Report on decentralised technology for a green city service platform

Evaluation report on blockchain-based platform and service architecture

Version 1

Deliverable 3.1.

Project title:	SimpliCITY – Marketplace for user-centered sustainability services
Project acronym:	SimpliCITY
Project duration:	10/2018–03/2021
Project number:	870739
Work package/Task:	WP3 / T3.1.
Project website:	www.simplicity-project.eu

Authors:

Thomas Layer-Wagner, Polycular OG

Robert Praxmarer, Polycular OG

Birgit Schönauer, Polycular OG

Christoph Wögerbauer, Polycular OG

Edith Ngai, University of Uppsala

Phan Huy Hung, University of Uppsala

This project has received funding in the framework of the Joint Programming Initiative Urban Europe.

Document versions:

Version	Date	Changes	Author/s
v0.1	19.10.2018	Start with basics about decentralised technologies	Christoph Wögerbauer, Thomas Layer-Wagner, Robert Praxmarer,
v0.2	28.10.2018	Add advantages and disadvantages of decentralised technologies	Christoph Wögerbauer, Thomas Layer-Wagner, Robert Praxmarer,
v0.3	25.11.2018	Restructured contents	Thomas Layer-Wagner, Robert Praxmarer, Edith Ngai, Phan Huy Hung
v0.4	05.12.2018	Add current developments in decentralised technology and Review	Thomas Layer-Wagner, Birgit Schönauer
v0.5	10.12.2018	Add IoT and Review	Edith Ngai, Thomas Layer-Wagner, Phan Huy Hung
v1.0	28.12.2018	Update and Review, Finalisation of Document	Birgit Schönauer, Christoph Wörgerbauer

Table of contents

1. Executive Summary

SimpliCITY will be an information platform developed in the SimpliCITY project and it will be implemented and tested in the cities of Salzburg (AT) and Uppsala (SWE). The platform will use incentivisation and nudging to boost regional sustainability services on a city level. The project focus is on three areas namely bike mobility, local production and consumption and social inclusion. For cities and their city managers, it should become easier to promote and boost regional sustainability services through a unified channel and platform. The platform will provide information, incentives and challenges to support services, so that not every single service has to have its own incentivisation and nudging system, but one throughout the city that ties the different city services together and creates a shared user base.

This report discusses the requirements and implications of leveraging decentralised software architecture and distributed ledger technology (DLT) for a service platform like SimpliCITY. The aim is to uncover benefits, but also threats of decentralised technology based on exemplary use cases in the ecosystem of the platform.

Part of this deliverable is also to investigate and understand the challenges beyond the technical feasibility. These challenges include data privacy, environmental sustainability, accessibility, cost and trust. The personal right to be forgotten is currently in contradiction with DLTs immutability. Are there any solutions or concepts yet targeting this problem? What should be taken into account to reduce the ecologic footprint? These and other challenges have to be considered in order to create the best possible foundation for a successful SimpliCITY project.

2. Administrative Information

Basic information on the SimpliCITY project and the present deliverable:

Project title	SimpliCITY - Marketplace for user-centered sustainability services
Project coordinator	Salzburg Research Forschungsgesellschaft mbH (SRFG), Salzburg, Austria; project manager: Petra Stabauer BSc MSc
Project partners	Polycular OG, Hallein, Austria Stadt Salzburg (City of Salzburg), Austria Salzburger Institut für Raumordnung und Wohnen – SIR (Salzburg Institute for Regional Planning & Housing), Salzburg, Austria Uppsala Kommun (City of Uppsala), Sweden University of Uppsala, Sweden
Funding	JPI Urban Europe, Innovation Actions (Call: Making Cities Work) Funding is being provided by Vinnova (Sweden) for the Swedish project partners, and the Austrian Research Promotion Agency (FFG) for the Austrian project partners.
Project nr.	870739
Deliverable number	D 3.1
Deliverable title	Evaluation report on blockchain-based platform and service architecture
Authors	Thomas Layer-Wagner (Polycular), Robert Praxmarer (Polycular), Birgit Schönauer (Polycular), Christoph Wögerbauer (Polycular), Edith Ngai (University of Uppsala)
Version & status	Version 1
Date	28 December 2018

3. Introduction

Decentralized programming techniques haven’t been developed just recently. They have a long history in the field of anonymous communications starting in 1979 by David Chaum (Chaum, 2003). Quickly followed by the idea of the first decentralized payment system in 1983 (Chaum, 1983).

In 1999, Napster was launched and became the first widespread decentralized technology used by the public (Washbourne, 2015). Napster was a data distribution application, a peer-to-peer network which anyone could join and use to share files with another. The huge success of this platform triggered a new wave of file-sharing platforms. Mainly due to copyright conflicts many of these don’t exist anymore. The reason for the advent of decentralized data distribution solutions during this new wave, was above all the need to overcome technical limits in network bandwidth.

Today, this limitation is no longer a bottleneck for centralised solutions. Before taking a closer look into the technical details we want to look at the benefits for decentralising nowadays?

4. What is decentralised software?

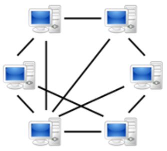
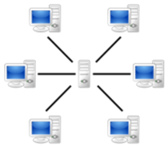
The Merriam-Webster dictionary defines “decentralization” as the “dispersion or distribution of functions and powers” (Definition Of DECENTRALIZATION, 2019). A central point of control is abandoned in favour of several points. Vitalik Buterin (Snyder, 2019), co-founder of the programmable blockchain Ethereum, distinguishes three types of software decentralisation (The Meaning Of Decentralization, 2019):

- **Architectural decentralization**
  A system does not consist of one single node (computer) but a multitude of nodes.
- **Political decentralization**
  No single individual or organization is exclusively in control.
- **Logical decentralization**
  If a node malfunctions, the system stays functional.

4.1. Technologies for decentralised software

4.1.1. Peer-to-peer networking (P2P)

Peer-to-peer networking is the model how distribution is done in a decentralised architecture. It’s the counterpart of the commonly used client-server model.

Peer-to-peer network:	Client-server network:
 *Figure 1: Peer-to-peer network (Source: Bieg, 2019)*	 *Figure 2: Client-server network (Source: Bieg, 2019)*

It describes how the connections between the nodes are modelled. In a peer-to-peer network, each node is equal which means that workloads and tasks are distributed.

4.1.2. Distributed Hash Table (DHT)

A DHT (wikipedia.org, 2019) is a data structure for a decentralized storage system in a structured P2P network. Data is stored in the form of key-value pairs. Any node can easily retrieve data if it has the given (unique) key. All nodes are responsible for maintaining the mapping from key to values, therefore the responsibility is distributed.

