
- Data Access Control
- Quantum Immunity

Others
- Scalability
- Automation

Figure: Source: [5]
How to solve

- infrastructure-related issues
- data management-related issues
- security-related issues

Solution: Blockchain
Blockchain-based Supply Chain (1/3)

- **Data silos:**
  - Distributed data

- **Counterfeiting issue:**
  - Data traceability through provenance-enabled blockchain

- **Confidential trade flows:**
  - Data accessibility and auditability based on roles / access levels
  - NFTs for use of IP assets

- **Trustworthy data sources:**
  - collect data from registered devices
  - cross-validate device data under predefined threshold settings
  - ensure freshness of data
  - aging management
  - firmware updates
Blockchain-based Supply Chain (2/3)

Figure: Trade event between seller-buyer [7].

Suggested reading: Hyperledger Sawtooth Lake
Blockchain-based Supply Chain (3/3)

Figure: Trade event between seller-buyer (Source: [7]).
Digital Twins

What are Digital Twins and how they operate?

[Diagram showing a physical entity, virtual entity, data connections, and data inconsistencies]

Figure: Building Digital Twins: A simple illustration (Source: [9]).

Suggested reading: What are DTs? [1, 10]
Gartner Hype Cycle for Emerging Technologies
Do we really need *blockchain*? 3

What should be stored on blockchain?

- critical data
- sources that can provide *track & trace*
- separating *dynamic* & *static* data

What are the design solutions for blockchain?

---

3 Suggested reading [6, 12, 11].
Blockchain-based Digital Twins

Figure: Source: [9]

GitHub link: More on Blockchain-based Digital Twins...
Table of Contents

1 Introduction
   ■ IoT Challenges
   ■ Role of blockchain-based technology for IoT

2 Blockchain-based architectures for solving IoT challenges
   ■ Types of blockchains: Access Mechanism
   ■ Types of blockchains: Control Mechanism
   ■ Types of blockchains: Structure
   ■ Consensus Mechanisms
   ■ Architectures for IoT

3 Blockchain-based IoT Application
   ■ Examples
     ■ Supply Chain
     ■ Digital Twins

4 Open Issues
Open Issues

- Lightweight Consensus Mechanisms
- IoT security & privacy
- Scalability
- Immutable vs. mutable chains
- Interoperability
- Trust management
Lightweight Consensus Mechanisms

- **Problems:**
  - Resource consumption
  - Limited throughput
  - Delay
Security & Privacy

- Eclipse attack (enables double spending and selfish mining)
- Sybil attack (network layer)
- Selfish mining (exploits blockchain fork algorithm)
- Wallet threats (vulnerable signatures, hash collision, and flawed key generation)
- Double spending (consensus, data, and application layers)
- 51% attack (consensus and data layer)
- Deanonymization
Problem: Trade-off between scalability and decentralization
Problem: User Privacy: How to exercise "Right to be forgotten"?
Interoperability

- **Problem**: How to enable blockchains to communicate with each other?
Trust management

- True state of reality: transactions on blockchain
- View of reality: recording a sensor measurement on blockchain
  - **Problem:** GIGO

Figure: Source: [5]
Blockchain for IoT: The Good, the Bad and the Ugly

- **The Good**
  - Security: Immutability and Tamper-resistant
  - Auditability: Provenance

- **The Bad**
  - Storage
  - Non-interoperable blockchain implementations
  - Skepticism in Blockchain Technology

- **The Ugly**
  - Data & Privacy risks
  - Quantum computers put blockchain security at risk
  - Resource consuming blockchain for resource-constrained IoT

---

4 [8, 3]
Consider a bottle filling plant with multiple participating entities (sensors, actuators, equipment, human resources) and activities (trade events, work in process). To procure distributed and secure data across multiple participating entities, we have to propose a blockchain-based framework. For the given IIoT scenario, how we can address the following issues?
Questions

• Which type of IoT architecture and blockchain type could be suitable for the given scenario? Give reasoning to support your opinion.

• Suppose an insider attacker attempts to manipulate the liquid level sensor measurements in order to trick the control system into filling the bottle beyond its limit. What are the possible solutions to avoid such attacks?
- IoT architecture: Gateway-based
- Blockchain type: Private (Permissioned)
- Define threshold values, deploy smart contracts
Scenario

Prior to the arrival of data at blockchain ledger, data trustworthiness can be jeopardized by tampering or due to malfunctioning of data generating sources, and/or data modification by any of the intermediate rogue participating sources. Such events may take place during supply chain processes or at manufacturing units where the malicious entities can be either external entities or authorized entities. The erroneous data may lead to the insertion of false data into the storage thereby resulting in *Garbage In Garbage Out* (GIGO) problem.

Question

Given that *blockchain do not guarantee the trustworthiness of data at the origin*, what are the possible ways to solve GIGO problem?
Assignment-II: Solution

- Collecting data only from registered devices
- Cross-validating the device data under predefined threshold settings
- Ensuring the freshness of data (AoI)
- Relying on reputation based trust mechanisms


Securing cyber-physical systems through blockchain-based digital twins and threat intelligence, 2021.

Digital twin in industry: State-of-the-art.

Do you need a blockchain?
In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 45–54, Zug, Switzerland, jun 2018. IEEE.

Blockchain for digital twins: Recent advances and future research challenges.
Thank You!

Q & A

Contact:
raimundas.matulevicius@ut.ee
sabah.suhail@ut.ee

Thesis Topics:
★ Blockchain-based Digital Twins
★ Digital Twins for Cyber-Physical Systems Security
★ Exploiting Digital Twins to Launch Covert Attacks on Cyber-Physical Systems: An Abuse Case of Digital Twins