Transparency, Trustworthy and Privacy-Preserving Supply Chains

Salil Kanhere
School of Computer Science and Engineering
UNSW Sydney, Australia
E: salil.kanhere@unsw.edu.au
W: www.salilkanhere.net

Collaborators: Sidra Malik (UNSW), Raja Jurdak (QUT), Volkan Dedeoglu (CSIRO’s Data61) and Naman Gupta (IIT Delhi)
Supply Chain Lifecycle

A system of organizations, people activities, involved in the distribution of raw material or finished goods

- Food
- Pharmaceutical
- Aerospace and Defense
- Practically any consumer goods
Supply Chain and Digitisation

- Efficiency gains
- Boosted revenue
- Improve productivity
- Traceability and transparency?
Traceability

Counterfeiting

Needles in Strawberries

Two dead from listeria linked to smoked salmon

Contaminated smoked salmon from Tasmania is the likely cause of two fatal listeriosis cases in New South Wales and Victoria.
Current Traceability Systems

- Siloed
- Centralized
- Unreliability of Data
- Consumer Access
BLOCKCHAIN IS THE ANSWER
What is Blockchain?

1. Someone requests a transaction
2. The requested transaction is broadcast to a P2P network consisting of computers, known as nodes
3. The network of nodes validate the transaction using cryptography.
4. Once verified, this transaction is represented as a new block.
5. The new block is then added to the existing blockchain.
6. The transaction is complete
### Permissionless

<table>
<thead>
<tr>
<th>Public</th>
<th>Anonymous users</th>
<th>Slow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examples: Bitcoin, Ethereum, NEM, IOTA</td>
<td>Examples: Bitcoin, Ethereum, NEM, IOTA</td>
<td>Examples: Bitcoin, Ethereum, NEM, IOTA</td>
</tr>
</tbody>
</table>

### Permissioned

<table>
<thead>
<tr>
<th>Private / Consortium / Public</th>
<th>Identified users</th>
<th>Fast</th>
</tr>
</thead>
<tbody>
<tr>
<td>PBFT, RAFT, PoET</td>
<td>PBFT, RAFT, PoET</td>
<td>PBFT, RAFT, PoET</td>
</tr>
</tbody>
</table>

Examples: Hyperledger, R3 (Corda), Ripple, Quorum
Smart Contracts

How Smart Contracts Work

**STEP 1**
An option contract is written as code into a blockchain.

**STEP 2**
An event (delivery of goods, an expiration date, etc.) triggers the execution of the coded terms of the contract.

**STEP 3**
Assets are released to the necessary parties.

**STEP 4**
Regulators can study the immutable transaction record to understand all activity that has taken place.
Benefits of Blockchain

• Tamper-proof storage of information

• Auditability/Transparency

• No reliance on third-parties

• Distributed trust

• Cryptographically secure

• Smart contracts can automate numerous processes
How can blockchain benefit supply chains?

- **False-labeling**
- **Mishandling**
- **Ensure data has not been changed**

**Traceability**
- Financial aspects b/w the seller and buyer
- Cross border trade
- Smart Contract based automation

- By food authority
- Ensure compliance with food safety/quality

**Trade Finance**

**Blockchain**

**Data Analysis**
- IoT in monitoring crop data
- Analysis of collected data
- Smart contract - trade flows, recall management etc.

**Insurance**
- Benefits in case of loss
- Farmer and insurer data
- BC ensures immutability
- Automated payments

**Audit**
- Periodic reports, automation
Generic Architecture
Challenges and Solutions

Challenges

- Instant availability of data
- Data prone to modification
- Access rules to write/retrieve data on blockchain
- Blockchain mechanisms cannot ensure data authenticity which is not generated on-chain
- Growing scale of national and global trade vs. blockchain resources
- Traceability and provenance data may reveal trade secrets to blockchain consortium and validators

Solutions

Traceability/Access
- ProductChain (2018)

Trustworthy Data

Scalability
- TreeChain (2020)

Privacy
- PrivChain (2021), TradeChain (2021)
ProductChain: Scalable Blockchain Framework to Support Provenance in Supply Chains

Sidra Malik  
*School of Computer Science and Engineering*  
*The University of New South Wales*  
Sydney, Australia  
sidra.malik@unsw.edu.au

Salil S. Kanhere  
*School of Computer Science and Engineering*  
*The University of New South Wales*  
Sydney, Australia  
salil.kanhere@unsw.edu.au