Although this system should work without fault while nodes are being removed/added or even failing, DHT do not provide data consistency and integration (Toonstra, 2019). In addition, scalability remains another challenge, since lookup times will increase with system scale.

4.1.3. Distributed Ledger Technology (DLT)

A distributed ledger is a decentralized database, one could also describe as record book, which holds a synchronised record of all transactions (worldbank.org, 2019). This means each node in the system has a copy of this ledger holding all recorded transactions. Before a transaction is added to the ledger it must be validated. Validation is achieved through a consensus mechanism which is different according to the distinct implementation. Once a transaction is validated, it is added to the ledger and distributed, so that all nodes update their ledger. Recorded transactions cannot be modified or deleted without alerting the other nodes that there is a manipulation attempt. Since all nodes have a copy of the record book they easily detect if others try changing content. This transparent system eliminates the need for any central authority or third party to validate transactions.

The creation and validation of transactions (records) employs cryptography for e.g. creating digital fingerprints (cryptographic hash) for records.

DL implementations can be categorized as follows:

- **Permission less** (unrestricted), public/shared systems - e.g. Bitcoin, Ethereum anyone can join and participate in the consensus process
- **Permissioned** nodes participating in the validation process are pre-selected by a network administrator (identity-verification) before joining the network (europa.eu, 2019).
    - **public/shared systems** – e.g. Microsoft Framework
      these can be viewed by anyone, but only participants can take actions
    - **private/shared systems** – Hyperledger
      for participants only

4.1.3.1. Validation - Consensus

Achieving consensus is a crucial part in DL projects, since transaction validation is achieved by applying a consensus method. These methods vary in different aspects like needed computational power, efficiency, speed and security just to mention a few. In short, a consensus method prevents fraud and hinders double spending of resources.

The blockchain and many other projects are currently using a “Proof-of-Work” (PoW) consensus finding algorithm. The main characteristic of the PoW algorithm is that is poses a hard-to-solve computational problem. Therefore, nodes, which want to solve the problem, so called miners, must invest time and computational effort. Still, other nodes can easily check if the solution is correct. The first miner to solve the problem is rewarded for the effort.[1] Since many nodes (miners) participate in this validation process much computational power is invested.

Due to the high energy consumption and the reasonable doubt whether DL is suited for larger scaled utilization with “Proof-of-Work” consensus a lot of other algorithms are currently being explored.

One of these is the “Proof of Stake” PoS algorithm, which will replace the PoW currently used in the programmable blockchain Ethereum (BTC-ECHO, 2019). In PoS (Medium, 2019) validation is carried out by a deterministic chosen node. The selection process considers multiple factors (e.g. deposited and locked cryptocurrency coins, coin age). The chosen miner (most often called forgers in this correlation) receives the transaction fees as reward for validating the transaction. In contrast to PoW this method is energy efficient, because not many miners race to find the solution first.

[1] Rewards are only required for public permissionless DLTs to guarantee network security.

One very interesting consensus algorithm is currently Raft (Medium, 2019). Additionally, a very interesting topic for further investigation would be to use time-invariant systems.

4.1.3.2. Blockchain

Blockchain is the most prominent implementation of DLT. The blockchain is the ledger as transaction records are organized in blocks. Typical block information are transaction data, timestamp and the block's cryptographic hash but can also contain additional information depending on the blockchain implementation (Golosova, The Advantages and Disadvantages of the Blockchain Technology, 2018).

So, each block contains a varying number of transactions which have been validated. Each block also has a reference to the previous block in form of a cryptographic hash, which is basically a digital fingerprint.

The current's block cryptographic hash, its fingerprint, considered the previous block's fingerprint in the creation process. By design once a block is created and accepted by general consent, it is added to the blockchain and cannot be altered without breaking the chain, because automatically generated fingerprints for all following blocks would be different from those fingerprints stored in the blockchain, each node has a copy of.

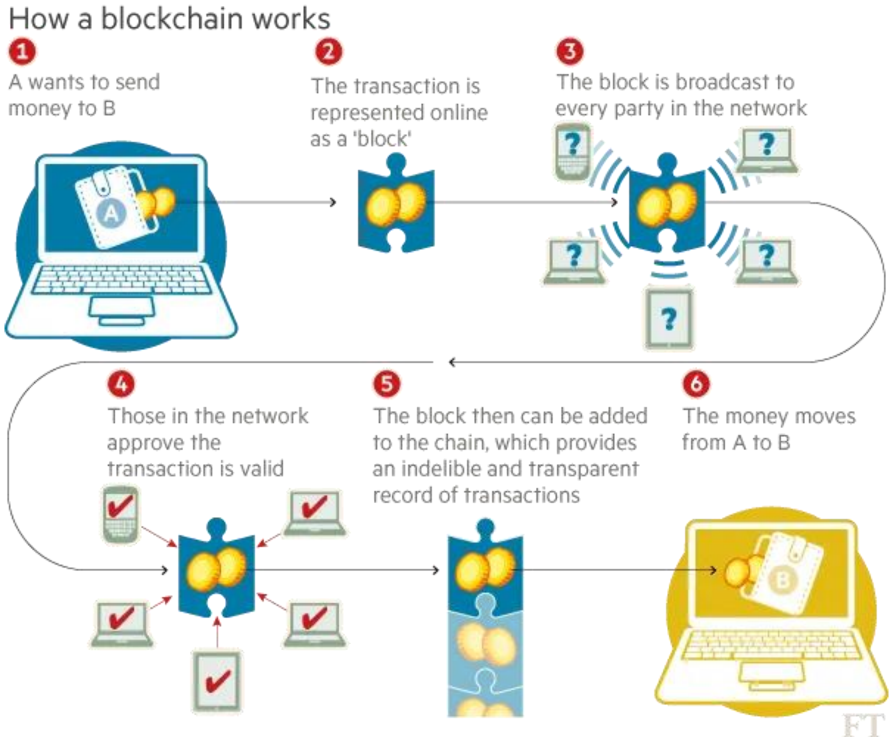

How a blockchain works
1
A wants to send money to B
A
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
?
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
B
FT

Figure 3: How a blockchain works (Source: Wild, 2015)

