

Blockchain methodologies applied to transaction operations on the Real Estate Market

Andres Salgado

International Technological University
San Jose, California, USA
salgadoandre533@students.itu.edu

Co Authors

Jorge Valdeiglesias, Kartikeya Yellayi

International Technological University
San Jose, California, USA

valdeiglesjorge744@students.itu.edu

yellayishiva1284@students.itu.edu

April 21 2018

The blockchain concept was proposed several years ago. Only in recent years has the concept evolved into full fledged applications and frameworks that allow users to solve everyday problems with this technologies. One of the many issues that society currently faces are the skyrocketing housing prices. A partial reason of this increase in prices is the many intermediaries that are part of the real estate buying and selling process. Our application attempts to find a proper way to replace some of the entities involved on the escrow process with smart contracts executed on a decentralized Ethereum network. The paper briefly touches on historical facts related to the use and adoption of cryptocurrencies, the legal framework that is currently in place for the escrow business, and an in-depth analysis of the code base used for the test application.

1 Introduction

With the advent of “blockchain” technologies, as well as the necessity to establish a system where transaction trust could be offloaded to machines, we ventured into exploring how a system based on the Ethereum blockchain could accurately execute a series of smart contracts in order to validate a transaction between two entities.

2 The blockchain and its influence on crypto-currencies

It's close to 10 years after Bitcoin was introduced by Satoshi Nakamoto. The reason crypto-currencies currently exist is due to the underlying technology made available by the blockchain. Thomas Lowenthal from Ars Technica [12] goes onto explaining the complexities of cryptographic currencies, the concept of mining and make-work, and goes onto comparing Bitcoin against the trusty greenback which also faced hurdles when it was first put into circulation.

No currency system is perfect. One of the caveats of implementing a digital currency is the problem of double-spending. Since there are no regulating agents (in this case governments or private entities) that can verify the authenticity of a given cryptocurrency, there has to be an engineered mechanism that can protect users from issues related to double spending and the use of counterfeit instruments. The blockchain solves these two basic problems inherent to its digital nature by applying the concepts of digital signatures and peer-to-peer networks.[14][9]. On cppcon 2016 David Schwarz[1] at cppcon 2016

Submitted to:

© Andres Salgado, C. Author & Jorge Valdeiglesias, Kartikeya Yellayi
This work is licensed under the
Creative Commons Attribution License.

spoke about "Developing Blockchain Software". On his talk he mentions key characteristics of "the blockchain". Section 2.1 goes onto describing such characteristics.

2.1 What is a blockchain and what is one good for?

- Blockchains record state and history
- State is modified by transactions
- Everyone eventually agrees on the transactions
- Can be used to transfer tokens and coins

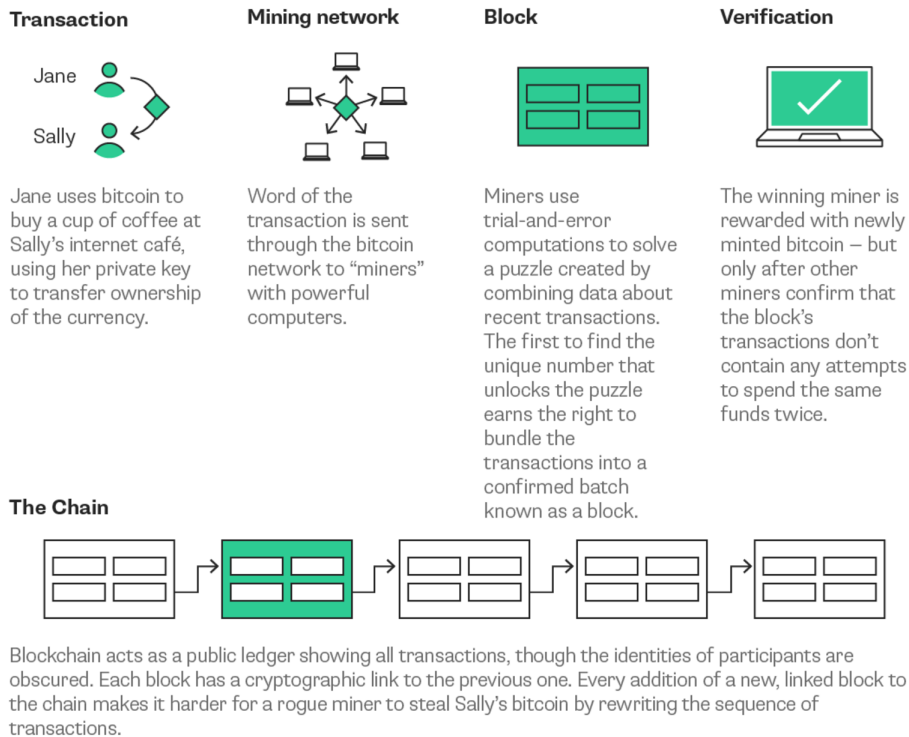
Based on this list, most of us would conclude that the blockchain is merely a database, but in actuality, the blockchain -according to Schwarz[1]- manages the double-spending problem.

