Smart Contract

Group 6
Member:
Yousef Zare
Sara Solatani
Erfan Najafi
Sobhan Safdarian
Mohammad Esmaeil MohammadZade

Table of Contents

01 Insurance

02 Supply Chain

03 Real Estate

04 Comparison

05 Implementation

Insurance

IT Fundamentals Course
Group 6

Reference:

Gatteschi, Valentina, et al. "Blockchain and smart contracts for insurance: Is the technology mature enough?." Future internet 10.2 (2018): 20.

future internet

MDPI

Article

Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?

Valentina Gatteschi [1,*], Fabrizio Lamberti [1], Claudio Demartini [1], Chiara Pranteda [2] and Víctor Santamaría [3]

[1] Politecnico di Torino, Dipartimento di Automatica e Informatica, Corso Duca degli Abruzzi 24, 10129 Torino, Italy; fabrizio.lamberti@polito.it (F.L.), claudio.demartini@polito.it (C.D.)

[2] Reale Group Innovation Team, Via Corte d'Appello 11, 10129 Torino, Italy; chiara.pranteda@realemutua.it

[3] Reale Group Innovation Team, Príncipe de Vergara, 125, 28002 Madrid, Spain; victor.santamaria@realeites.com

[*] Correspondence: valentina.gatteschi@polito.it

Received: 30 December 2017; Accepted: 14 February 2018; Published: 20 February 2018

Abstract: Blockchain is receiving increasing attention from academy and industry, since it is considered a breakthrough technology that could bring huge benefits to many different sectors. In 2017, Gartner positioned blockchain close to the peak of inflated expectations, acknowledging the enthusiasm for this technology that is now largely discussed by media. In this scenario, the risk to adopt it in the wake of enthusiasm, without objectively judging its actual added value is rather high. Insurance is one the sectors that, among others, started to carefully investigate the possibilities of blockchain. For this specific sector, however, the hype cycle shows that the technology is still in the innovation trigger phase, meaning that the spectrum of possible applications has not been fully explored yet. Insurers, as with many other companies not necessarily active only in the financial sector, are currently requested to make a hard decision, that is, whether to adopt blockchain or not, and they will only know if they were right in 3–5 years. The objective of this paper is to support actors involved in this decision process by illustrating what a blockchain is, analyzing its advantages and disadvantages, as well as discussing several use cases taken from the insurance sector, which could easily be extended to other domains.

Keywords: blockchain; bitcoin; insurance; smart contracts

1. Introduction

A blockchain is a distributed ledger maintained by network nodes, recording transactions executed between nodes (i.e., messages sent from one node to another). Information inserted in the blockchain is public, and cannot be modified or erased [1]. Smart contracts are self-executing contracts (generally saved on a blockchain) whose terms are directly written into lines of code [2].

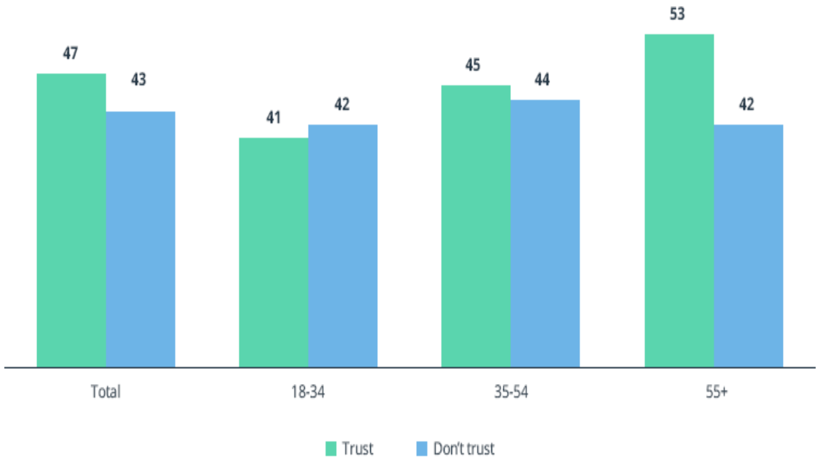
Recently, blockchain and its relations with smart contracts has received increasing attention from media, which started to address it as "The next big thing" [3], "The new black", "The philosopher's stone" [4] or "The new Graal" [5]. In [6], blockchain has been compared to inventions such as the steam or combustion engine, since it is potentially able to bring benefits to a variety of everyday activities and business processes.

According to Gartner's hype cycle, blockchain is at the peak of inflated expectations, where the enthusiasm is at the highest level possible [7]. Nonetheless, concerns started to be expressed as well about a massive adoption of blockchain [5,8–13]. The common denominator in the above concerns is that technology is considered, on the one hand, to be not fully mature yet [5,9] and, on the other hand, to be overhyped [8], since its application often produces outcomes that could be achieved using well-mastered alternatives [10].

Future Internet **2018**, *10*, 20; doi:10.3390/fi10020020 www.mdpi.com/journal/futureinternet

Purpose of using the smart contract

- The main challenge of the insurance industry is mistrust
- Only 29% of customers trust insurers



Types of blockchains

- Private blockchain
    - Decentralization
    - No central authority is available
- Public blockchain
- Consortium blockchain
    - Lower validation and shorter validation times
    - Reduce the risk of attacks
    - Increase privacy

Consortium

- The most appropriate architecture for insurance is a consortium

Blockchain

- Only a limited number of users are allowed to approve transactions
- Blockchain tracks the sender of each transaction
- Restore the status of the blockchain by controlling a small number of nodes
    - Driving violation that has been reported to the wrong person

Architecture

- Public blockchain
  - Companies that goal to provide payment services for use
  - Higher transaction costs
- Black Insurance
  - Platform based on two separate but connected blockchains
  - The public part of the system is connected with a blockchain of the Privacy Consortium
  - Combines these two models to use the best of both worlds

Smart contract applications

- Speed up processing as well as reduce costs
- More complex uses
  - Include oracles to collect real-world information
  - Oracle is the agent that obtains and validates external data and provides it to smart contracts
- Reimburse automatically
- Part of the insurance is also associated with IoT
  - Intelligent systems that use sensors in homes

Smart contract applications

- Everyone can check the smart contract
  - Comparing situations becomes easier
- Reduce additional costs by using an encryption mechanism
- Customers are identified by a unique address
  - There is no need to provide identification for the first or later contracts
  - reduces the time and cost of data collection
- Combined with the IoT process for automatic registration
  - GPS data can be used for automatic collection