Raja Jurdak  
*Data61, CSIRO*  
Brisbane, Australia  
raja.jurdak@csiro.au

*Published in: 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*

**Date of Conference:** 1-3 Nov. 2018  
**INSPEC Accession Number:** 18290154

**Date Added to IEEE Xplore:** 29 November 2018  
**DOI:** 10.1109/NCA.2018.8548322

**ISBN Information:**  
**Publisher:** IEEE  
**Conference Location:** Cambridge, MA, USA
ProductChain - Contributions

- Holistic approach, **Consortium** to manage a **permissioned blockchain**

- **Transaction Vocabulary**
  - Integration of IoT data from embedded sensors
  - Improved writing accessibility to the ledger
  - Each Food Supply Chain (FSC) participant has a well-defined role

- **Scalable Network Architecture**
  - Use Sharding

- **Access Control List**
  - Hide trade flows, limit read/write access to ledger
ProductChain: Consortium
## ProductChain: Access Control

<table>
<thead>
<tr>
<th>Members</th>
<th>Transaction Type</th>
<th>Global ledger at BCglob</th>
<th>Local Ledger</th>
<th>Modify Access Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Participating</td>
<td>Create</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Transfer</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>produce</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Participating</td>
<td>Create</td>
<td>x</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Transfer</td>
<td>x</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>produce</td>
<td>x</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Governance Board</td>
<td>Create</td>
<td>x</td>
<td>x</td>
<td>✓ By majority vote</td>
</tr>
<tr>
<td></td>
<td>Transfer</td>
<td>x</td>
<td>x</td>
<td>✓ By majority vote</td>
</tr>
<tr>
<td></td>
<td>produce</td>
<td>x</td>
<td>x</td>
<td>✓ By majority vote</td>
</tr>
<tr>
<td>Validators</td>
<td>Create</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Transfer</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>produce</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
</tr>
</tbody>
</table>
ProductChain: Network Architecture
ProductChain: Transaction Vocabulary

Create Transaction, \( \{Tx\}_c \) : uni-sig

Transfer Transaction, \( \{Tx\}_tr \) : multi-sig

Produce Transaction, \( \{Tx\}_p \) : uni-sig
Trust: Challenges

• How do we trust data written into the blockchain?
  • Hashed data on the blockchain represents digital observations of physical events

• Need for a trust management system with the following requirements
  • Multi-faceted assessment of trustworthiness of logged data
  • Flexibility for ascribing trust to the supply chain entities and commodities and at different granularities
  • Automation of various processes – reputation computation, rewards, penalties
  • Minimal overheads
TrustChain: Trust Management in Blockchain and IoT supported Supply Chains

Sidra Malik, Volkan Dedeoglu, Salil S. Kanhere, and Raja Jurdak

Published in: 2019 IEEE International Conference on Blockchain (Blockchain)

Date of Conference: 14-17 July 2019
Date Added to IEEE Xplore: 02 January 2020
INSPEC Accession Number: 19246030
DOI: 10.1109/Blockchain.2019.00032
Publisher: IEEE
Conference Location: Atlanta, GA, USA, USA
TrustChain: Contributions

BC-based **reputation/trust framework**

Flexible and granular

Smart contracts for **automation**

**Accountability** mechanisms

Hyperledger Fabric **Implementation**

Minimal **overheads**
TrustChain

Data Layer

Multi-sourced Data Observations:

• Sensors
• Buyer’s Rating (in a trade event)
• Regulatory Bodies
TrustChain

Blockchain Layer

- Profiles for supply chain entities and commodities
- Reputation and Trust Module
- Smart Contracts
- ACL
- Ledger

Data Layer
- sensor data stream
- trade events
- regulatory endorsements

Supply Chain Entities
TrustChain

Blockchain Layer

Smart Contracts

Commodity Rating

Quality Contract

Rating Contract

Commodity Reputation

Participant Reputation

Commodity's Profile

Primary Producer

Primary Producer's Profile

Temperature warning

TX_sens

TX_cr

Seller

Buyer

Regulator

Regulator's Rating

Buyer's Profile

Seller's Profile

Regulator's Profile

Commodity Rating

TX_tr

Commodity Reputation
TrustChain

Reputation and Trust Model

• Commodity Reputation

\[ Rep_{sens} = [Rep_{sens}(t_0), Rep_{sens}(t_1), \ldots, Rep_{sens}(t_{n-1})] \]