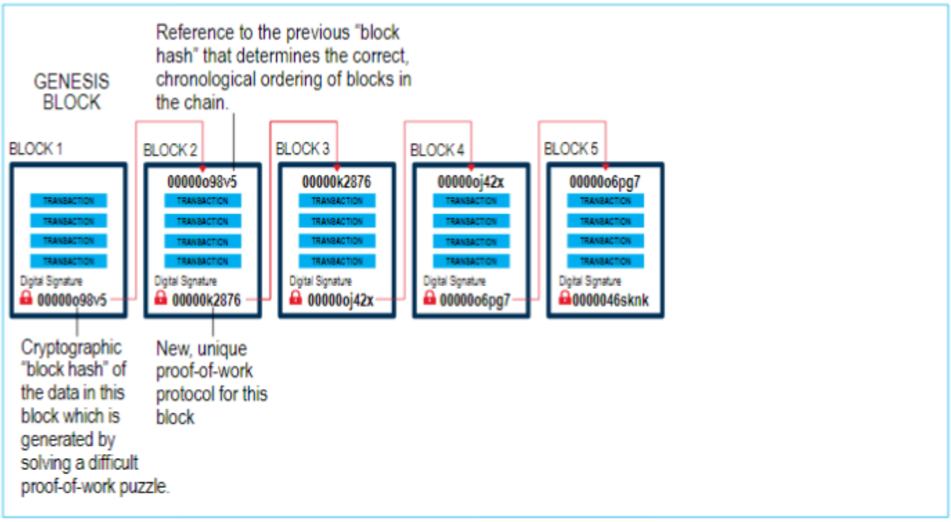

GENESIS BLOCK
Reference to the previous "block hash" that determines the correct, chronological ordering of blocks in the chain.
BLOCK 1
BLOCK 2
BLOCK 3
BLOCK 4
BLOCK 5
00000o98v5
00000k2876
00000oj42x
00000o6pg7
TRANSACTION
Digital Signature
00000o98v5
00000k2876
00000oj42x
00000o6pg7
0000046sknk
Cryptographic "block hash" of the data in this block which is generated by solving a difficult proof-of-work puzzle.
New, unique proof-of-work protocol for this block

Figure 4: Distributed Ledger Technology (DLT) (Natarajan, Krause, & Gradstein, 2017)

4.1.3.3. Cryptography

Cryptography is a crucial characteristic of DLT. A cryptographic hash is calculated based on the transaction data and applies a timestamp. A block has a collection of transaction and is signed with a digital signature like a contract signature.

DLT uses public key cryptography which is also known as asymmetric cryptography. Asymmetric cryptography uses two sets of keys to encrypt and decrypt content. Each participant has a public and a private key. The private key is as the name suggests, only known to the owner, and is used for digital signature. The public key on the other hand is known and is used for authentication.

With this technique, it is possible to share a public key for your counterpart to encrypt some content, which can only be decrypted by the linked private key. Additionally, it can be ensured that an encrypted content belongs to the owner of the private key. The blockchain is using this to know e.g. sender and receiver of transactions.

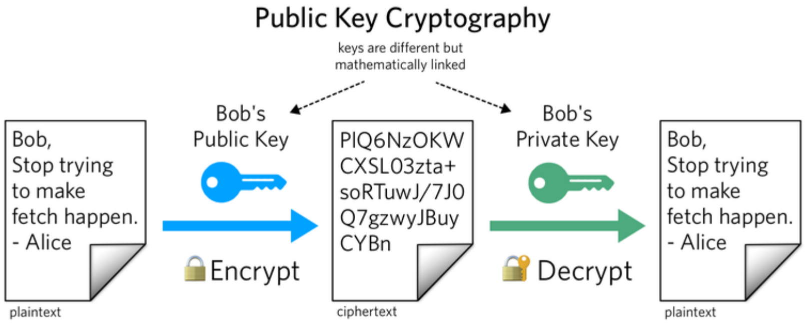


Figure 5: Public key cryptography (twilo.com, 2019)

4.2. Overall advantages

4.2.1. Trust

In centralized systems, trust is achieved by the involvement of central authorities (e.g. bank and a government ensuring deposits). This institution-based trust does not apply to decentralized systems, which do not have any central authority by design. But this statement is not necessarily true.

In case of the cryptocurrency Ether, fake news reporting the death of its founder and active developer Vitalik Buterin caused a big financial loss. This incident indicates that society is not only trusting the system as such but is rather still in need to connect to the technology through a person (theconversation.com, 2019) or institution.

But how can decentralized technologies create trust?

A user needs to understand basic principles of DL first, to see the benefits of decentralized systems. To create and maintain trust in this new technology, it will be important that users understand the system functionality. Explanation of decentralised systems in an easy and understandable transparent way must be accomplished. To facilitate this crucial step, user experience is essential (Stanford Graduate School Of Business - Blockchain For Social Impact, 2019).

Maintaining public trust is a challenge. Fostering this trust will possibly entail making users feel, they are being part of the decision-making process. Furthermore, it will be of importance that changes, improvements and such are openly communicated to users.

Main benefits consist of the following aspects:

- **Decentralization**

  There is no need for a central authority for validation, thus transactions can be carried out directly. This can result in faster transactions, lower costs and better scalability.

- **Transparency**

  All nodes have a copy of the ledger. All relevant nodes must agree that a transaction is valid. The adding of any record needs validation through a consensus mechanism. Changes are propagated across the system.

- **Automation / Adaptability**

  Programmable blockchains allow the usage of smart contracts which contain applications. These applications are executed automatically if a certain condition is met (e.g. funds received).

- **Immutability**

  Once a transaction is added to the ledger it cannot be changed or deleted. All nodes have a copy of the ledger and transactions / blocks are identified by cryptographic hashes. Any change would reflect in different hashes which will not be in accord with the ledger of each node.

- **Speed / Efficiency**

  Since there is no need for any third party to authorize transactions and put these into actions, transactions can be executed directly – or in the case of smart contracts – applications performing different actions are executed directly.