Example Smart contract applications

- In case of death, the smart contract can automatically transfer the testator money through its own request which is encrypted in the blockchain
  - Put restrictions on reaching legal age
  - Oracle can be used to check death records
- Automatically calculate premium by reading all information related to a person for fraud prevention
  - Different part must work together to store each person's information
  - By reviewing and comparing data from previous claims

Advantages of using Smart Contract

- Less fraud through transparency
- Task automation
- Save time on verifying claims
- Protect policy documents
- Risk assessment

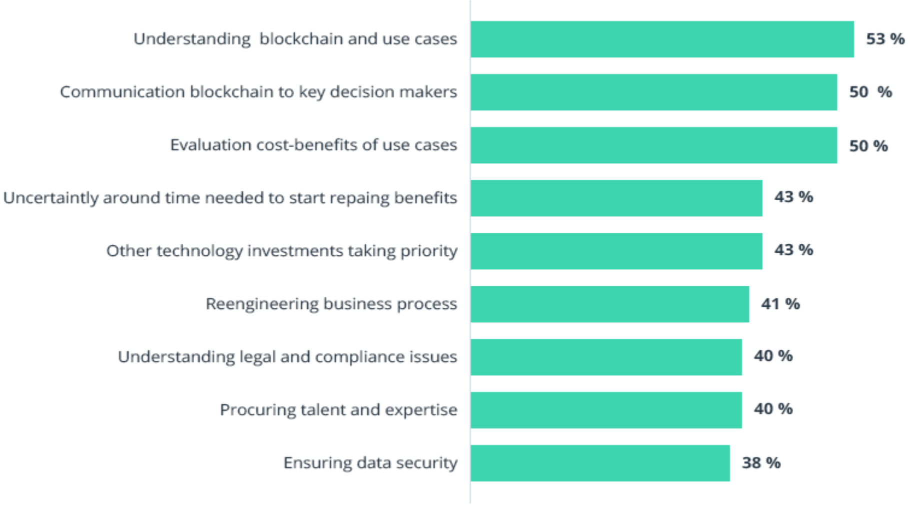
Constraints of using Smart Contract

- Completely convert to programming code
  - It can be difficult to convert code to tasks that are easily done on paper
  - Good faith , Reasonableness
- Disadvantage related to scalability is energy consumption and performance
  - Reduce the number of transactions per second compared to the traditional method
  - Space is also an issue, because data is duplicated at each network node
- Possible bugs in code

Constraints of using Smart Contract

- Uncertainty of legal regulations
- Limited contract scope

concerns that limit the popularization of smart contracts



Supply Chain

IT Fundamentals Course
Group 6

Reference:

Wang, Shangping, et al. "Smart contract-based product traceability system in the supply chain scenario." *IEEE Access* 7 (2019): 115122-115133.

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 31, 2019, accepted August 8, 2019, date of publication August 16, 2019, date of current version August 30, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2935873

Smart Contract-Based Product Traceability System in the Supply Chain Scenario

SHANGPING WANG[1], DONGYI LI[1], YALING ZHANG[2], AND JUANJUAN CHEN[1]
[1]School of Science, Xi'an University of Technology, Xi'an 710048, China
[2]School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China

Corresponding author: Dongyi Li (dyli61610@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61572019, in part by the Key Research and Development Program of Shaanxi under Grant 2019GY-028, and in part by the Start-Up Fund for Ph.D. Teachers in Xi'an University of Technology under Grant 256081502.

ABSTRACT With the improvement of living standard, people begin to pay more attention to food safety and product quality. Therefore, for consumers, it is necessary to establish a reliable system that can trace the source of products. However, most existing traceability systems tend to lack transparency, data is primarily stored within the enterprise, and the cost of tampering with data is very low. Besides, the supply chain nodes are easy to evade responsibility when product safety or quality issues arise under the traditional centralized management model, and it is difficult to trace the root of issues. The development of blockchain technology provides us with new ideas for realizing the traceability of products in supply chain scenarios. Due to its characteristics of decentralization, transparency, and immutability, blockchain can be effectively used to alleviate the above problems. In this paper, we propose a product traceability system based on blockchain technology, in which all product transferring histories are perpetually recorded in a distributed ledger by using smart contracts and a chain is formed that can trace back to the source of the products. In particular, we design an event response mechanism to verify the identities of both parties of the transaction, so that the validity of the transaction can be guaranteed. And all events are permanently stored in the form of logs as a basis for handling disputes and tracking responsible entities. Furthermore, a system prototype is constructed based on the testing framework of Truffle. The contract code is deployed on a test network TestRpc that runs in local memory, and a decentralized web page interface is implemented based on the prototype. Finally, the system security analysis and experimental results show that our solution is feasible.

INDEX TERMS Blockchain, smart contract, supply chain, traceability, accountability.

I. INTRODUCTION

The supply chain is a net-chain structure formed by independent or semi-independent economic entities in the process of product manufacturing and trading. It widely exists in many fields such as manufacturing industry, service industry, high-tech industry, and so on. The supply chain connects multiple entities such as suppliers, manufacturers, distributors, retailers, and customers. Complex supply chains can go through hundreds of stages, span months or even longer, and involve multiple regions around the world. In this scenario, it is difficult to find the root of the issue when the product has safety or quality problems because the supply chain involves a large number of entities. Especially in the food supply chain, ensuring food safety and traceability of sources can increase consumer trust. And for consumers, the government agencies or authorities need to respond more promptly and accurately to food scandals and accidents [1]. What's more, the quality, integrity, and availability of the product are critical for consumers, and product traceability ensures a high level of product [2]. At present, relevant departments and consumers in many countries advocate the traceability of the food supply chain, and have begun to improve the corresponding laws and regulations. For example, Canada enforces the use of bar codes, plastic hanging ear tags, or two electronic button ear tags to identify the initial herd. The National Livestock Identification System (NLIS) is Australia's permanent livestock identity system that tracks the entire process from birth to slaughter. It can be seen that the establishment and improvement of the traceability system is very necessary.

The supply chain is more emphasis on how to guarantee the long-term preservation and searchability of information,

The associate editor coordinating the review of this article and approving it for publication was Aniello Castiglione.