2.2 What the blockchain does for bitcoin

Figure 1 describes how the blockchain validates bitcoin as cryptocurrency system[9] .

How Blockchain Works for Bitcoin

When payment is made with a physical coin, the person who handed it over can't spend it again. Preventing "double spending" in a digital currency is more complicated.



Source: Bloomberg

BloombergQuickTake

Figure 1: Image Source: BloombergQuicktake

2.3 Principal advantages of cryptocurrencies

Not only does Bitcoin comply with providing security to users that require to exchange currency within the system, but by December 2017[4] the 6 most important cryptocurrencies in world, among those *Ethereum* which is currently the second cryptocurrency based on market capitalization (**41.4 billion**), manage to continue on a growth path, with its value and market capitalization following an upwards trend, a sign of how confident the public feel about cryptocurrencies as a method to exchange value.

3 Legal Framework

In today's current economy, a legal framework is established so that in the case that two entities require to exchange property, goods or services, this exchange can be performed with the backing of a system that effectively transfers value from one entity to another.

For the purpose of the current body of research, our model specifically targets the escrow process of a real estate sale. Figure 2 describes the many entities and processes involved on the execution of an escrow during the sale of a property.

4 Beyond Bitcoin (other industries and its use)

Besides solving the issue of how to allow for a feasible digital currency, the blockchain has opened the door towards the development of new uses of the technology, that do not necessarily address the exchange of assets in a digital manner. This exposure has allowed millions of dollars to be poured into research and development of proper blockchain applications in a variety of fields with distinct uses and outcomes. One of the businesses that seems to be benefiting the most from this investments is the logistics business. Many companies are involved in the process of carrying goods. Most importantly, because there are several actors involved in such process, a delay in shipment can prove to be catastrophic to huge shipments.

Currently the majority of companies that engage in gathering data to make business decisions use different types of database systems in order to store, query and build statistical models out of collected data. When the interaction with that data doesn't require sharing such information, companies are equipped to process it, but when two or more entities[11] need to share such data, it is often complicated to achieve a consensus on how such exchange should be handled.¹

¹Olga Kharif on her article "Blockchain Goes Beyond Crypto-Currency" explains how companies in Finland, Sweden, Estonia and Latvia are beginning to use a blockchain system in order to share information.



Figure 2: Infographic "What is Escrow (detail)[8] Source: First American Financial Corporation

5 Ethereum and smart contracts

Back in 1996, Nick Szabo² laid much of the ground work of what we currently know as "Smart Contracts". On "Smart Contracts: Building Blocks for Digital Markets"[5] Szabo makes a conspicuous argument on how our society has built a structure based on the common law of contracts. He³ is meticulous when explaining the role that contracts play into our current free market economy. The article's introduction does not try to impose digital contracts as a replacement to our current system of values and the concept of agreements and contracts, but instead opens the door to a discourse on how computers in a digital society can improve or aid towards making the then current system more functional.

Experts conclude that *Bitcoin* has done to the blockchain what e-mail did to the internet. To further this notion of what the blockchain is capable of, it can be said that *Bitcoin* is a digital currency using the blockchain as a vehicle to function digitally. There are certain tasks that *Bitcoin* can perform, but they are limited compared to that of the scope of what *Ethereum* does. One of the main advantages of *Ethereum* is that it applies the same principles that the blockchain uses on *Bitcoin* with the added functionality of smart contracts⁴ as a method to exchange any item of value, this being money, content, shares or property.