- **Cost Reduction**

Decentralising parts of a software system can contribute to cost saving in the following fields:

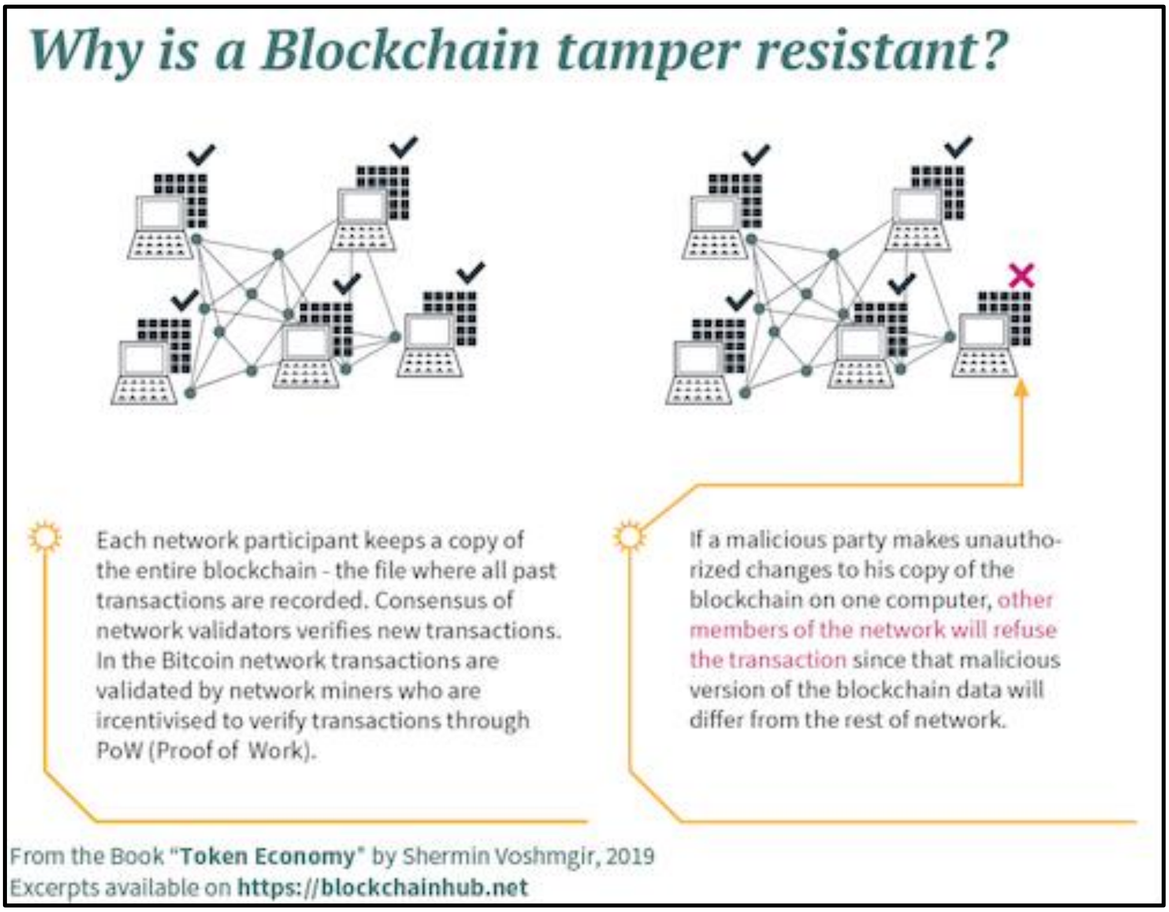
  - Network usage
  - Storage usage
  - Computational usage

4.2.2. Fault tolerance

Decentralised software has the benefit of a higher fault tolerance. Even with failing parts, the overall functionality of the system can be maintained. This in turn means, that there is a higher system availability in general. From the user's perspective, the system is more reliable which again increases the value of the system. A prerequisite of fault tolerance is political distribution, meaning that too much power must not be gathered in relation to location, used client software etc. (Medium, 2019).

4.2.3. Security / Fraud prevention

In a decentralised system, there is, by design, no single point of attack. As a result, malicious attacks are more difficult. Of course, this does not mitigate the need of proper security methods for different system components.
Since all nodes of a system control processes, fraud is detected very fast and the integrity of the system is maintained.



Why is a Blockchain tamper resistant?

Each network participant keeps a copy of the entire blockchain - the file where all past transactions are recorded. Consensus of network validators verifies new transactions. In the Bitcoin network transactions are validated by network miners who are incentivised to verify transactions through PoW (Proof of Work).

If a malicious party makes unauthorized changes to his copy of the blockchain on one computer, other members of the network will refuse the transaction since that malicious version of the blockchain data will differ from the rest of network.

From the Book "**Token Economy**" by Shermin Voshmgir, 2019
Excerpts available on **https://blockchainhub.net**

Figure 6: Why is a Blockchain tamper resistant? (Source: Voshmgir, 2019)

Still, each of the following components poses a potential security risk and must be managed:[2]

- Network infrastructure & maintenance (backups)
- Identity Access Management (permissioned DL)
- Ledger
- Integrity of the Consensus Mechanism
- Cryptography
- Cryptographic Keys
- Smart Contracts
- Privacy

Depending on the implementation, privacy can become a problematic topic if identifiable information is written on the (immutable) ledger (more in section 3.1.1.).

4.3. Overall disadvantages

The following list should give a brief overview of the key disadvantages or hindrances:

- **Loss of control / Speed of action**

  In the aspect of a single individual or organization control will be lost. Changes in the system will take more effort as every node of the system must be in accordance.

- **No central point for distribution / correction**

  If there is no central point for distribution or correction, it will take more effort to redistribute updates to every single point of the system. This may be noticeable as it will take longer that changes take effect. But the necessary time for updates will be deeply dependent on the network circumstances. It could even be conversely, and distribution takes place faster.

- **Scalability / Transaction Speed**

  As Harish et. al (Natarajan, Krause, & Gradstein, Distributed Ledger Technology (DLT) and blockchain, 2017) note, permissionless blockchains like Bitcoin, are limited in transaction speed, which is less imminent for Ethereum. On the other hand, permissioned blockchains have a higher transactions speeds and a greater capacity but are less transparent and lack scale. Furthermore, there still exists concerns regarding resilience and robustness of DLT for large volume transactions.

- **Complexity**

  A higher number of moving parts always means higher complexity. So, it will be more difficult to get everyone to understand what is going on. If a system is more complex system development is likely to be more expensive.

- **Power consumption / Environmental cost**

  The system needs to distribute and update changes immediately to maintain transparency and integrity. This results in quite a high energy consumption for keeping the system up-

[2] Following: "EY - Blockchain & Distributed Ledger Technology From A Cybersecurity Perspective". 2019. *Ey.Com*. Accessed July 31 2019. https://www.ey.com/nl/nl/services/advisory/advisory-for-financial-services/ey-blockchain-and-dlt-from-a-cyber-security-perspective.

to-date. Similar applies to techniques for finding consensus to different degrees, since nodes might need to invest time and effort in this process (Golosova, The Advantages and Disadvantages of the Blockchain Technology, 2018). Especially the Proof-of-Work consensus method has a large energy footprint.

4.4. Current developments in decentralised technology

4.4.1. Cryptocurrencies, Bitcoin, Tokens

A cryptocurrency is a digital asset using cryptography to secure transactions and verify the transfer of assets (wikipedia.org, 2019). Another important fact is that cryptocurrencies are not issued and managed by a central authority and is therefore decentralized (investopedia.com, 2019).