Introduction

- The supply chain is a net-chain structure formed by independent or semi-independent economic entities in the process of product manufacturing and trading
    - National Livestock Identification System
- It is difficult to find the root of the issue when the product has safety or quality problems
    - Especially in the food supply chain, ensuring food safety and traceability of sources can increase consumer trust

Traditional Supply Chain

- The data is mostly recorded by each enterprise in a centralized ledger that is stored locally
    - It may be falsified privately
- Inconsistency between nodes data due to the fact that data has likely been tampered

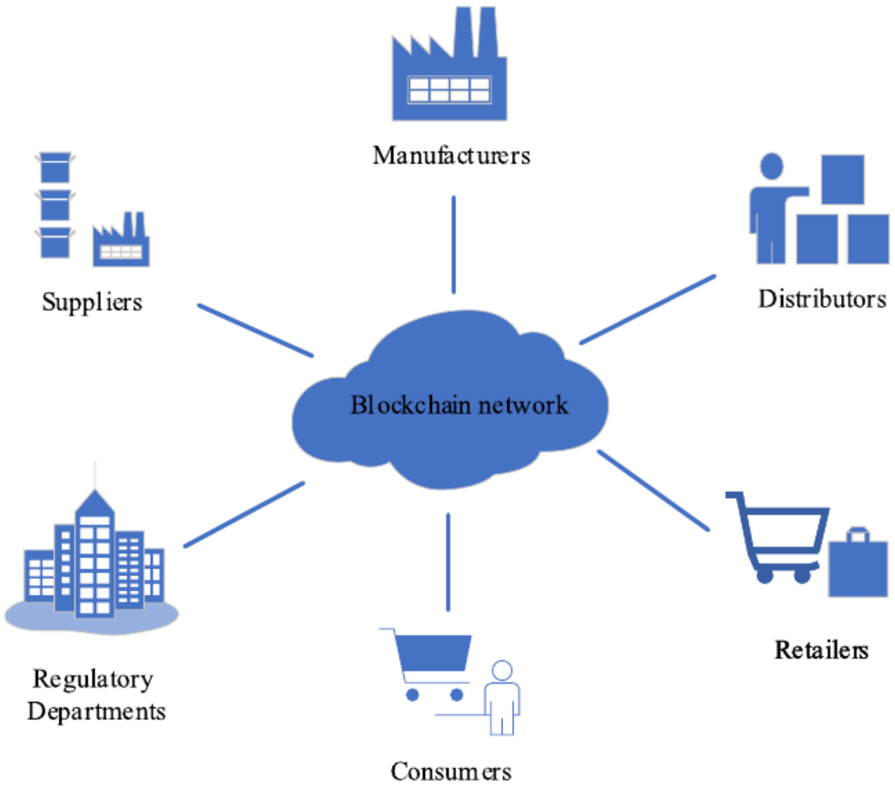
Challenges Solved by the System

- Product traceability process is easily interrupted and accountability is hard to achieve
  - Decentralized product traceability system based on blockchain technology
- The nodes in the network are mutually untrustworthy
  - An event response mechanism for KYC

System Model

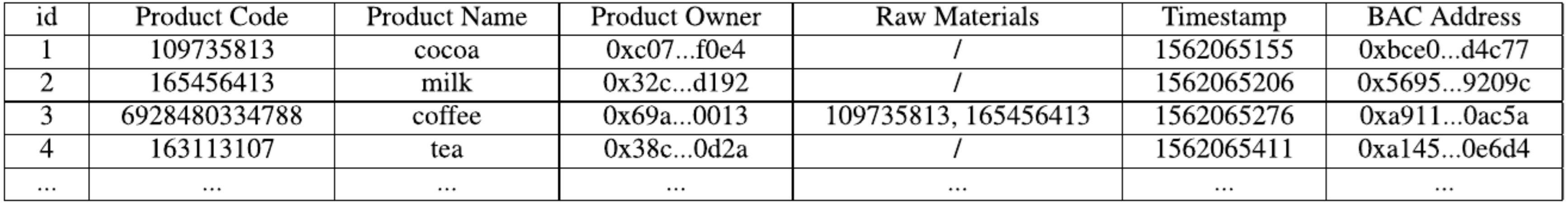
System security requirements:

- Data Accessibility
- Data Immutability
- System Autonomy
- Resistance to Man-in-the-middle Attacks



Smart Contract Design

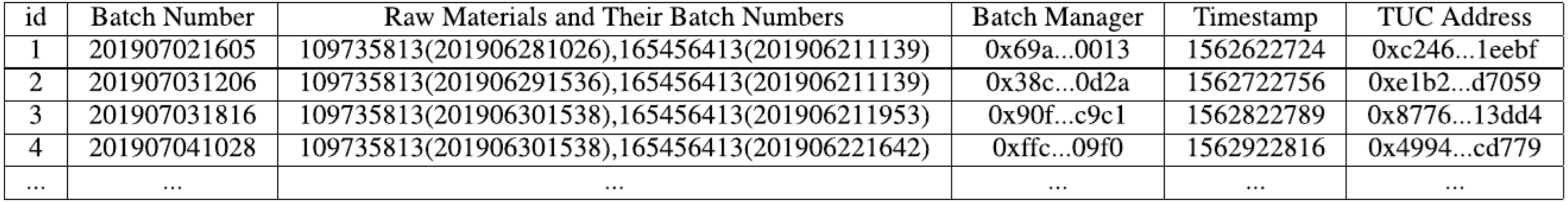
- Product Registration Contract (PRC)
    - Provides a product registration function register()
    - Product code, product name, product owner, and raw materials or parts
    - BAC contract address



id	Product Code	Product Name	Product Owner	Raw Materials	Timestamp	BAC Address
1	109735813	cocoa	0xc07...f0e4	/	1562065155	0xbce0...d4c77
2	165456413	milk	0x32c...d192	/	1562065206	0x5695...9209c
3	6928480334788	coffee	0x69a...0013	109735813, 165456413	1562065276	0xa911...0ac5a
4	163113107	tea	0x38c...0d2a	/	1562065411	0xa145...0e6d4
...	...	...	...	...	...	...

