Blockchain-based Traceability in Agri-Food Supply Chain Management: A practical Implementation

Miguel Pincheira Caro, Muhammand Salek Ali, Massimo Vecchio and Raffaele Giaffreda
Agenda

• What is a Blockchain?
• How does it work?
• Benefits of Blockchains to the Internet of Things
• Use case: from-farm-to-fork
• The proposed architecture
• Implementations
• Performance analysis
• Conclusions
What is a Blockchain?
What is a Blockchain?

• the technology behind the Bitcoin cryptocurrency.
What is a Blockchain?

• the technology behind the Bitcoin cryptocurrency.
• immutable, time-stamped “chain of blocks”.


What is a Blockchain?

• the technology behind the Bitcoin cryptocurrency.
• immutable, time-stamped “chain of blocks”.
• smart contracts provide scripting capabilities.
What is a Blockchain?

• the technology behind the Bitcoin cryptocurrency.
• immutable, time-stamped “chain of blocks”.
• smart contracts provide scripting capabilities.
• several implementations and variations are available.
What is a Blockchain?

- the technology behind the Bitcoin cryptocurrency.
- immutable, time-stamped “chain of blocks”.
- smart contracts provide scripting capabilities.
- several implementations and variations are available.
What is a Blockchain?

- the technology behind the Bitcoin cryptocurrency.
- immutable, time-stamped “chain of blocks”.
- smart contracts provide scripting capabilities.
- several implementations and variations are available.

Is a peer to peer network, maintaining a distributed record of cryptographically signed transactions.
How does it work?
How does it work?

- A user signs a transaction and sends it to the network.
How does it work?

• A user signs a transaction and sends it to the network.
• The nodes perform basic validations (signatures, timestamp, etc.)
How does it work?

• A user signs a transaction and sends it to the network.
• The nodes perform basic validations (signatures, timestamp, etc.)
• Smart contracts perform programmed logic (validations, calculations)
How does it work?

- A user signs a transaction and sends it to the network.
- The nodes perform basic validations (signatures, timestamp, etc.)
- Smart contracts perform programmed logic (validations, calculations)
- A miner works to create a valid block for new transactions (consensus algorithm)
How does it work?

- A user signs a transaction and sends it to the network.
- The nodes perform basic validations (signatures, timestamp, etc.)
- Smart contracts perform programmed logic (validations, calculations)
- A miner works to create a valid block for new transactions (consensus algorithm)
- The new block is appended to the blockchain
What is a Blockchain?

Blockchain technology is NOT only for Fintech!!!
Benefits of Blockchains to the Internet of Things
Benefits of Blockchains to the Internet of Things

• Decentralization.
  • Peer to Peer Network.

• Transparency.
  • Immutable distributed records.

• Authenticity.
  • Cryptographically signed transactions.

• Autonomous transactions
  • Smart contracts
Use Case: “from-farm-to-fork”
Use Case: “from-farm-to-fork”

- **Actors** benefit from a **decentralized** and **trusted information** repository.
Use Case: “from-farm-to-fork”

- **Actors** benefit from a **decentralized** and **trusted information repository**.
- **IoT** devices take advantage of a **decentralized infrastructure** and provide a **cryptographically signed** representation of physical assets.
Use Case: “from-farm-to-fork”

- **Actors** benefit from a **decentralized** and **trusted information** repository.
- **IoT** devices take advantage of a **decentralized infrastructure** and provide **cryptographically signed** representation of physical assets.
- **Smart contracts** enable **autonomous transactions** (e.g., certifications for organic products, alarms in case of cold chain anomalies, etc.)
Use Case: “from-farm-to-fork”

- **Actors** benefit from a **decentralized and trusted information repository**.
- IoT devices take advantage of a **decentralized infrastructure** and provide **cryptographically signed** representation of physical assets.
- **Smart contracts** enable **autonomous transactions** (eg. certifications for organic products, alarms in case of cold chain anomalies, etc.)
- **Consumers** benefit from an **immutable, transparent history** of the product.
AgriBlockIoT - 3 Layer Architecture
AgriBlockIoT - 3 Layer Architecture