Released in 2009 (newyorker.com, 2019) Bitcoin (web.archive.org, 2019) is described to be the origin of the blockchain technology and was definitely the starting point of the blockchain hype.

Bitcoin’s great success wouldn't have happened without the financial crisis of 2007-2008 upfront. The financial crisis created mistrust towards the financial system and its central controlled banks. Bitcoin was welcomed as the solution and technical answer to the trust issue. Nowadays this technology is explored for solving the problem of declining trust in a lot of different areas.

After Bitcoin, a lot of cryptocurrencies were invented and mostly seen as a new opportunity of investment. Many of these new cryptocurrencies were funded with Initial Coin Offering (ICO). This funding method is unregulated and declared these ventures right from start as highly risky. The result was the cryptocurrency crash in 2018 which reminded of the initial financial crisis of 2007-2008.

What are Tokens? The term token is used differently but in relation with cryptocurrencies it either describes the digital asset itself (e.g. Bitcoin is a cryptocurrency token) or is used as a unit value (token as unit or coin of a cryptocurrency).

4.4.2. DApps, Ethereum, Smart Contracts, Hyperledger

There is currently not yet a common definition for decentralised applications (DApps). Some definitions state DApps must be open-source, run on a blockchain and need to have a consensus mechanism (blockchainwelt.de, 2019) (hackernoon.com, 2019). A consensus mechanism involves having rewards for miners in the form of cryptographic tokens of value (e.g. bitcoin).

In 2015 Ethereum (ethereum.org, 2019) was launched, a programmable blockchain having a cryptocurrency called Ether (ETH). Ethereum introduced self-executing smart contracts which follow a set of agreed upon rules. Once the contract is live, these rules cannot change (Ethereum Explained, 2019). Smart contracts have applications (DApps), which are automatically executed if some conditions are met. By offering to create and use DApps, there is a broad spectrum of possible simple or complex transactions (e.g. registering property rights).

Hyperledger is currently one of the most interesting projects in the view of decentralised applications and smart contracts. Hyperledger is group of blockchain players for collaborative development of business blockchain technologies started and still under the Linux Foundation.

In contrast to Ethereum, Hyperledger uses permissioned blockchains. This means that the access is restricted, members are verified and registered so that some actions can only be performed by (certain) members. As a result, less power consuming consensus mechanisms can be applied and not all nodes are involved in e.g. validation.

Currently, five different Hyperledger frameworks are using smart contracts (hyperledger.org, 2019), each of them having a different focus:

1. Hyperledger Burrow is a permissionable smart contract machine
2. Hyperledger Fabric a distributed ledger focussing on facilitating transactions between enterprises while being highly flexible and scalable to be adaptable for any industry. Businesses can define the used asset type and value for a transaction. A group of participants can also create a separate ledger of transaction
3. Hyperledger Indy is a distributed ledger focussing on self-sovereign identities
4. Hyperledger Iroha is designed to be easily integrated into enterprise infrastructure projects
5. Hyperledger Sawtooth is a highly modular platform for building, deploying and running distributed ledgers for businesses

5. Use cases of ledger technology within a service platform

The use of new technologies is always a great chance for innovation or can add great value to the users or the product itself. But of course, not every new technology is suitable to be used without a detailed consideration. We will present possible use-cases for DLT within a service platform such as SimpliCITY and later explore and discuss challenges involved.

5.1. Use of distributed ledger technology (DLT) for a green city service platform

5.1.1. Authentication

Authentication is still one of the key parts for every application connected to any cloud features. Central solutions to authentication are a weak point and often a target for hackers. To avoid this design flaw decentralised solutions could have a great benefit.

But not only in the view of security, also in the view of privacy. With the help of the General Data Protection Regulation (GDPR) principles for “Self-Sovereign Identity” (SSI) are on the rise for popularity (github.com, 2019) (p2pfoundation.net, 2019). DLT based solutions for SSI are looking very promising.

Additionally, as even the European Union is in a fight to maintain its sovereignty again large corporations, it will be a very bad decision if we give such key features for our digital services into the hands of these corporations.

Broader seen is this use case not only very interesting for digital services. It will simplify identity administration for different services (passport, driver license, …) for states. One great example for this case is e-Estonia (https://e-estonia.com). Even if DLT has still unsolved topics conflicting to GDPR, Austria believes that SSI based on DLT would currently be the best possible solution to fulfil the requirements of GDPR (youtube.com, 2019).

So, let us now start to explore some of the interesting existing projects which are trying to solve the overall problems of central managed identities:

- **ID2020** (https://id2020.org)
  ID2020 is an alliance founded in 2014 (wikipedia.org, 2019). Their goal is that every human is able to prove one's identity – it's a fundamental human and universal human right (medium.com, 2019). ID2020 is trying to coordinate and channel different projects to create the pathway for an efficient and responsible implementation at scale (id2020.org, 2019). They are not focused on implementation work itself.

- **DIF** (http://identity.foundation)
  DIF is a young formation founded in 2017. In contrast to ID2020, DIF is focused on the engineering task to establish an open ecosystem for decentralized identity. They try to create they necessary open standards with inclusion of the big players in this field.

- **Hyperledger Indy** (https://www.hyperledger.org/projects/hyperledger-indy)
  Hyperledger Indy is a distributed ledger only designed for identity. A lot of Hyperledger Indy is based on the work of sovrin (https://sovrin.org) which is also sponsoring Hyperledger Indy. Hyperledger Indy seems to be one of the few projects with a great potential to be used right now.

- **Identity on top of the Stellar Network** (https://www.stellar.org)
  The Stellar Ecosystem Proposal (SEP 0010 - https://github.com/stellar/stellar-protocol/blob/master/ecosystem/sep-0010.md) seems very promising to be used to solve identity in web projects on top of the Stellar network. It seems as an implementation that could be realised with this protocol relatively easy.

- **RE:claimID** (www.aisec.fraunhofer.de/de/fields-of-expertise/projekte/reclaim.html)
  RE:claimID is not directly based on any DLT related project. It's based on the GNU Name System (GNS) a decentralised and censorship-resistant replacement for DNS. The downside of this project is it's under the copyright of the Fraunhofer AISEC Institute.

- **uport** (https://www.uport.me)
  Uport can be used to register a Uport ID on the Ethereum blockchain via the Uport mobile app. It's an already usable solution but can't be used independently without the use of the app.

These examples show that DLT based authentication is subject to active research and development worldwide and we see a great potential. Therefore, we would adopt one of the existing solutions for SimpliCITY.