Smart Contract Design

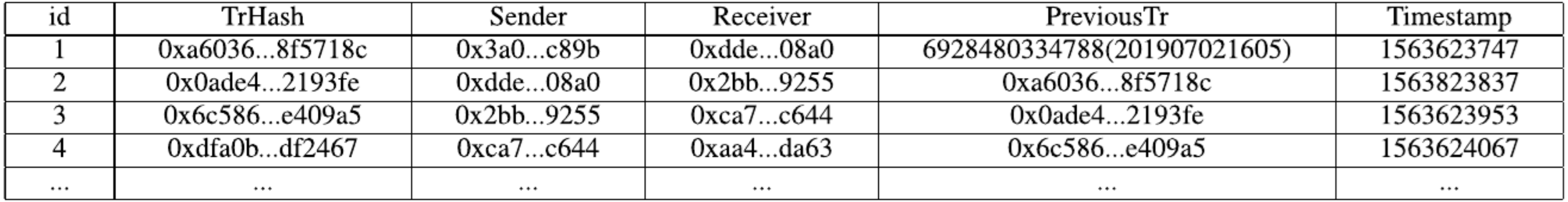
- Batch Addition Contract (BAC)
    - Provides the function addBatch() to add the production batch information of the product
    - Batch number, the batch manager, the timestamp, and the batch number of raw materials used to produce this batch of products
    - TUC contract information



id	Batch Number	Raw Materials and Their Batch Numbers	Batch Manager	Timestamp	TUC Address
1	201907021605	109735813(201906281026),165456413(201906211139)	0x69a...0013	1562622724	0xc246...1eebf
2	201907031206	109735813(201906291536),165456413(201906211139)	0x38c...0d2a	1562722756	0xe1b2...d7059
3	201907031816	109735813(201906301538),165456413(201906211953)	0x90f...c9c1	1562822789	0x8776...13dd4
4	201907041028	109735813(201906301538),165456413(201906221642)	0xffc...09f0	1562922816	0x4994...cd779
...	...	...	...	...	...

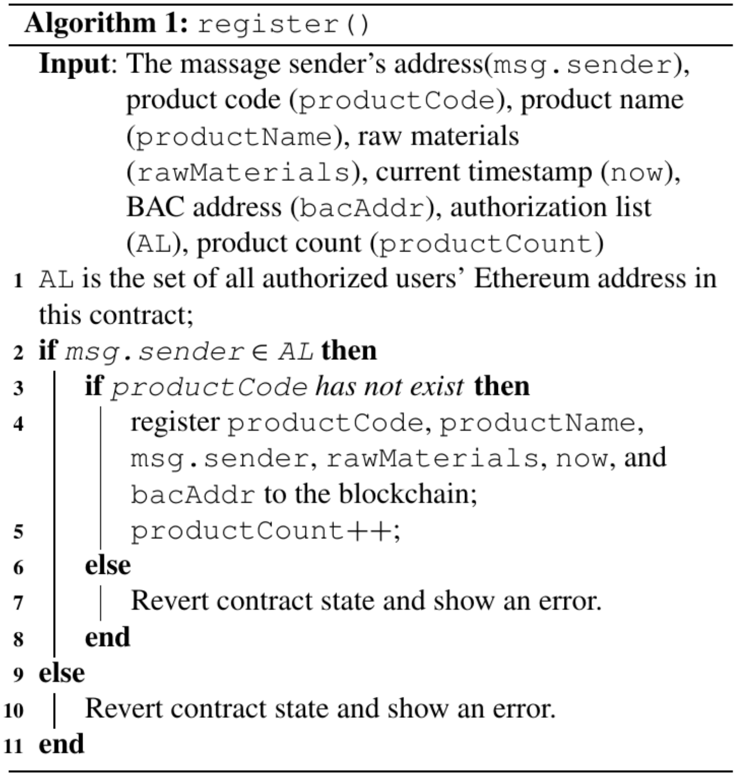
Smart Contract Design

- Transaction Update Contract (TUC)
    - When adding the production batch information and provides the function updateTr() to update the transaction history for this batch of products



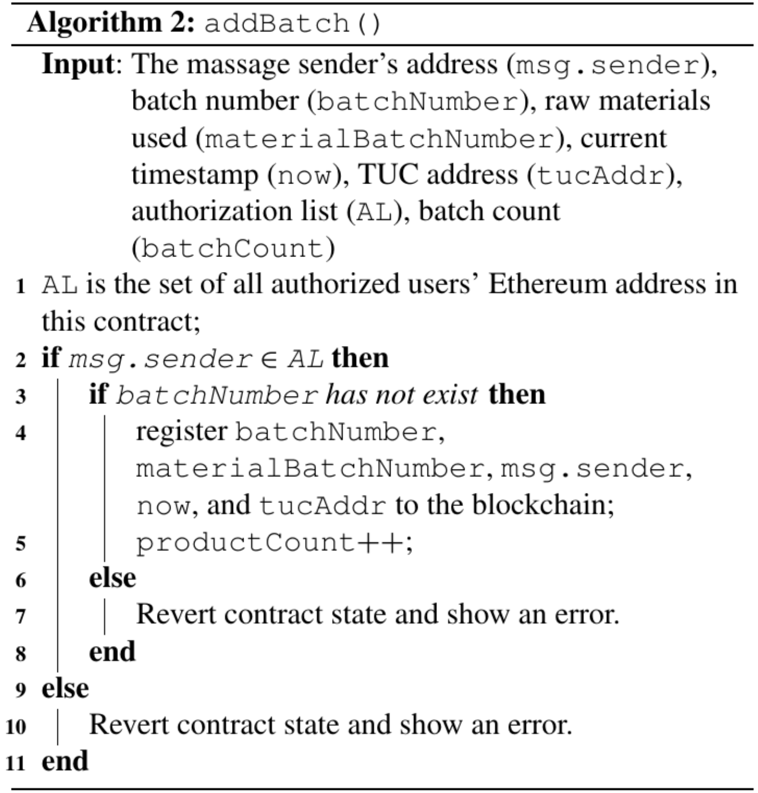
id	TrHash	Sender	Receiver	PreviousTr	Timestamp
1	0xa6036...8f5718c	0x3a0...c89b	0xdde...08a0	6928480334788(201907021605)	1563623747
2	0x0ade4...2193fe	0xdde...08a0	0x2bb...9255	0xa6036...8f5718c	1563823837
3	0x6c586...e409a5	0x2bb...9255	0xca7...c644	0x0ade4...2193fe	1563623953
4	0xdfa0b...df2467	0xca7...c644	0xaa4...da63	0x6c586...e409a5	1563624067
...	...	...	...	...	...

