

Is it possible to develop a real-Time practical decentralized application to help to the decision of business Process?

Fatemeh Heshmati¹, Lansana Sangare ², Abderrazzak Aarab³, Mohammed Alaa eddine Cherni⁴, Nestor Patient Tchamba Sefekme⁵

Institute of Computer Science

Hochschule Ruhr West, University of Applied Sciences

Bottrop, Germany

Abstract

The blockchain is a cryptocurrency technology known as a public ledger to which everyone has access but without a central authority having control. This technology allows not only individual person but also companies to collaborate with trust and transparency. The integration smart contract with blockchain cause reduce the cost and provide high security. The most known application of the blockchains are the cryptographic currencies such as bitcoin and recently a new technology emerged for the building of Internet-based apps called decentralized applications (DApps). Depending on the functionality of the DApp, different data structures are used to store application data. For example, WAVES is a decentralized blockchain platform focusing on custom blockchain tokens operations. In this article, we developed a platform to back up the data in the Waves blockchain and use them later for decision making. And then the method and implementation of this platform are explained.

Key word: Blockchain, Smart Contract, Waves, DApp

1 Introduction

Considering the capabilities of the blockchain and smart contract technology many companies today use the both in their company process. A smart contract is basically a computer program that runs and executed on blockchain Network and after blockchain technology many applications came to the surface a smart contract is one major application of this technology (Mohanta, Panda, & Jena, 2018)..

Waves Platform is an open-source Blockchain platform allowing users to build applications, create and distribute new cryptocurrencies. The platform is also like crowdfund. This platform is decentralized. Crypto fan can use waves Platform to create customized tokens and transfer digital assets on the Blockchain¹.

The present Article is divided into 7 chapters including this introduction. The second chapter explains the current state of art. The next chapter describes the architecture implementation of our web platform. The conclusive results are presented in the chapter Evaluation, which will be discussed below. Lastly, we explain about the future of Blockchain technology.

2 Related Work

2.1 Smart Contract

In 1994 Nick Szabo first introduced the Concept of a Smart Contract (szabo, 1997) which is basically a computer program that runs and executed in blockchain network and after the rise of the Blockchain technology in the last decade many applications came to the surface a Smart contract is one major application of this technology (Mohanta, Panda, & Jena, 2018) .“A *Smart contract is a computer program that takes the form of a digital contract and consists of a Value, address, function, state*” (Mohanta, Panda, & Jena, 2018) as well as exact details and terms found in any form of physical contract . It provides many advantages for both parties of the contract or transaction. One major advantage is the high security and trust provides within the application². The characteristics of a

¹ <https://cryptodigestnews.com/what-you-should-know-about-waves-platform>

² <https://www.cognizant.com/whitepapers/blockchains-smart-contracts-driving-the-next-wave-of-innovation-across-manufacturing-value-chains-codex2113.pdf>, [June 2016]

Smart contract are (Mohanta, Panda, & Jena, 2018): Machine readable code run on blockchain platform and part of one application program. The advantage of smart contract in comparison of ordinary transactions is that who do not know each other and who do not trust each other can transaction together. Considering the smart contract capabilities, all commercial, service and production platforms can be completely transformed into the smart contracts because transactions are made more efficient, safer and cheaper through smart contracts. Smart contracts are suitable for currencies like Ether, Bitcoin and Lif. In the future, smart contracts could be used in the most industry, such as finance, logistics and insurance industry³.

2.2 Blockchain

A blockchain is a software mechanism that is used to create a decentralized Application. All transactions made by users are saved in the Blockchain. Each block contains a hash of previous block, which creates a chain of blocks associated with each other. Blockchain has an automated structure and creates security in the software, which prevents fraud (Prusty, 2017). At present, advanced technology companies have their own blockchain projects, and this trend is increasing. For example, companies such as IBM, Microsoft and Samsung (Bahga, 2016) have their own blockchain projects. Blockchain protocols are open-source, therefore, anyone can use a similar or slightly modified version (Müller-Bloch et al., 2017a). Blockchain is shared on networked computers called nodes and if one node deceitfully its version of the blockchain changed, that version will be changed by other nodes (Müller-Bloch et al., 2017b). In Network, nodes are confirmed using the proof-of-work algorithm. Then the transactions are bundled into blocks and they must be accredited to be added to the blockchain (Müller-Bloch et al., 2017c).