5.1.2. Service listing

One task within the project is to get an overview and map the services within a city. This also needs a thorough selection process. For an information platform, like SimpliCITY, with aggregated services, it we see a benefit in basing the listing of services on a distributed ledger with a user vote consensus mechanism to decide which services gets listed and supported by the platform. This application of direct democracy provides its own challenges. How can people make an informed decision on services listed for approval? This could be circumvented by new forms of public consensus by ideas of liquid democracy or other concepts that enable individuals to shift their vote to an expert of their choice.

Adding such a feature could not only be very interesting for the citizens to take part in the decision process, but also to automate and curate the process and make the process more efficient for city managers and administrators of such a system as well.

5.1.3. Reward System

A reward system based on DLT with consensus based on smart contracts which for example reward user for participation in a survey, reward first 10 users or award user with the highest score. A reward is the same as a token or number of tokens. Such a system can motivate users to use service and be seen both as an inlet and outlet of tokens. This would potentially be very easy integrated on top of existing blockchain projects and just implementing this in the SimpliCITY architecture at a later stage.

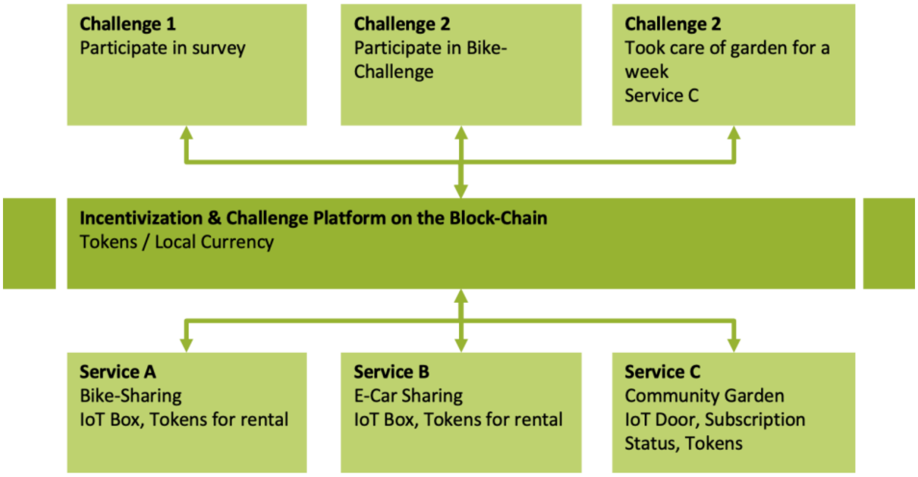

Challenge 1
Participate in survey
Challenge 2
Participate in Bike-Challenge
Challenge 2
Took care of garden for a week
Service C
Incentivization & Challenge Platform on the Block-Chain
Tokens / Local Currency
Service A
Bike-Sharing
IoT Box, Tokens for rental
Service B
E-Car Sharing
IoT Box, Tokens for rental
Service C
Community Garden
IoT Door, Subscription Status, Tokens

Figure 7: Incentivization architecture (Source: Layer-Wagner, 2019)

One issue in this use-case is the amount of transaction and the potential costs resulting from these transactions. Ethereum and Hyperledger-based architecture discuss solutions like state channel transaction that are running off-chain, to circumvent a large ammount of small transactions between two parties.

Regarding blockchain based reward system, we proposed a solution to motivate sustainable development with an incentive system. We suggested a decentralized distributed system that uses a blockchain database. The system is a network of nodes, each of which plays a role of a company or a citizen. Citizens can request the system to incentivize them with tokens. The tokens then can be used as vouchers to consume products and services in member companies. Taking the system requirements and the financial incentive model into consideration, the system under design is characterized by the following features:

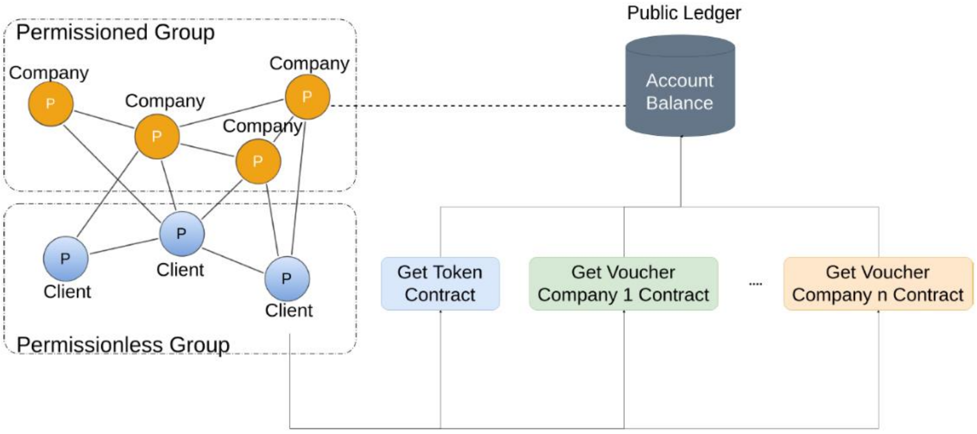


Figure 8: System architecture (Source: Layer-Wagner, 2019)

Access Control

The Blockchain network will consist of two groups with different access controls and privileges: permissionless (public) group and permissioned (private) group. The public group represents normal users (citizens) with limited power, where they can be free to join or leave. The members of this group can propose new transactions, but they can not participate in the consensus process. In contrast, the private group is intended to be used by companies, where they need permission to join the network. The members in the private group actively take part in the consensus process to maintain the network. The feature of access control in the network is desirable because companies in the network have a level of trust in each other but normal users are completely untrusted by the network.

Ledger

The distributed ledger needs to keep track of the account balance for each citizen in term of tokens. The number of tokens can increase when users request the system to incentivize them or decrease when users convert their tokens into vouchers. Users can interact with the public ledger via smart contracts.

Business Logic

In order to support the financial incentive model presented in the previous section, smart contracts will be used to implement the business logic in the system. The business logic is captured in two main areas:

- The system must define how many tokens users can earn for each request corresponding to each sustainable activity.
- Companies can define their own incentive policies.

5.1.4. IoT

The Internet-of-Things (IoT) provides valuable opportunity for development of smart cities through a wealth of urban environmental data. However, the centralized model of existing IoT systems has high maintenance cost. In addition, there is a justified lack of trust in the devices from the customer side. From the manufacturer's side, the current centralized model has a high maintenance cost – consider the distribution of software updates to millions of devices for years after they have been long discontinued. From the consumer's side, there is a justified lack of a trust in devices that ‘‘phone home’’ in the background and a need for a ‘‘security through transparency’’ approach.