Algorithms



Algorithm 1: `register()`

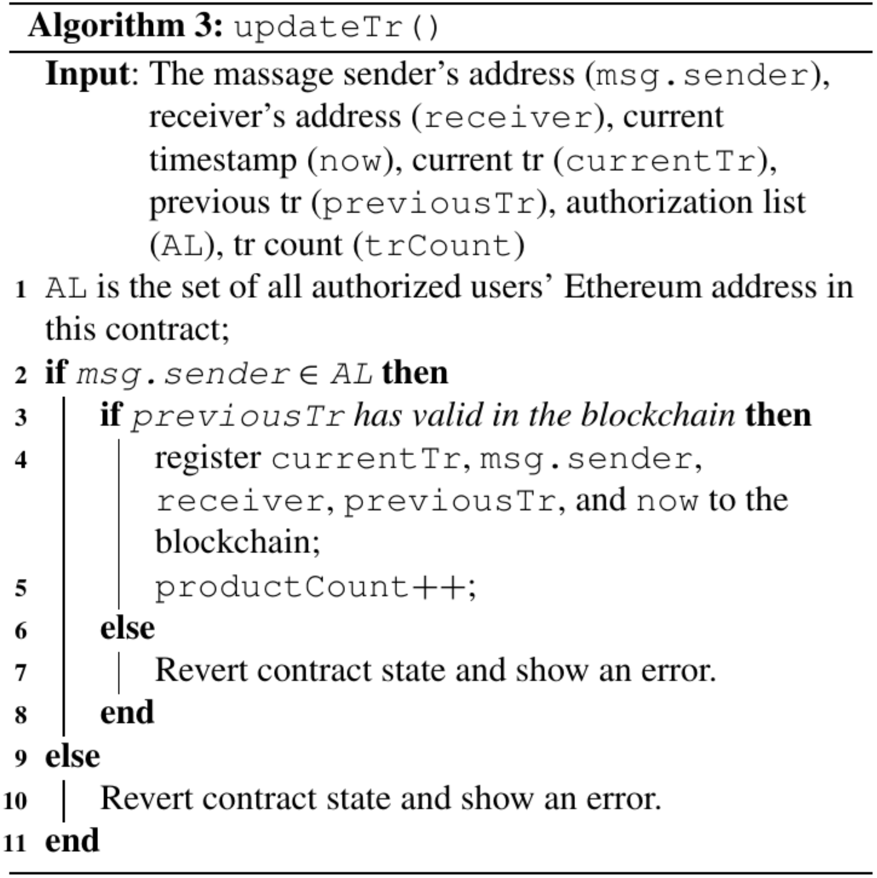
```
Input: The massage sender's address(msg.sender),
       product code (productCode), product name
       (productName), raw materials
       (rawMaterials), current timestamp (now),
       BAC address (bacAddr), authorization list
       (AL), product count (productCount)
AL is the set of all authorized users' Ethereum address in
this contract;
if msg.sender ∈ AL then
    if productCode has not exist then
        register productCode, productName,
        msg.sender, rawMaterials, now, and
        bacAddr to the blockchain;
        productCount++;
    else
        Revert contract state and show an error.
    end
else
    Revert contract state and show an error.
end
```



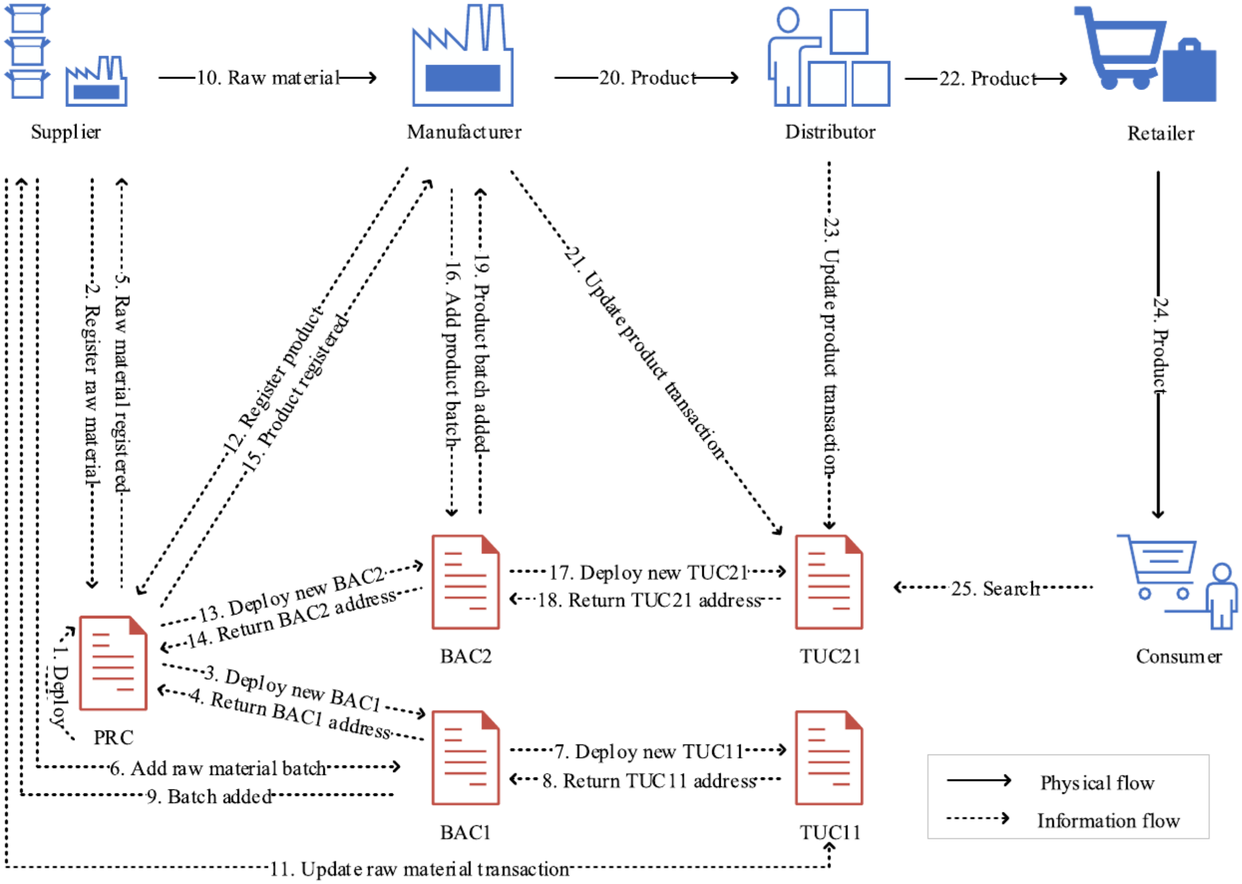
Algorithm 2: `addBatch()`

```
Input: The massage sender's address (msg.sender),
       batch number (batchNumber), raw materials
       used (materialBatchNumber), current
       timestamp (now), TUC address (tucAddr),
       authorization list (AL), batch count
       (batchCount)
AL is the set of all authorized users' Ethereum address in
this contract;
if msg.sender ∈ AL then
    if batchNumber has not exist then
        register batchNumber,
        materialBatchNumber, msg.sender,
        now, and tucAddr to the blockchain;
        productCount++;
    else
        Revert contract state and show an error.
    end
else
    Revert contract state and show an error.
end
```

