Deliverable Proof – Report resulting from the finalisation of Deliverable 1 – Comparative Study of Blockchain Architectures

KIC project the report results from	*Blockchain Solution for Incentivising Low-Emission Transportation (LET-Chain)*
Name of report	Comparative Study on Blockchain Architectures
Date of report	31.12.2017

Supporting documents:

Relevant report

In corporation with

BLOCKCHAIN BÜRO

An initiative of

Climate-KIC is supported by the
EIT, a body of the European Union

31.12.2017

Comparative Study on Blockchain Architectures

Abstract

The goal of this part of the project was it to find a suitable blockchain architecture that will fulfill the needs of the LETchain: Offering a platform to develop a cryptocurrency that represents the incentive for sustainable transportation. The following rating criteria have been applied:

- Programmability
- Operating costs
- Security
- Trustability
- Usability

The following platforms have been taken into account: Bitcoin Colored Coins, Ethereum, NXT, IBM Hyperledger, Symbiont Distributed Ledger and RSK. These Blockchain Technologies were studied and rated in the process.

The study resulted in a clear winner: The Ethereum Blockchain stands out in its ability to be a platform for a self-made cryptocurrency. High usability, very low operation costs and a great degree of freedom to program in the Solidity language make the Ethereum platform a good tool.

Prelude

One aim of the LETChain project is it to develop a cryptocurrency token that can be used as an earmarked representative of incentives given to workforces that use a sustainable way of transportation to commute to their workplace. This offers the possibility to control the use of incentives and to trace the flow of mentioned tokens. The development and the operation of such a token will be based on an existing Blockchain Technology platform. The description and rating of existing platforms that come into question is the content of this paper.

Description of studied blockchains

BITCOIN COLORED COINS

Described in 2008 in the White Paper of Satoshi Nakamoto[1] and started in January 2009, Bitcoin is the incubator of Blockchain Technology. The first and oldest cryptocurrency was and is still used as a role model for many other Blockchain Projects in succession. It offers a protocol to transfer ownership of a token from one party to another that doesn't require trusted third parties to verify the right to do so. Bitcoin also offers the possibility to manage and represent real world assets. For this purpose the Bitcoin scripting language is used:

> «Bitcoin's scripting language allows to store small amounts of metadata on the blockchain, which can be used to represent asset manipulation instructions. For example, we can encode in a Bitcoin transaction that 100 units of a new asset were issued and are now credited to a given bitcoin address. A colored coins wallet can create a Bitcoin transaction that encodes sending 50 units of an asset from one address to a new address, and so on.»[2]

The script language is purposefully not Turing-complete with no loops. It is transmitted within a bitcoin transaction.[3] Informally spoken, calling a computer Turing complete

---

[1] https://bitcoin.org/bitcoin.pdf

[2] https://en.bitcoin.it/wiki/Colored_Coins

[3] https://en.bitcoin.it/wiki/Script

means that it can execute any algorithm. The tokens' real world value is attached to the tokens by the asset issuer's promise to redeem the tokens for services or goods.[4] The token issuer is therefore responsible for the link between colored coin and real world asset. An example for the use of colored coins would be the issuing of coupons such as Airline Miles.
Two types of peers in the Bitcoin Network are distinguished: Nodes to broadcast transactions and hold Blockchain data, and mines to verify transactions and store them into blocks. Bitcoin uses a proof-of-work consensus mechanism. This means miners must provide a proof-of-work that had to be done to verify a block. This proof can not be forged.