These issues can be solved with a scalable, trustless peer-to-peer model that can operate transparently and distribute data securely, which are the key features of blockchain. However, there are some challenges when designing a blockchain based sustainable IoT system. One research direction is to explore energy-efficient solutions that address the consensus energy concerns, enable high scalability, and provide suitable business models. We identify and discuss several major problems in developing blockchain based sustainable IoT system for smart cities here.

Energy-efficient Consensus Mechanism

Consensus algorithm must be designed in blockchain to maintain a public ledger among trustless network. Proof of Work (PoW) is the most popular algorithm widely used in the blockchain area. However, PoW are controversial because of its massive energy consumption. In the IoT system including a lot of devices and sensors, it is not sustainable and environment-friendly to maintain such blockchain based IoT system. The alternative is Proof of Stake based on coinage. However, it is considered inappropriate to apply to IoT network because the major components are sensors. One important research direction is to investigate how to reduce the communication overhead and energy consumption of consensus.

High Scalability

Compared to a properly configured centralized database, a blockchain solution will generally underperform, resulting in lower transaction processing throughput and higher latencies. This problem is mainly blamed on the block size and the consensus algorithm. It will be interesting to analyze the functions of the block, modularize the separate functions and redesign the block structure to provide high scalability.

Novel Business Models

The Blockchain Based IoT System will facilitate the sharing of services and resources leading to the creation of a marketplace of services between devices. However, to make the ecosystem sustainable, business models have to be designed to meet the need of such unique market.

5.2. Challenges for green service platforms

Considering the use cases described above we will discuss the challenges involved that go beyond the technical implementation and feasibility for the usage of DLT.

Data Privacy

With the new General Data Protection Regulation (GDPR) data privacy got a big boost in its significance. The personal right to be forgotten is currently in contradiction with DLTs immutability. For now, there is not a common solution to this problem available. Concepts of zero-knowledge proof might provide an answer. The implementation zk-SNARK from Zcash looks for now very promising.

Nearly all existing blockchain projects use personally identifying information (PII). Even if this PIIs are strong obfuscated, they are still the weak point to track user’s behaviour. Hyperledger Indy for example is one of the first projects which is using pairwise “decentralized identifiers” (DIDs) in connection with zero-knowledge proof. With this technologies Hyperledger Indy seems like the perfect candidate to be in accordance with GDPR, if zero-knowledge can live up to our expectation. Additionally, Hyperledger Indy stores all PII related private data off-chain, which will only get exchanged in an encrypted peer-to-peer manner. This is not a unique feature of Hyperledger, but should exemplary show, how data privacy and GDPR conformation can be achieved in the auth.

We would welcome more research in this field very much, as it’s a blocking issue for any business working with EU citizen, whether the utilization of DLT is a good idea. The only available alternative is rethinking GDPR, which of course is out of scope for any business.

Environmental Sustainability

The proof of work protocol, one current implementation of a consensus protocol, is known to be quite hungry on computational power. It is widely known because is used in Bitcoin and its forks. From an environmental point of view a waste of energy resources is not sustainable, for a platform like SimpliCITY. Environmental sustainability is yet very underrated in the digital landscape. Most services which are sold as green services, are just buying green power without any further contribution to more sustainability. One very interesting project which is showing off this pain point very good is the solar-powered website “Low-tech Magazine” (https://solar.lowtechmagazine.com/about.html). This website will even go offline during long periods of cloudy weather.

There are manifold alternatives to the proof of work protocol and therefore the energy consumption running the platform should be taken into consideration. Ethereum, Hyper-Ledge or for example the Austrian blockchain solution 0bsnetwork use a non-proof-of-work approach like proof-of-stake. This is far more energy efficient, cost-effective and therefore scalable, but also guarantee fast transaction rates necessary for real-time applications.

Swapping the consensus algorithm helps to lower the energy consumption, but what should not be forgotten is that digitisation and exponential growth consume a lot of resources. So we should not only think about how we can lower consumption, but also how we could even avoid it.

Accessibility, ease of use and cost

For a platform to be widely adopted accessibility and user experience are key for citizens, city managers and service providers. There the question arises how potential users (citizens and city managers) would interact with DLT and what sort of client pre-requisites that might afford. The service providers, that want their services to be promoted, will be required to implement either the SimpliCITY API or directly implement their clients as decentralized applications (e.g. ĐApps in Ethereum) which is a question of effort and economic gain.

Implementation costs are one of the biggest in the field of software development. A comparison of the costs for certain implementations against common proofed existing solutions is an important thing in the view of economic success for software projects. But of course, the benefits of new implementations need to get balanced against the downsides of existing solutions. The implementation costs are hard to estimate and not foreseeable mainly due to non-existing projects with a similar scope and also very dependent on the service providers involved and their technical solution.

Trust, transparency and security

Trust and transparency are often named key benefits of DLT. Implementation of crypto currencies have proven the potential danger of certain implementations of core protocols. There are concerns of reverse transactions and double-spends by miners or miner groups owning 50% plus of hashing power in the network. These and issues regarding availability of services need to be overcome in the use-case of public city services. If such issues are resolved transparency make a huge impact on user behaviour. For example, in the case of donations, transparency has a direct positive effect on the willingness to donate.

5.3. Expert Feedback

In connection with activities in the SimpliCITY project we found several opportunities to present and discuss our ideas with experts in the industry. During the Industry Meets Makers (IMM) (see also deliverable 3.3), which is conceived as an open innovation community building format with focus on Austria we presented the SimpliCITY project to the participants and had first conversations about both the platform and on technology implementation details of the platform and a token and DLT solution. We presented the Reward system mentioned in 3.2. as “Token 4 Sustainable City Services”. The IMM events resulted in contacts with several start-up and SME companies focused on DLT technology and concepts.

Here we will present excerpts of related discussion:

- From a technical perspective a ‘Token 4 Sustainable City Services’ could be possibly integrated as a token system underneath SimpliCITY. The most crucial step would be to create a proof of concept for the gamification and incentive system that is able to be widely adopted by different services and systems. If these prerequisites are met, an expansion of SimpliCITY utilizing blockchain does not only seem possible but provide the benefit of an open platform and interface that the connected services could implement against.
- The work that is currently done on typical use cases like supply-chain management could be transferred for the topic of local production and consumption.
- The combination of IoT and blockchain offers opportunities regarding bike and e-bike sharing and tracking. With narrow band IoT the energy consumption can be drastically reduced and with a small footprint of the hardware can even be integrated into a bike’s frame.
- A token solution can also be leveraged for donations and voluntary work to have a transparent and open platform (see Fig. 7).