Due to the advantages that *Ethereum* offers, it was chosen to dig deeper into finding a toolset that would allow the app to thrive towards developing a self-serving real estate property exchange tool.

5.1 RSA silently working on the background

Szabo puts great emphasis on explaining the background of RSA[13] and its critical role on smart contracts. The ideal metaphor uses two subjects -in this case Alice and Bob- to explain how public cryptography's mathematical intricacies work to create a pair of *keys* in this case a public one and private one that serve as a cryptography based exchange of messages. The importance of the use of RSA based encryption is directly related to the underpinning of the principles of contract design⁵ and are rooted on common law, economic theory, and contractual conditions, which in turn derive the principles of observability, verifiability, privity, and enforceability.

5.2 Smart Contract definition

An abridged definition of the smart contract provided by the *Solidity* documentation page goes as follows:

A contract in the sense of Solidity is a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain.[3]

In a strict technical sense, the smart contract is programmable to comply with any set of defined conditions. Because the smart contract is rooted in code, any prerequisite that was celebrated between two parties on a traditional contract, can have its clauses translated into code, therefore allowing for any legal conditions to exist digitally.

Figure 3 illustrates how a smart contract would execute the sale of a property. In this case two parties, the buyer and the seller, **exchange** an asset through a contract that supports the digitizing of a land deed

²Nick Szabo is credited as one of the first proponents of the use of smart contracts on the digital realm.

³Szabo does a marvelous job on explaining how our society arrived to the use of contracts and how these contracts are the bedrock of a free market economy.

⁴Smart contracts are currently handled by the Solidity language. Further information about solidity can be found at the development website <https://solidity.readthedocs.io/en/develop/>[6]

⁵Szabo goes on to explaining these principles on the *Some Basic Principles of Contract Design* subsection of [5]

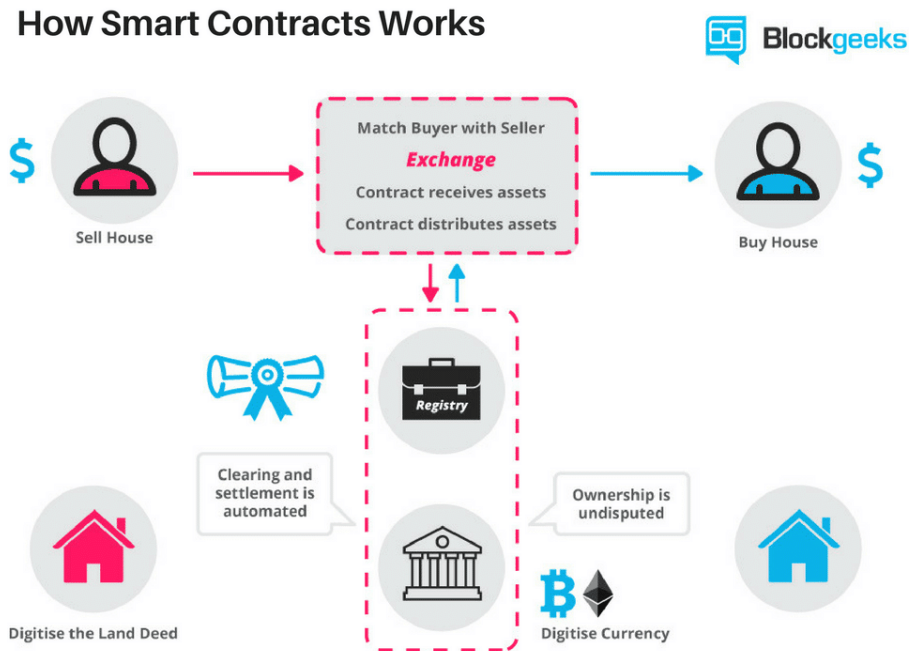


Figure 3: Image Source: Blockgeeks

and the subsequent digitizing of the currency, allowing for an ordered settlement and thus cementing the idea that the ownership of the asset was properly transferred to the new owner[15].

5.3 Zeroing on Ethereum

Ethereum's versatility, served as the perfect platform to deploy a generalized decentralized app seeking to solve smart contract transactions. Dr. Gavin Wood in his introduction to *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER* summarizes the objectives of building "a trustful object messaging compute framework." [16] Parting from these principles the platform choice selected for accomplishing the objective of the thesis revolved around the use of a framework grounded on *Ethereum*.