Algorithms



```
Algorithm 3: updateTr()
Input: The massage sender's address (msg.sender),
       receiver's address (receiver), current
       timestamp (now), current tr (currentTr),
       previous tr (previousTr), authorization list
       (AL), tr count (trCount)
AL is the set of all authorized users' Ethereum address in this contract;
if $msg.sender \in AL$ then
    if previousTr has valid in the blockchain then
        register currentTr, msg.sender,
          receiver, previousTr, and now to the
          blockchain;
        productCount++;
    else
        Revert contract state and show an error.
    end
else
    Revert contract state and show an error.
end
```



The process of product registration, transferring, and tracking

Real Estate

IT Fundamentals Course
Group 6

Reference:

Ullah, Fahim, and Fadi Al-Turjman. "A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities." Neural Computing and Applications (2021): 1-22.

Neural Computing and Applications
https://doi.org/10.1007/s00521-021-05800-6

S.I. : MACHINE LEARNING APPLICATIONS FOR SECURITY

A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities

Fahim Ullah[1] · Fadi Al-Turjman[2]

Received: 16 October 2020 / Accepted: 5 February 2021

Abstract
Blockchains-based smart contracts are disrupting the smart real estate sector of the smart cities. The current study explores the literature focused on blockchain smart contracts in smart real estate and proposes a conceptual framework for its adoption in smart cities. Based on a systematic review method, the literature published between 2000 and 2020 is explored and analyzed. From the literature, ten key aspects of the blockchain smart contracts are highlighted that are grouped into six layers for adopting the smart contracts in smart real estate. The decentralized application and its interactions with Ethereum Virtual Machine (EVM) are presented to show the development of a smart contract that can be used for blockchain smart contracts in real estate. Further, a detailed design and interaction mechanism are highlighted for the real estate owners and users as parties to a smart contract. A list of functions for initiating, creating, modifying, or terminating a smart contract is presented along with a stepwise procedure for establishing and terminating smart contracts. The current study can help the users enjoy a more immersive, user-friendly, and visualized contracting process, whereas the owners, property technologies (Proptech) companies, and real estate agents can enjoy more business and sales. This can help disrupt traditional real estate and transform it into smart real estate in line with industry 4.0 requirements.

Keywords Blockchain · Smart contracts · Smart real estate management · Smart cities · Smart contract implementation · Smart contract design

1 Introduction and background

Smart cities are characterized by their focus on people, communities, and advanced technology usage [1–3]. This concept of technologies has been widely discussed, leading to smart cities being explored as a digital city, intelligent city, ubiquitous city, wired city, hybrid city, information city, and many more [4]. Big9 technologies are a recent concept where the adoption of nine such key technologies is explored and recommended to be adopted in the smart city. These include drones, the Internet of Things (IoT), clouds, software as a service (SaaS), big data, 3D scanning, wearable technologies, virtual and augmented realities (VR and AR), and artificial intelligence (AI) and robotics [5–7]. Researchers have explored these technologies over time, and their adoption frameworks presented for smart cities. These include the technology acceptance models for smart real estate management [5, 7–9], cloud computing model for smart city logistics [10], smart city reference model to build smart city innovation ecosystems [11], citizen-centric technology acceptance model for urban technologies [12] and unified smart city model for smart city conceptualization and benchmarking. In addition to these technologies, new avenues in using technology in smart cities have emerged, such as blockchain technology in the mining of cryptocurrencies in 'bitcoin housing' [8, 9, 13].

A cryptocurrency is a digital or virtual currency that is secured by cryptography [14]. Such security makes it nearly impossible to counterfeit or double-spend. The word "cryptocurrency" is derived from the encryption techniques that secure the network. A cryptocurrency is a medium of exchange for currency such as the Australian

✉ Fahim Ullah
f.ullah@unsw.edu.au

[1] PhD Scholar, School of Built Environment, University of New South Wales, Kensington 2052, Sydney, NSW, Australia

[2] Research Center for AI and IoT, Near East University, Nicosia, Mersin 10, Turkey

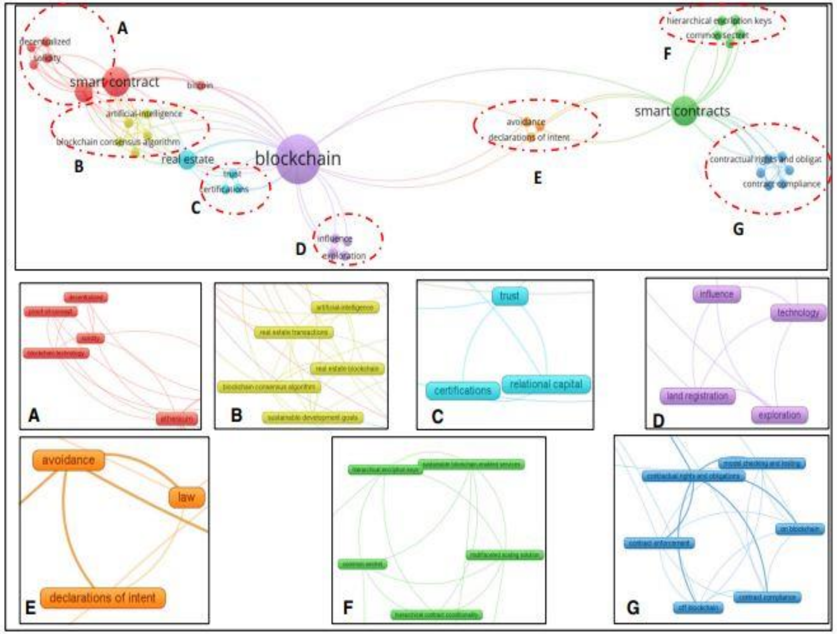
Published online: 22 February 2021

Introduction

- related to technology, which is characterized by three key aspects
  - Stability
  - Innovation
  - Focus on the user
- Smart real estate management that involves the use of blockchain technology