6. Conclusion

The utilisation of distributed ledger technology (DLT) for a service platform like SimpliCITY is overall feasible and creates opportunities for the future integration for city and 3rd party-based services. Especially a token system in connection with the gamification and incentivisation mechanisms of the platform is promising. Though a blockchain implementation sounds possible it is the gamification and incentivisation system that must prove sound and robust first.

For this approach to work, the incentivisation system must also by easy to understand not only from a user's perspective but also for companies. The process of e.g. participating in a challenge to receive tokens and being able to use token for e.g. renting an E-Car must be intuitive and straight forward. Further motivation might be promoted by displaying saved money values. Other challenges, as noted above, target topics like accessibility, cost and sustainability. Latter ones are in direct relation to system scalability and efficiency.

In our preliminary study, a blockchain based reward system is designed successfully to operate without the need for a trusted third party. All companies have an equal right and responsibility for maintaining and operating the network by themselves. The design fulfils almost all the requirements presented; however, it has some problems with the extensibility. The system is not effective when the number of companies is large. The design in this work is more suitable for a network with a small number of companies. In the future, we would like to improve the scalability and efficiency of the system, and further investigate novel business models.

References

Bieg, M. (2019, 07 31). Retrieved from https://commons.wikimedia.org/wiki/File:P2P-network.svg

blockchainwelt.de. (2019, 01 28). Retrieved from https://blockchainwelt.de/dapp-dezentralisierte-app-dapps/

BTC-ECHO. (2019, 07 31). Retrieved from https://www.btc-echo.de/ethereum-code-fuer-proof-of-stake-bis-ende-juni-fertiggestellt/

Chaum, D. (1983). *Blind signatures for untraceable payments.* In Advances in cryptology, pp. 199-203: Springer, Boston, MA,.

Chaum, D. (2003). *Untraceable electronic mail, return addresses and digital pseudonyms.* In Secure electronic voting, pp. 211-219.: Springer, Boston, MA.

Definition Of DECENTRALIZATION. (2019, 07 31). Retrieved from https://www.merriam-webster.com/dictionary/decentralization

Ethereum Explained. (2019, 07 31). Retrieved from https://www.upfolio.com/ultimate-ethereum-guide

ethereum.org. (2019, 07 30). Retrieved from https://www.ethereum.org/beginners/

europa.eu. (2019, 07 31). Retrieved from http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

github.com. (2019, 03 21). Retrieved from https://github.com/infominer33/DIDecentralized

Golosova, J. a. (2018). *The Advantages and Disadvantages of the Blockchain Technology.* p.1: IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE).

Golosova, J. a. (2018). *The Advantages and Disadvantages of the Blockchain Technology.* pp. 1-6: IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE).

hackernoon.com. (2019, 07 30). Retrieved from https://hackernoon.com/what-are-decentralized-applications-dapps-explained-with-examples-7ff8f2c4a460

hyperledger.org. (2019, 07 30). Retrieved from https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf

id2020.org. (2019, 03 21). Retrieved from https://id2020.org/overview

investopedia.com. (2019, 07 30). Retrieved from https://www.investopedia.com/terms/c/cryptocurrency.asp

J. Wild, M. A. (2015). *Technology: Banks seeks the key to blockchain*. Retrieved from https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64?segid=0100320#axzz3qK4rCVQP

Medium. (2019, 07 30). Retrieved from https://medium.com/@spsingh559/detail-analysis-of-raft-its-implementation-in-hyperledger-fabric-d269367a79c0

Medium. (2019, 07 31). Retrieved from The Meaning Of Decentralization: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

Medium. (2019, 07 31). Retrieved from https://medium.com/nakamo-to/what-is-proof-of-stake-pos-479a04581f3a

medium.com. (2019, 03 21). Retrieved from https://medium.com/id2020/our-manifesto-78c6969ca960

Natarajan, H., Krause, S. K., & Gradstein, H. L. (2017). *Distributed Ledger Technology (DLT) and blockchain*. Retrieved from http://documents.worldbank.org/curated/en/177911513714062215/Distributed-Ledger-Technology-DLT-and-blockchain

Natarajan, H., Krause, S. K., & Gradstein, H. L. (2017). *Distributed Ledger Technology (DLT) and blockchain*. Retrieved from http://documents.worldbank.org/curated/en/177911513714062215/Distributed-Ledger-Technology-DLT-and-blockchain

newyorker.com. (2019, 07 03). Retrieved from https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency

p2pfoundation.net. (2019, 01 21). Retrieved from https://wiki.p2pfoundation.net/Self-Sovereign_Identity

Snyder, B. (2019, 07 31). *Meet Vitalik Buterin*. Retrieved from The 23-Year-Old Founder Of Bitcoin Rival Ethereum: https://www.cnbc.com/2017/06/22/meet-vitalik-buterin-the-founder-of-bitcoin-rival-ethereum.html

Stanford Graduate School Of Business - Blockchain For Social Impact. (2019, 07 30). Retrieved from p.21: https://www.gsb.stanford.edu/faculty-research/publications/blockchain-social-impact

The Meaning Of Decentralization. (2019, 07 31). Retrieved from https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

theconversation.com. (2019, 01 28). Retrieved from https://theconversation.com/the-blockchain-does-not-eliminate-the-need-for-trust-86481

Toonstra, G. (2019, 07 31). *Distributed Hash Tables*. Retrieved from http://radialmind.blogspot.com/2009/09/distributed-hash-tables.html

twilio.com. (2019, 03 18). Retrieved from https://www.twilio.com/blog/what-is-public-key-cryptography

Washbourne, L. (2015). *A survey of P2P Network security.* p.2.

web.archive.org. (2019, 07 30). Retrieved from https://web.archive.org/web/20160813163512/http://www.trsllc.com/wp-content/uploads/2013/05/White_Paper_Bitcoin_101.pdf

wikipedia.org. (2019, 03 21). Retrieved from https://en.wikipedia.org/wiki/ID2020

wikipedia.org. (2019, 07 31). Retrieved from https://en.wikipedia.org/wiki/Distributed_hash_table

wikipedia.org. (2019, 03 19). Retrieved from https://en.wikipedia.org/wiki/Cryptocurrency

worldbank.org. (2019, 01 21). Retrieved from https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt

youtube.com. (2019, 03 22). Retrieved from https://www.youtube.com/watch?v=l5laRZfn8AI

Appendix

- Blockchain_Based_Innovation_Reward_System.pdf