Research concluded that the chosen framework needed to have current front-end and back-end technologies, as well as to show signs of current community engagement and active development.

6 Truffle as a development platform

Truffle is a Javascript based development framework[7]. *Truffle* offers the following advantages as a tool:

- Built-in smart contract compilation, linking, deployment and binary management.
- Scriptable, extensible deployment and migrations framework.
- Automated contract testing for rapid development.
- Network management for deploying to any number of public and private networks.

- Package management with EthPM and NPM, using the ERC190 standard.
- Configurable build pipeline with support for tight integration.
- External script runner that executes scripts within a Truffle environment.

7 Application requirements (what to install)

The following software is required to run the experimental app:

- Truffle
- Ganache
- Node.js
- MongoDB
- Metamask
- Compatible Browser (Google Chrome or any other browser that supports the Metamask extension)
- Docker

7.1 Ganache

In order to deploy and test the validity and accuracy of contracts written within the coding environment, it is necessary to write the contracts to the blockchain. The creators of *Truffle* simultaneously develop and maintain a separate component named *Ganache*. *Ganache*[2] is a personal deployable test Ethereum network capable of accepting commands, with a GUI interface that allows users to inspect and control how the chain operates. It is a requirement for Ganache to run in the background in order to properly test the validity and actionability of any given contract code executed within the application.

8 Application logic

Property state depicts the logic around the contract and how its state changes based on data input and user interaction.

9 Application usage scenarios

On the current development stage the following changes of state are supported:

- Contract deployment
- Token transfer
- Property publishing
- Offer submission
- Party acceptance

9.1 Contract Deployment

The contract deployment stage is intimately related to the correct execution of the *Truffle* environment. The following requirements should be satisfied prior to running the commands shown in *Figure 3*

- Windows, Linux or Mac OS X
- NodeJS 5.0+ recommended.

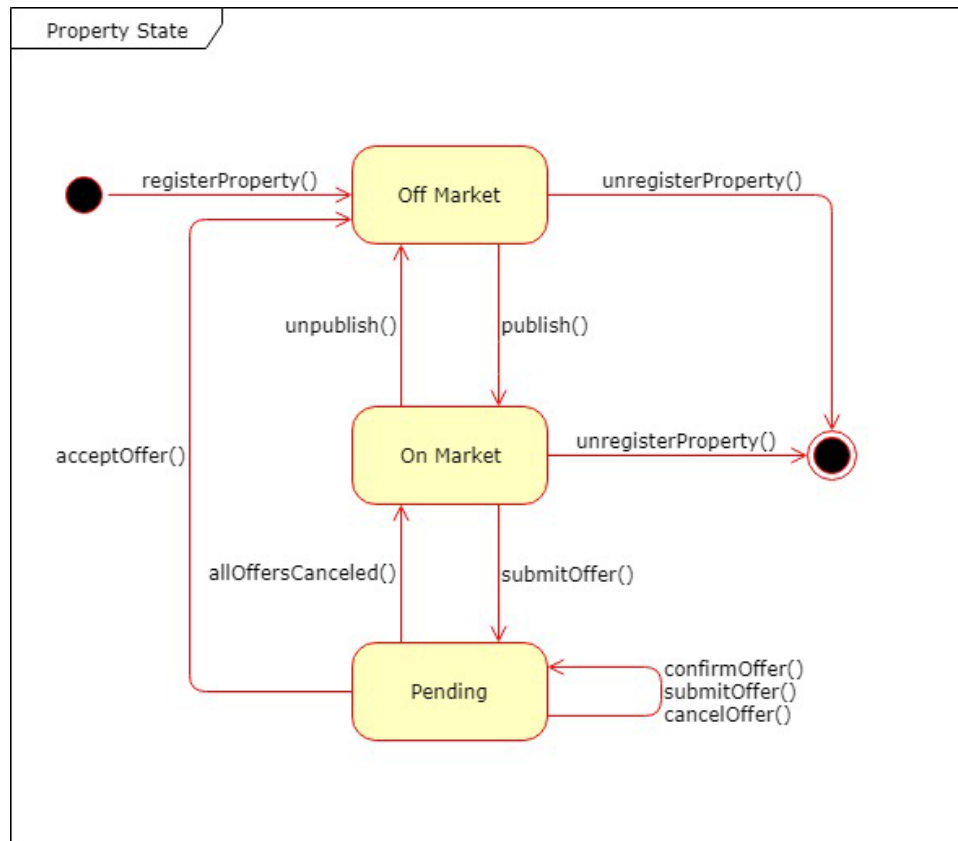


Figure 4: Property State Diagram. Author: Jorge Valdeiglesias

```
npm install -g truffle
```