In January 2018, the bitcoin network counts ~10'000 nodes.[5] This number is relatively low as most of the wallet clients don't run full nodes (that save the full blockchain) anymore to save disk space on user's devices.
Blocktime: ~10 minutes

ETHEREUM

The need of a real distributed computing platform was first fulfilled by Ethereum in 2014. The Project is founded and guided by Vitalik Buterin. It's the oldest platform that can deal with a variety of Smart Contracts. These are contracts that «run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference».[6] Smart contracts are deterministic exchange mechanisms controlled by digital means that can carry out the direct transaction of value between untrusted agents.[7]
The Ethereum Virtual Machine (EVM) can execute Smart Contracts on a shared global infrastructure. They are treated as autonomous scripts or decentralized applications that are stored in the Ethereum Blockchain for later execution by the EVM. Instructions embedded in Ethereum contracts are paid for in ether (the token of the Ethereum Blockchain) and can be implemented in a variety of Turing-complete scripting languages. The many opportunities to interact with this Blockchain are to «create markets,

[4] https://en.bitcoin.it/wiki/Colored_Coins

[5] https://coin.dance/nodes

[6] https://www.ethereum.org

[7] Szabo, Nick (1997). "The Idea of Smart Contracts". Archived from the original on 2 May 2017.

store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract)»[8] or to create a cryptocurrency. This broad usability made Ethereum the Blockchain of choice for ICO (Initial Coin Offerings) in 2017 and gained a lot of publicity in the process. To write scripts or decentralized applications the programming language Solidity is used. After written, the Solidity code is compiled into bytecode that is executable on the EVM.
Ethereum currently uses a proof-of-work consensus. With its «Serenety» release, the network plans to switch from a hardware mining to virtual mining (proof-of-stake). If successfully executed, this switch will be a fundamental change to the Ethereum network and lower the power consumption drastically.
In January 2018 the Ethereum network counts ~34'000 nodes.
Blocktime: ~14 seconds

NXT

Established in 2013, NXT is a Blockchain platform that was was specifically conceived as a flexible platform on which to build applications and financial services.[9]

> «Nxt is an advanced blockchain platform which builds on and improves the basic functionality of pioneering cryptocurrencies such as Bitcoin. Cryptocurrency and financial systems are the first widely used applications of blockchain technology, but the blockchain and its associated technology can be used for so much more.» [10]

NXT uses a proof-of-stake consensus mechanism. This is the unique characteristic in comparison to other Blockchains. In it's White Paper, proof-of-stake is described as follows:

> «Nxt uses a system where each coin in an account can be thought of as a tiny mining rig. The more tokens that are held in the account, the greater the chance that account will earn the right to generate a block. The total

---

[8] https://www.ethereum.org

[9] "Nxt Wants to Be a Digital Infrastructure of Everything". *CoinTelegraph*. Retrieved 22 December 2014.

[10] https://nxtplatform.org

> reward received as a result of block generation is the sum of the transaction fees located within the block. Nxt does not generate any new tokens as a result of block creation.»[11]

All initial NXT tokens have been released to 73 entities through a one-time fundraiser via Bitcoin. Like in Ethereum it's possible to create new currencies within the NXT blockchain.

In January 2018, the NXT network runs on 355 nodes.[12]
Blocktime: ~1 minute

Latest developments: In January 2018 the ARDOR Project was launched. This second version of the NXT Blockchain (NXT 2.0) is a designated Cryptocurrency platform. It has a broad functionality and offers, among others, the following functionalities:

- Asset-Exchange
- Decentralized marketplace
- Alias-System
- Monetary System (sub-currencies)
- Datastorage (Data Cloud)
- Voting system
- Phasing (Multisignature)
- Account Control / Account Properties[13]

These functionalities would make it a considerable candidate for this project. The project started too late to be taken into account for this paper but will be watched in the future.

---

[11] «nxt whitepaper» http://nxtwiki.org/wiki/Whitepaper:Nxt

[12] https://www.peerexplorer.com

[13] https://bitcointalk.org/index.php?topic=1891452.0

HYPERLEDGER

Hyperledger is an open-source project which was founded in 2015 by a collaborative effort by the Linux foundation and several companies such as IBM or Google in order to support the implementation of the Blockchain Technology for global business transactions.[14] The goal is to create an open platform to share the framework, codes, the underlying technology and the idea freely via the Github platform. Hyperledger is not restricted to be the underlying technology of a cryptocurrency but is applicable to all sorts of ideas to make confidential secure transactions possible. Closely related to Hyperledger is the Hyperledger fabric, which is an implementation of a distributed ledger platform created by the Hyperledger project team of the Linux foundation which enables the running of smart contracts and implement related technologies[15]. The advantage lies within its modular architecture that allows for easy adjustments and implementation of further functions.