**API:** Provides a high level interface for devices and users
AgriBlockIoT - 3 Layer Architecture

**API:** Provides a high level interface for devices and users

**Blockchain:** smart contracts implementing the business logic for autonomous events
**AgriBlockIoT - 3 Layer Architecture**

**API:** Provides a high level interface for devices and users

**Controller:** Transform all the high level calls to blockchain transactions

**Blockchain:** Smart contracts implementing the business logic for autonomous events
AgriBlockIoT - 3 Layer Architecture

**API:** Provides a high level interface for devices and users

**Controller:** Transform all the high level calls to blockchain transactions

**Blockchain:** smart contracts implementing the business logic for autonomous events

Edge devices may be also nodes on the peer to peer network and not just clients
Implementations


- “Traditional” blockchain
- Focused on improving Bitcoin’s smart contract capabilities
- Available since 2013
- Maintained by Ethereum Foundation
- The transaction is a fixed structure
- Storage on LevelDB
Implementations

“Traditional” blockchain
- Focused on improving Bitcoin’s smart contract capabilities
- Available since 2013
- Maintained by Ethereum Foundation
- The transaction is a fixed structure
- Storage on LevelDB

“Modular” Blockchain
- Focused on “Enterprise Level” blockchain.
- Version 1.0 avail. 01/2018
- Maintained by Linux Foundation, created by Intel
- Transactions can be forged by users
- Storage using LMDB
A digital sensor updates its state on the blockchain through a smart-contract.
Performance analysis: metrics

A digital sensor updates its state on the blockchain through a smart-contract

- Tested 100 times for each implementation (ETH and HL)
- Measured metrics:
  - Latency (Time to update the value on the network)
  - Network Traffic (transmitted and received)
  - CPU Load/Usage
Preliminary results: comparison

**Performance of AgriBlockIoT in terms of latency, network traffic, and CPU load.**

<table>
<thead>
<tr>
<th></th>
<th>latency [seconds]</th>
<th>network tx [bytes]</th>
<th>network rx [bytes]</th>
<th>CPU load [%]</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟦 Ethereum</td>
<td>16.55</td>
<td>528’108</td>
<td>682’415</td>
<td>46.78</td>
</tr>
<tr>
<td>🟨 Sawtooth</td>
<td>0.021</td>
<td>19’303</td>
<td>20’641</td>
<td>6.75</td>
</tr>
</tbody>
</table>
Preliminary results: comparison

**Performance of AgriBlockIoT in terms of latency, network traffic, and CPU load.**

<table>
<thead>
<tr>
<th></th>
<th>latency [seconds]</th>
<th>network tx [bytes]</th>
<th>network rx [bytes]</th>
<th>CPU load [%]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethereum</td>
<td>16.55</td>
<td>528’108</td>
<td>682’415</td>
<td>46.78</td>
</tr>
<tr>
<td>Sawtooth</td>
<td>0.021</td>
<td>19’303</td>
<td>20’641</td>
<td>6.75</td>
</tr>
</tbody>
</table>

- More mature platform
- Blocks are made even without transactions
- **Better consistency**
- Focused on a public, permissionless blockchain
- **Existing public network with cryptocurrency**
## Preliminary results: comparison

**Performance of AgriBlockIoT in terms of latency, network traffic, and CPU load.**

<table>
<thead>
<tr>
<th></th>
<th>latency [seconds]</th>
<th>network tx [bytes]</th>
<th>network rx [bytes]</th>
<th>CPU load [%]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethereum</td>
<td>16.55</td>
<td>528’108</td>
<td>682’415</td>
<td>46.78</td>
</tr>
<tr>
<td>Sawtooth</td>
<td>0.021</td>
<td>19’303</td>
<td>20’641</td>
<td>6.75</td>
</tr>
</tbody>
</table>