Figure 5: npm command

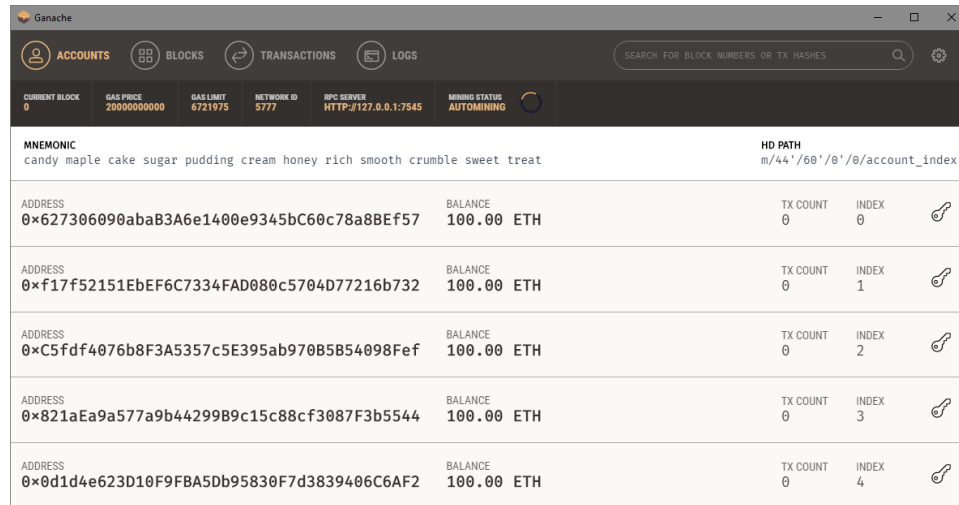
After this step it is required before any new *truffle* operation, to have a functioning test blockchain in place. *Ganache* is the tool of choice. It is available in two flavors, a desktop application and a command-line tool. For current test purposes the user will download the appropriate desktop application compatible with their running operating system.

Figure 6 shows an account overview after successful *Ganache* installation.⁶

9.2 Token transfer

The token transfer stage is a practical step that shows an actual transaction between two parties taking place. Digital assets are transferred between two key holders. The underlying code for this operation is driven by the *solidity* framework. Figure 7 shows the code involved during this stage.

⁶An extensive guide on how to install and deploy *Ganache* is available at the following address <http://truffleframework.com/docs/ganache/using>



ACCOUNTS		BLOCKS	TRANSACTIONS	LOGS
CURRENT BLOCK: 0 GAS PRICE: 20000000000 GAS LIMIT: 6721975 NETWORK ID: 5777 RPC SERVER: HTTP://127.0.0.1:7545 MINING STATUS: AUTOMINING				
MNEMONIC candy maple cake sugar pudding cream honey rich smooth crumble sweet treat		HD PATH m/44'/60'/0'/0/account_index		
ADDRESS	BALANCE	TX COUNT	INDEX	
0x627306090aba83A6e1400e9345bc60c78a8BEF57	100.00 ETH	0	0	
0xf17f52151EbEf6C7334FAD080c5704D77216b732	100.00 ETH	0	1	
0xC5fdf4076b8F3A5357c5E395ab970B5B54098Fef	100.00 ETH	0	2	
0x821aEa9a577a9b44299B9c15c88cf3087F3b5544	100.00 ETH	0	3	
0x0d1d4e623D10F9FBA5Db95830F7d3839406C6AF2	100.00 ETH	0	4	

Figure 6: Image Source: CONSENSYS 2017

```

function transfer(address _to, uint256 _value) public returns (bool) {
    require(_to != address(0));
    require(_value <= balances[msg.sender]);

    balances[msg.sender] = balances[msg.sender].sub(_value);
    balances[_to] = balances[_to].add(_value);
    emit Transfer(msg.sender, _to, _value);
    return true;
}

```

Figure 7: Token transfer function based on *OpenZeppelin*[10]

9.3 Property Publishing

Property publishing is one of the core features of the researched app. This feature allows a platform user to add a listing of a property, which in turn initiates a transaction that gets recorded on the blockchain. This step would be akin to having a seller start the escrow process during a regular sale on the real estate market. Figure 8 shows the code involved during this stage.