• Seller’s Reputation

\[ Rep_{seller} = w_1 \times Rep_{sens}(t) + w_2 \times Rep_{trader}(t) + w_3 \times Rep_{reg}(t) \]

\[ R(t_n) = \sum_{t=t_0}^{t=t_n} Rep_{seller}(t) \times \beta(t_n - t) \]

\[ T_{trader}(t_n) = \alpha_0 \cdot R(t_n) + \alpha_1 \cdot f_1 + \alpha_2 \cdot f_2 + \ldots + \alpha_N \cdot f_N \]

### Trust Feature and Feature Score

<table>
<thead>
<tr>
<th>Number of Successful Transactions</th>
<th>Feature Score ( (f_1) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>1-3</td>
<td>0.5</td>
</tr>
<tr>
<td>4-6</td>
<td>1.5</td>
</tr>
<tr>
<td>&gt;= 6</td>
<td>2</td>
</tr>
</tbody>
</table>
TrustChain

Application Layer

- Profiles for supply chain entities and commodities
- Reputation and Trust Module
- Smart Contracts
- ACL
- Ledger

Data Layer
- Sensor data stream
- Trade events
- Regulatory endorsements

Supply Chain Entities
TrustChain

Application Layer

Queries
• Computing trust rating for supply chain entities and reputation of commodity
• Properties of commodities and traders

Rewards
• Incentivizing honest traders

Penalties
• Penalize dishonest behaviour
PoC: Evaluations

Throughput and Latency vs. Transaction Send Rate
Privacy: Challenges

Traceability

Privacy
Privacy Preservation

Issues

Hide Identities

Hide Data
Privacy Preservation Solution

- Use multiple identities for trade
- Hide Identities
- Share Proofs on Data
- Hide Data

PrivChain

TradeChain
PrivChain: Provenance and Privacy Preservation in Blockchain enabled Supply Chains

Sidra Malik, Volkan Dedeoglu, Salil S. Kanhere, and Raja Jurdak

to appear in Proceedings of IEEE Blockchain 2022, August 2022

https://arxiv.org/abs/2104.13964
PrivChain: Key Contributions

- **Zero-Knowledge Proof (ZKP) based privacy preservation** solution where proof of provenance is provided without disclosing privacy-sensitive data

- **Automated verification** of the provenance proofs and the integration of the **incentive mechanism** that enforces instant rewards

- Proof of concept implementation with **minimal overheads** for proof verification
Basics

Zero Knowledge Proofs
• cryptographic methods in which a prover can attest to a verifier that some secret information is true without revealing any details about the secret

Pedersen Commitment
non-interactive secret sharing scheme
• a user commits to a secret
• sends a verifier a commitment to the secret without disclosing the secret itself
• secret is shared with the verifier at some later point in time
• verifier computes a new commitment from the secret and verifies it by comparing it to the previous commitment shared by the committer
PrivChain
Framework
PrivChain

Setup
PrivChain

Proof Generation

\[ TX_{cr} = \left[ ID_g \ | \ H_{data} \ | \ L_{\phi_{loc}} \ | \ Sig_s \right] \]
PrivChain
Proof verification and Incentive Payments

\[ Req_{\text{pay}} = \left[ \text{com}_{\text{inc}} | \text{Enc}(\left( \$_{\text{inc}} | r \right) | ID_{\text{sell}}), PK_{\text{bank}} \right] | \text{Sig}_{\text{buy}} \]

1. \( \phi_{\text{loc}}, \text{com}_{\text{inc}} \)
2. verify \( \phi_{\text{loc}} \)
3. issue \( Req_{\text{pay}} \)
4. retrieve \( \$_{\text{inc}}, \text{verify com}_{\text{inc}}, \text{Pay} \)

\[ TX_{\text{trade}} = \left[ ID_g | H_{\text{data}} | L_{\phi_{\text{loc}}} | \text{com}_{\text{inc}} \right.
\left. | region | \text{Sig}_s | PU_s | \text{Sig}_b | PU_b \right] \]
PrivChain
Trade Flow Protection

• The provenance of a final product: finding the origin of each ingredient using a \( TX_{\text{produce}} \)

\[
TX_{\text{produce}} = \left[ ID_{FP} | Enc((ID_{g1}, ..., ID_{gn}), Key) | [\text{regions}] | \text{Sig}_{\text{buy}} \right]
\]
PrivChain
Evaluations
TradeChain: Decoupling Traceability and Identity in Blockchain enabled Supply Chains