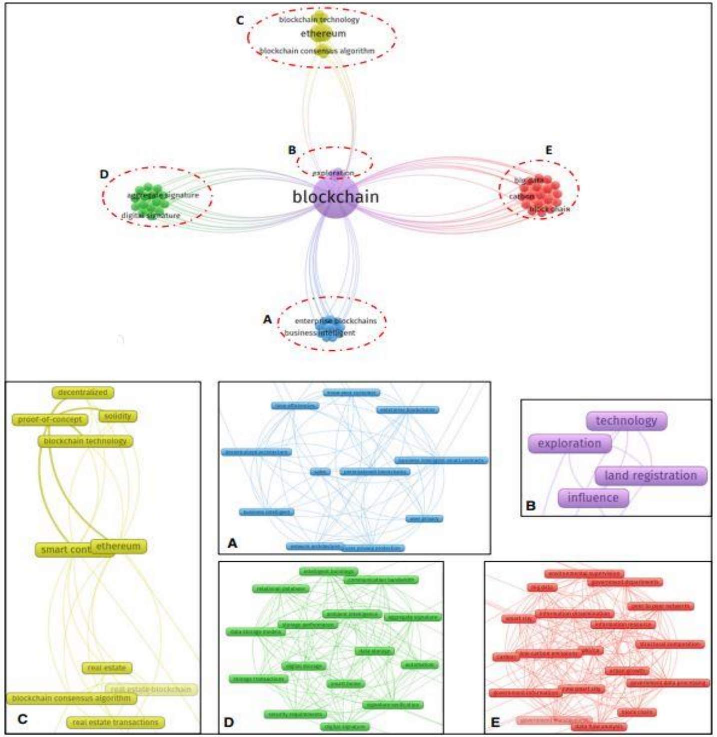
Relation between blockchain and smart contract

Category	Keyword
Computer	Solidity, Ethereum, Decentralization and Blockchain
Transactional	real state transaction, use of artificial intelligence
communicational	Trust, certifications
Technology	Impact of technology, blockchain land registration
Legal	Law, avoidance
Network	hierarchical encryption, common secret
Agree and adapt	Compliance and execution of the contract



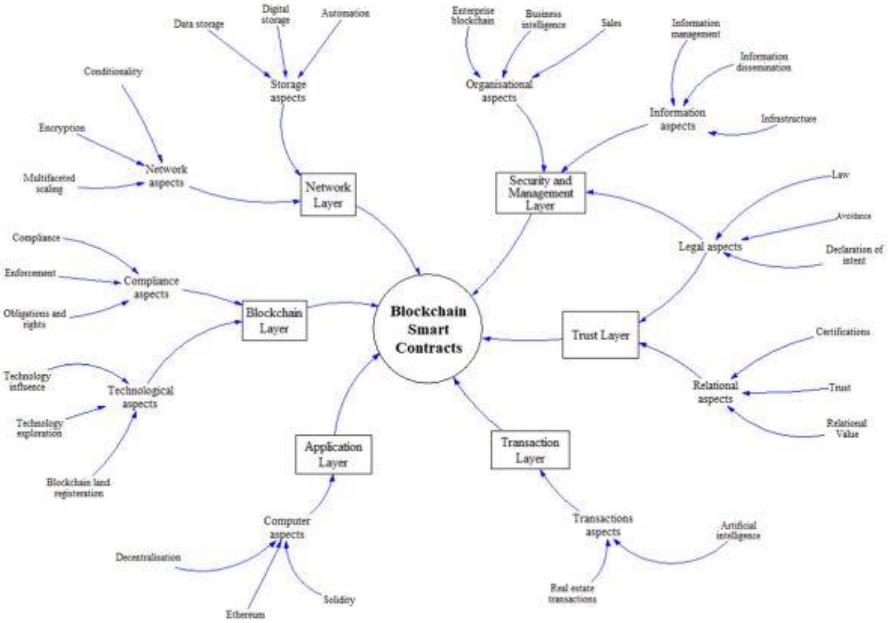
Classification of blockchain

Category	Keyword
Organizational	user data business intelligence
Technology	Impact of technology, blockchain land registration
Computer	Solidity, Ethereum, Decentralization and Blockchain
Memory	Data storage ,signature verification
Informational	Information management, information infrastructure