9.4 Offer submission

On this stage the smart contract updated the state of the *submitOffer* function based on the user input on the value of the property. This action triggers a series of events including notifying the intended seller of the buyers established offer. Figure 9 contains the code used for satisfying this function.


```
function registerProperty(string propertyId, uint256 propertyPrice)
public {
    properties[propertyId].owner = msg.sender;
    properties[propertyId].price = propertyPrice;
    properties[propertyId].state = 0;
    emit PropertyUpdated(propertyId, msg.sender);
}
```

Figure 8: State change once property is registered

```
function submitOffer(string propertyId, uint256 offer) public
onlyOnMarket(propertyId) {
    balances[msg.sender] -= offer;
    offers[msg.sender].propertyId = propertyId;
    offers[msg.sender].offer = offer;
    offers[msg.sender].submittedAtBlockNumber = block.number;
    properties[propertyId].state = 2;
    emit PropertyUpdated(propertyId, msg.sender);
}
```

Figure 9: State change once property is registered

10 Conclusions

Blockchain technologies are evolving at an accelerated pace. The application presented on this paper tackles an issue at the heart of the Real Estate market. If this application was to be deployed into production, it would replace a significant number of job posts directly related to the escrow business.

The authors are cautiously optimistic that in order for the free market to start accepting the use of applications and services dependent on the blockchain, a series of processes need to be put in motion. The most important movement towards cryptocurrency adoption has already begun to cause ripples on financial markets. It is only a matter of time until goods and services exchanged on the blockchain based currency markets begin to displace those traded via fiat currencies, and at the current pace of innovation, it is apparent that there is willingness from venture capitalist to properly fund companies interested in developing solutions based on a generalized global ledger.

We are anticipating an upward trend in interest towards the use of blockchain technologies, and predict that based on successful deployment of decentralized applications, the industry will create a snowball effect that most likely will disrupt the value exchange mechanisms currently in place globally.

10.1 Project tangible achievements

The application proposed on this paper achieves the following objectives:

- Successfully establishes a private local Ethereum test blockchain.

- Allows for proper user authentication via private keys in order to affect the blockchain transaction sequence.
- Successfully records a token transfer transaction between *User A* and *User B*.
- Allows for *User A or B* to publish a property for sale. The publishing of the property gets recorded on the blockchain as well.
- Establishes the validity of the smart contract code written on every change of the property state figure (as seen on Figure 4).
- Enables the exchange of value, albeit a fictitious one, between seller and buyer within the ethereum based test environment.
- Defines a proper implementation of the application on Web 3.0 environment.

11 Acknowledgements

We would like to thank Dr. Alex Wu for his invaluable input during the course of our studies and research.

References

- [1] CppCon 2016: David Schwartz Developing Blockchain Software.
- [2] Ganache. <http://truffleframework.com>.
- [3] Introduction to Smart Contracts Solidity 0.4.24 documentation.
- [4] The Most Important Cryptocurrencies Other Than Bitcoin? — Investopedia.
- [5] Nick Szabo – Smart Contracts: Building Blocks for Digital Markets.
- [6] Solidity Solidity 0.4.23 documentation.
- [7] Truffle Documentation. <http://truffleframework.com/docs/>.
- [8] What Is Escrow? <http://www.firstam.com/ownership/what-is-escrow>.
- [9] Bitcoin and Blockchain. *Bloomberg.com* (2013).
- [10] Zeppelin-solidity: OpenZeppelin, a framework to build secure smart contracts on Ethereum, Apr. 2018.
- [11] KHARIF, O. Blockchain Goes Beyond Cryptocurrency.
- [12] LOWENTHAL, T. Bitcoin: Inside the encrypted, peer-to-peer digital currency.
- [13] MILANOV, E. The rsa algorithm. *RSA Laboratories* (2009).
- [14] NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 9.
- [15] ROSIC, A. What Are Smart Contracts? A Beginners Guide to Smart Contracts.
- [16] WOOD, G. Ethereum: A secure decentralised generalised transaction ledger.