Sidra Malik*, Naman Gupta† Volkan Dedeoglu‡, Salil S. Kanhere*, and Raja Jurdak§
*UNSW, Sydney †IIT, Delhi ‡CSIRO Data61, Brisbane §QUT, Brisbane
{sidra.malik, salil.kanhere}@unsw.edu.au, naman.gupta1003@gmail.com, volkan.dedeoglu@data61.csiro.au, r.jurdak@qut.edu.au

http://dx.doi.org/10.1109/TrustCom53373.2021.00155
TradeChain: Key Contributions

- integrated framework for **two separate ledgers**:
  - IDML for decentralised identity management and
  - TML for recording trade events on the ledger
- supply chain entities can
  - use **ZKPs on their credentials** while trading on TML
  - define **dynamic access rules** for traceability and data collation
- A PoC implementation on **Hyperledger Indy and Fabric** to demonstrate efficacy and minimal overheads
Decentralisation of Identity Management

Decentralised, “trustless” ID Provider

- The peer-to-peer relationship secured by public/private key cryptography
- Decentralised registry that verifies the relationships
- Returning people to direct, private connections
- “Me (user)” centric

Self-Sovereign Identity (SSI)
TradeChain
Overview

A. On-Boarding & Credentialling
B. join based on ZKP
C. log trade
D. obtain access token
E. query using token
F. fetch trade info

IDML
stores identities

TML
stores trades

QSC
TML smart contract

Trader

Requester
TradeChain
Detailed Framework

Identity Management Ledger (IDML)

1: Register
2: Onboarding
4: Publish DIDs
3: Create DIDs
5: Get credentials
6: Request to join the trade ledger
12: Logs supply chain transactions

User/Trader

Steward

Trade Management Ledger (TML)

7: ZKP proof request
9: Validate
11: Allowed to transact
10: Approved request
8: Send proof
13: Get access token
14: Query with token

TML Admin

TML Smart Contract

Query Smart Contract (QSC)

15: Validate token
16: Fetch query results
17: Return results

Information requester
TradeChain
Token-based Querying
TradeChain Evaluations

Time Overheads
TradeChain
Evaluations

(a) Registering a commodity $TX_{cr}$

(b) Trading a commodity $TX_{tr}$

(c) Querying TXns based on token

(d) Querying and Returning filtered results
Future Opportunities

• Interoperability
  • need to design protocols and standards to develop an interoperability architecture among the **growing parallel solutions**
  • Various interoperability approaches can be adopted such as APIs and gateways, pub-sub models, notaries, smart contracts, etc.

• Garbage in Garbage out
  • Reputation modules are not the only option!
  • other solutions such as incorporating **smart biological fingerprints** have still not been fully explored

• Incentives
  • Mechanisms **to incentivise** famers/small-scale suppliers need to be designed
  • **Smart contracts** for actioning incentives
Future Opportunities

- **Governance**
  - some central monitoring or **governance is required for regulatory purposes**
  - need to devise a **governance framework** which allows some level of **autonomy**, but at the same time, can assist the government bodies with having an **oversight over the trade activities**

- **Sustainability**
  - Quantifying the **carbon footprint** of complex supply chains is necessary
  - Mechanisms to check if **sustainability practices** were adopted
  - Improving working/living conditions of farmers
Blockchain for Cyberphysical Systems
Ali Dorri, Salil Kanhere, Raja Jurdak
Copyright: 2020
Pages: 290
ISBN: 9781630817831
Artech House, USA/UK
PhD Opportunity @ UNSW Sydney

PhD Scholarship on Collaborative Surveillance in Security Operations
Centres @ UNSW Sydney and CSIRO’s Data61

Published on May 13, 2022

We have an opening for a PhD candidate to work on an existing project on collaborative surveillance in security operations centres.

This PhD project will conduct research on human-machine collaboration to support collaborative surveillance in Security Operations Centres (SOCs) with the aim of addressing “alert fatigue”. With cyber security risks increasing daily, security analysts at SOCs need to be effective in prioritizing alerts to ensure that critical security issues are identified and addressed promptly. However, identifying critical alerts in a SOC is a bit like looking for a needle in a haystack when it is moving at high speed. The research questions that this project will address is how the human and AI component can collaborate with each other, getting to the appropriate prioritization and action, without cognitive overload and attention loss. The AI needs to assist with the prioritization of alerts, provide rationale for the prioritization, and provide appropriate visualizations. The human expert needs to input knowledge to help with the prioritization. The resulting human-AI symbiosis will not only lead to improved SOC productivity but also ease the emotional toll on cybersecurity analysts. The developed solutions will be applicable to any application domain that has a command-and-control centre with situation awareness.

https://shorturl.at/oBCIT
W: www.salilkanhere.net
E: salil.kanhere@unsw.edu.au
www.linkedin.com/in/salilkanhere