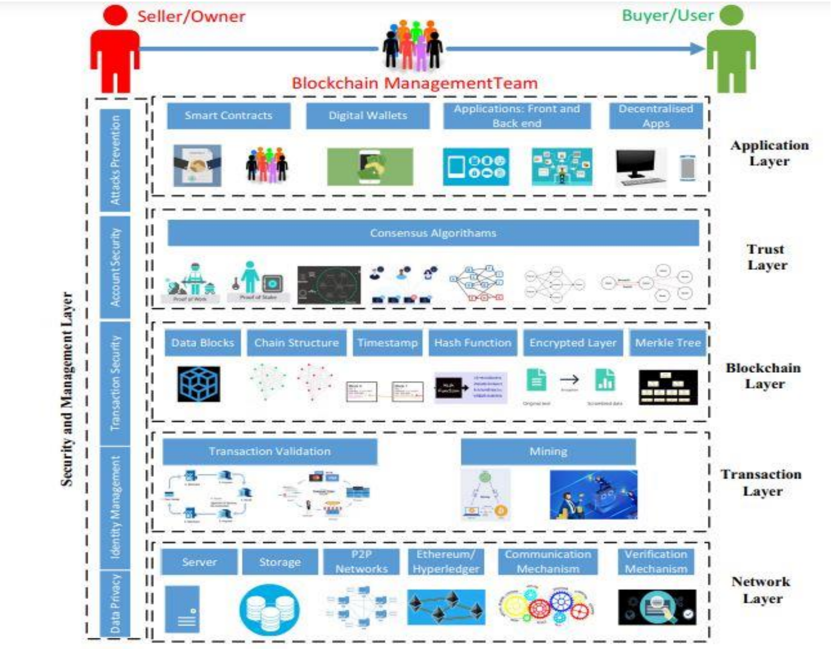
Blockchain in smart real estate

- It is made of 6 layers
- Combine 10 categories in these layers



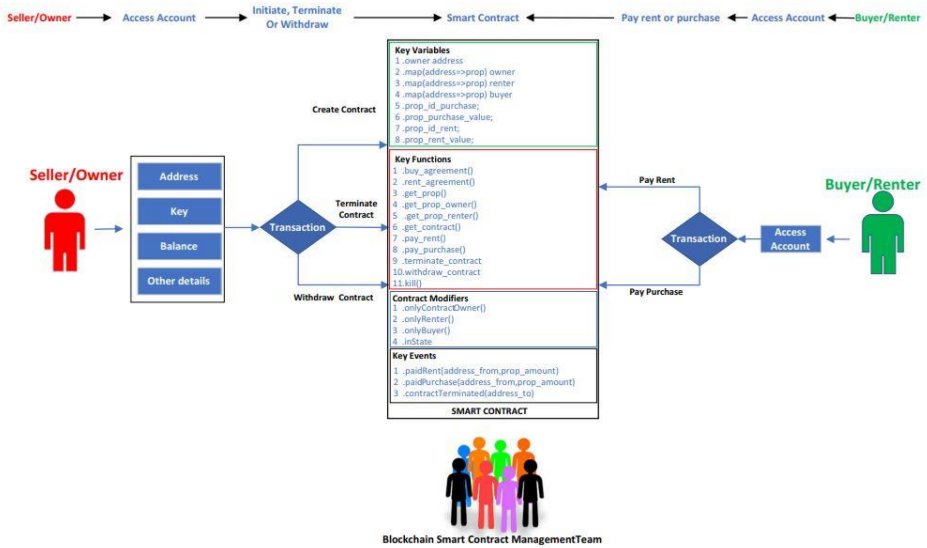
Classification of blockchain

layer	goals
Network	communication and verification mechanisms
Transaction	validation and processing and currency extraction
blockchain	hash function, chain structure, encrypted layer
Trust and confidence	Consensus development mechanism and authenticate transactions in the network
Application	Front-end and back-end applications
Security and management	Securing and managing smart contracts



smart real estate management

- The owner can create, terminate or cancel the contract
- The user can access his account and authorize transactions
- In smart contract function the parties are exchanged and the smart contract is set.



Key Variables
1 .owner address
2 .map(address=>prop) owner
3 .map(address=>prop) renter
4 .map(address=>prop) buyer
5 .prop_id_purchase;
6 .prop_purchase_value;
7 .prop_id_rent;
8 .prop_rent_value;

Key Functions
1 .buy_agreement()
2 .rent_agreement()
3 .get_prop()
4 .get_prop_owner()
5 .get_prop_renter()
6 .get_contract()
7 .pay_rent()
8 .pay_purchase()
9 .terminate_contract
10.withdraw_contract
11.kill()

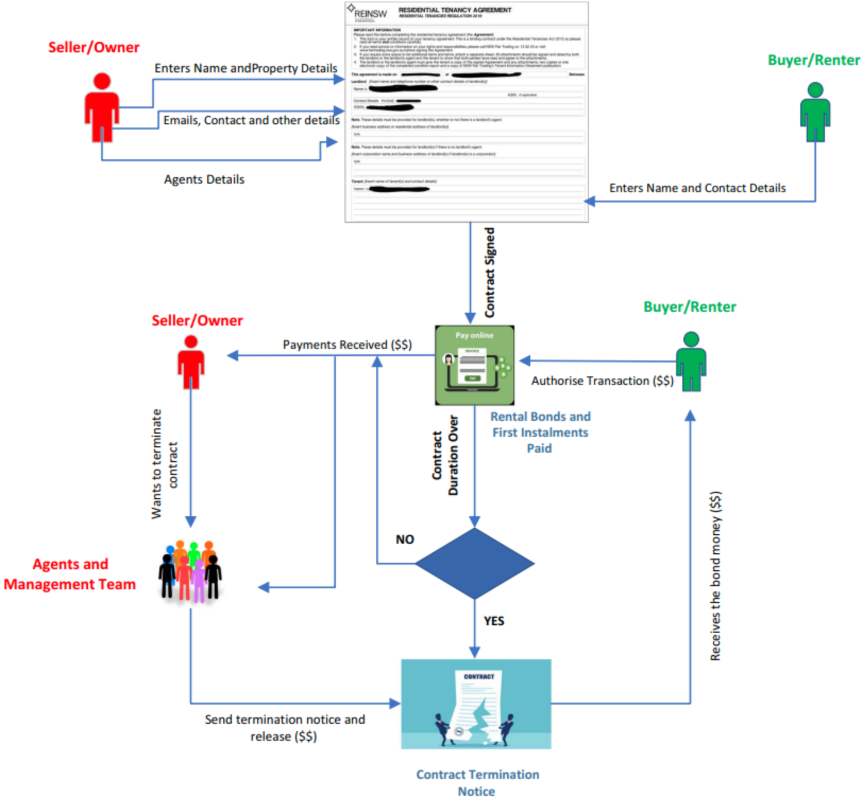
Contract Modifiers
1 .onlyContractOwner()
2 .onlyRenter()
3 .onlyBuyer()
4 .inState

Key Events
1 .paidRent(address_from,prop_amount)
2 .paidPurchase(address_from,prop_amount)
3 .contractTerminated(address_to)

SMART CONTRACT

implement and terms of smart contract termination

- Access with Web page
- The owner registers the details of the real estate in the smart contract
- The user registers the details of the desired contract
- Deposit and withdraw money automatically


Seller/Owner
Enters Name andProperty Details
Emails, Contact and other details
Agents Details
REINSW
RESIDENTIAL TENANCY AGREEMENT
Buyer/Renter
Enters Name and Contact Details
Contract Signed
Seller/Owner
Payments Received ($$)
Pay online
Buyer/Renter
Authorise Transaction ($$)
Rental Bonds and First Instalments Paid
Wants to terminate contract
Contract Duration Over
NO
YES
Agents and Management Team
Receives the bond money ($$)
CONTRACT
Send termination notice and release ($$)
Contract Termination Notice

Comparison

IT Fundamentals Course
Group 6

Comparison between three applications

- Establish trust between the parties of the contract
- Decentralized
- Create transparency
- Less fraud
- Unchangeable
- Do not completely remove third parties

Implementation

IT Fundamentals Course
Group 6