From the technological point of view, Hyperledger aims to be, through its modular approach as flexible as possible, which in turn attracts many different industries. The Hyperledger fabric distinguishes between two kinds of peers. A validating peer, which is a network node responsible for maintenance, transaction validation and consensus, and a non-validating peer, which is a node functioning as a proxy, which connects clients to validating peers. Moreover, three different types of transactions are defined within the protocol to enable companies a greater flexibility when setting up a Blockchain for their own purpose.[16]

Concluding it can be said that Hyperledger is an important tool for industries to gain knowledge about the Blockchain Technology and have access to a platform that strongly facilitates the implementation of new ideas.

---

[14] Cachin, C. (2016, July). Architecture of the Hyperledger Blockchain Fabric. *IBM Research – Zurich*. Retrieved from https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf

[15] Cachin, C. (2016, July). Architecture of the Hyperledger Blockchain Fabric. *IBM Research – Zurich*. Retrieved from https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf

[16] Cachin, C. (2016, July). Architecture of the Hyperledger Blockchain Fabric. *IBM Research – Zurich*. Retrieved from https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf

SYMBIONT DISTRIBUTED LEDGER

The distributed ledger solution of Symbiont seems to be in a very early stage. The website describes it as follows:

> «a blockchain platform for building networks in which multiple, independent entities may share data and logic in real time. It is a decentralized database that replicates and executes application logic in the form of smart contracts. This platform may be used to create financial instruments–such as loans and securities–in a digital form from their inception. Assembly was purpose-built to meet the standards of institutional finance in security, reliability and performance.»[17]

The third party SDK for this Blockchain is still under construction, therefore no testing or programming activities can take place. Due to the absence of a White Paper, no further insights into the technology could be gained.
Symbiont Distributed Ledger will be left out of this comparison.

RSK

> «RSK is an Ethereum-like sidechain to Bitcoin that intends to launch before the end of the year (2017). The initial version of the sidechain will be mostly controlled by a federation of well-known Bitcoin companies, but the plan is to further decentralize the platform by giving more control to bitcoin miners over time.» [18]

According to its White Paper it combines three aspects:

- A Turing-complete resource-accounted deterministic virtual machine (for Smart Contracts)
- A two-way pegged Bitcoin sidechain (for BTC denominated trade)

---

[17] https://symbiont.io/technology/

[18] https://www.coindesk.com/bitcoin-startup-rsk-launch-smart-contracts-sidechain-2017/

- A dynamic hybrid merge-mining/federated consensus protocol (for consensus security), and a low-latency network (for fast payments).[19]

RSK aims to be a Smart Contract platform that incorporates a Turing-complete Virtual Machine to Bitcoin. It works as a Bitcoin sidechain. This means, RSK has no own token but Bitcoin (BTC) can be transferred to the RSK Blockchain and become «Smart Bitcoin» (SBTC). They are equivalent to Bitcoin and can be transferred back with no additional costs, except for RSK transaction fees.[20] RSK has an unusual governance system whereby the parties and stakeholders of the network obtain votes depending on their role.

> «RSK allows the creation of crypto-assets (or altcoins) secured by the Bitcoin network. Given RSK's flexibility to price the contract's fuel these application (as all others) could be used from students to banks and corporations.»[21]

In January 2018, the RSK network consists of 20 nodes. This number is very low due to the project's early maturity level.
Blocktime: ~10 seconds

---

[19] RSK Whitepaper, https://uploads.strikinglycdn.com/files/ec5278f8-218c-407a-af3c-ab71a910246d/RSK%20White%20Paper%20-%20Overview.pdf

[20] RSK Whitepaper, https://uploads.strikinglycdn.com/files/ec5278f8-218c-407a-af3c-ab71a910246d/RSK%20White%20Paper%20-%20Overview.pdf