- More mature platform
- Blocks are made even without transactions
- **Better consistency**
- Focused on a public, permissionless blockchain
- **Existing public network with cryptocurrency**

- More modular platform
- Blocks are made only when transactions arrive
- **Faster response**
- Adaptable to any type of blockchain (i.e. permissioned)
- **User most deploy network with customs transactions**
Preliminary results: comparison

**Performance of AgriBlockIoT in terms of latency, network traffic, and CPU load.**

<table>
<thead>
<tr>
<th></th>
<th>latency [seconds]</th>
<th>network tx [bytes]</th>
<th>network rx [bytes]</th>
<th>CPU load [%]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethereum</td>
<td>16.55</td>
<td>528’108</td>
<td>682’415</td>
<td>46.78</td>
</tr>
<tr>
<td>Sawtooth</td>
<td>0.021</td>
<td>19’303</td>
<td>20’641</td>
<td>6.75</td>
</tr>
</tbody>
</table>

- More mature platform
- Blocks are made even without transactions
- **Better consistency**
- Focused on a public, permissionless blockchain
- Existing public network with cryptocurrency
- More modular platform
- Blocks are made only when transactions arrive
- **Faster response**
- Adaptable to any type of blockchain (i.e. permissioned)
- User most deploy network with customs transactions
Preliminary results: comparison

Performance of AgriBlockIoT in terms of latency, network traffic, and CPU load.

<table>
<thead>
<tr>
<th></th>
<th>latency [seconds]</th>
<th>network tx [bytes]</th>
<th>network rx [bytes]</th>
<th>CPU load [%]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethereum</td>
<td>16.55</td>
<td>528’108</td>
<td>682’415</td>
<td>46.78</td>
</tr>
<tr>
<td>Sawtooth</td>
<td>0.021</td>
<td>19’303</td>
<td>20’641</td>
<td>6.75</td>
</tr>
</tbody>
</table>

- More mature platform
- Blocks are made even without transactions
- Better consistency
- Focused on a public, permissionless blockchain
- Existing public network with cryptocurrency

- More modular platform
- Blocks are made only when transactions arrive
- Faster response
- Adaptable to any type of blockchain (i.e. permissioned)
- User most deploy network with customs transactions
Conclusions
Conclusions

• Our architecture enables seamless integration of IoT devices into publicly available Blockchain implementations.
Conclusions

• Our architecture enables seamless integration of IoT devices into publicly available Blockchain implementations.

• Devices can be full fledged users of the blockchain, while smart contracts provides autonomous transaction executions.
Conclusions

• Our architecture enables seamless integration of IoT devices into publicly available Blockchain implementations.

• Devices can be full fledged users of the blockchain, while smart contracts provides autonomous transaction executions.

• Different Blockchain implementations provides different functional and non functional features.
  • Faster response time \textit{vs} Better consistency
  • Existing cryptocurrency \textit{vs} User defined transactions
  • Cost of use \textit{vs} Cost of deployment
Conclusions

• Our architecture enables seamless integration of IoT devices into publicly available Blockchain implementations.

• Devices can be full fledged users of the blockchain, while smart contracts provides autonomous transaction executions.

• Different Blockchain implementations provides different functional and non functional features.
  • Faster response time vs Better consistency
  • Existing cryptocurrency vs User defined transactions
  • Cost of use vs Cost of deployment
Conclusions

• Our architecture enables seamless integration of IoT devices into publicly available Blockchain implementations.

• Devices can be full fledged users of the blockchain, while smart contracts provides autonomous transaction executions.

• Different Blockchain implementations provides different functional and non functional features.
  • Faster response time vs Better consistency
  • Existing cryptocurrency vs User defined transactions
  • Cost of use vs Cost of deployment

We plan to extend the performance analysis to more constrained hardware architectures and also to include other blockchain implementations into our reference architecture.
thank you.

Miguel Pincheira Caro
mpincheiracaro@fbk.eu
PhD Candidate
OpenIoT Research Unit FBK CREATE-NET
University of Trento