[21] RSK Whitepaper, https://uploads.strikinglycdn.com/files/ec5278f8-218c-407a-af3c-ab71a910246d/RSK%20White%20Paper%20-%20Overview.pdf

Rating according to the predefined criteria of studied blockchains

DESCRIPTION OF THE RATING CRITERIAS

The following section will be dealing with a rating of the researched Blockchain Technologies. The rating refers to usability in this project. I've come up with five criteria to estimate how suitable a specific technology is. *Programmability*: What is the degree of freedom one has in programming this Blockchain? Is it close to «Turing-completeness»? Is there an SDK or another development environment? *Operation costs*: What are the costs to run this blockchain. This criteria could have basically only applied to Hyperledger. In the cases studied, this was the only Technology in which a fee was charged. *Security*: How to classify security is not trivial. In the studied Technologies two extremes were found: on one side the permissioned network of IBM, where all access can be controlled. This is a closed Blockchain architecture with which only dedicated parties can interact with the Technology. This minimizes the risk of malicious peers trying to manipulate the network beyond it's foreseen use case. On the other side there is Ethereum/Solidity that has a high complexity and therefore a high risk of holding exploits or bugs that have not yet been found. Where other Blockchains have a limited way to interact and therefore a smaller attack surface, Ethereum's versatility comes at a price. It has to be said that Ethereum stands out in this discussion because of its widespread distribution. Many users on a Blockchain also means that the probability that bugs are found is higher. Blockchains with a lower distribution like NXT, or moreso, RSK don't have enough scale to prove their resilience against attacks. *Trustability*: Another criteria that combines several factors. What does governance look like? Who writes code? How distributed is the network? How is consensus reached? *Usability*, finally, expresses a general appraisal about how frictionless it would be to work with the given Blockchain Technology. Documentation, support and distribution play a role in this category.

Each category is rated with a number (1-5) in which 1 is poor and 5 is ideal. In the following matrix, those numbers are represented by colors:

RATING MATRIX

	Programmability	Operation costs	Security	Trustability	Usability	Score
Bitcoin Colored Coins	Limitied due to lack of Turing completeness					**19**
Ethereum			Presence of attack vectors due to high complexity	Centralized governance	Lots of resources and documentation	**21**
NXT				Badly distributed	Well documented but not widely used	**19**
Hyperledger		High monthly fees	Permissioned Network	Permissioned Network		**19**
RSK	Unknown	Unknown	Unknown			**6**

Tab 1: Rating matrix

COMMENTS ON THE RATING

The Ethereum Blockchain stands out for it's ability as a platform for a self-made cryptocurrency. High usability, very low operation costs and a great degree of freedom to program in the Solidity language make the Ethereum platform a good tool. This opinion has been confirmed during the last year by thousands of ICO (Initial Coin Offerings) choosing Ethereum as a weapon of choice to generate an own coin or manufacture tokens that represent a share of their companies. It offers a low entry-level to program a cryptocurrency and can be operated at very low costs.

Bitcoin Colored Coins, NXT and Hyperledger share the second position in this rating.

The main drawback on Bitcoin Colored Coins, responsible for the minus points in usability, is the lack of being a «full» framework that can execute most algorithms.
NXT, on the other hand, has this ability but lacks in distribution. Only a few hundred nodes and and a bad distribution of NXT coins made a dent in its rating.

Hyperledger is a mighty platform and usable for a broad variety of use cases. This makes it not ideal for this special case in generating a local currency. Infrastructure costs, monthly fees and a steep learning curve are non ideal aspects for a proof-of-concept that is aimed in this LETchain project. Put in simpler terms, Hyperledger would be an overkill for the project in its current state. If the proof-of-concept is successful and the team decides to take the project further, Hyperledger should be considered again as it offers a lot of advantages for a closed, mighty and scalable infrastructure.
With only 20 nodes RSK is a too small, too young a project. It lacks of substance that can be evaluated.