2.3 DApp

A DApp is an open source application whose backend runs on a decentralized peer-to-peer

network and source. Depending on the functionality of the DApp, different data structures are used to store application data. For example, the Bitcoin DApp uses the blockchain data structure. There is no central server in DApp to coordinate the peers and decide what is right and wrong (Prusty, 2017). To solve this challenge there are certain protocols (specifically called consensus protocols). Consensus protocols are designed specifically for the type of data structure that DApp utilises. For example, Bitcoin employs the proof-of-work protocol to achieve consensus (Prusty, 2017)s. Every DApp requires a client for the user to use the DApp. For that, a node in the network is required. The Nodes of a DApp provide an API only and give the ability to the developers to develop many clients using the API (Prusty, 2017). Clients of DApps need to be open source and need to be downloaded for use; otherwise, the concept of decentralization will fail. DApps account cannot have the same username- and password-based functionality like centralized applications because passwords cannot determine that the data change for an account has been requested by the owner. There are quite a few ways to implement user accounts in DApps. The most popular way is employing a public-private key pair. The hash of the public key is the unique identifier of the account. To make a change to the account's data, the user should sign the change with the use of his/her private key. Users need to keep their private keys safely. Users will lose access to their account forever, if they lose their private keys⁴.

3 Architecture

3.1 Structure

A web platform is developed in this Article using Visual Studio (Write Code), Terminal (Run), testnet (Test) and NodeJs (For Build & Configure). These should constitute the basis for creating a fast and convenient platform for the development and delivery of a software project. All developers can apply code together, fix and deduce the work in a group project.

³ <https://blog.qsc.de/2018/09/blockchain-welche-vorteile-bieten-smart-contracts/>, [24.09.2018]

⁴ Prusty, N., (April 2017):” building Blockchain Projects”, Birmingham, UK, www.packtpub.com, ISBN 978-1-7812-214-7,

After that, after the code has been executed, the web platform is available, which serves to decide on the best option within a business process. The customer dimension has been implemented with JavaScript und will interact with the NodeJs layer, server dimension. The customer rating was implemented to allow the user to enter data that will be recorded in our database (**Blockchain**). In the blockchain it exists a simple data structure (like database). Data are managed as a transaction in individual, chronologically linked blocks. The data are stored in the blockchain, secured against manipulation. In general, Blockchain is a solution that brings together various "best practices" in computer science, especially in the areas of cryptography and peer-2-peer networks. As the name implies, Blockchain is a chain of records known as blocks. In the middle of a transaction, data is structured as key-value pairs. Keys are non-empty UTF-8 strings and are case-sensitive. Four data types are supported: Boolean, Integer, String, and Byte Array. Each value is assigned a data type. For values, a one-byte type code is first written indicating the value type. Then the value is encoded as follows:

```
"Data": [{"key":"string","type":"string","val ue":"Hallo"}]
```

3.2 Use case

The behaviour of a system is indicated by a use case from the user's point of view. A function or set of actions is determined by a use case worked out by a system that is relevant to an actor. Suitable use cases for the business process includes creating new questions, creating options, choosing options, creating criteria, and evaluating criteria. With an include relationship, a use case is included in another use case. It is a compelling relationship and is characterized as a "must-have relationship". An extend relationship is an optional relationship and is therefore often referred to an "optional relationship". The property of an existing or planned system with simple models is illustrated by use case. The user is a role, a person, an organization or another system. He acts as an actor interacting with a system to

achieve a specific goal in a defined sequence of actions. The name of the use case results from the target⁵. Below is the use-case of the current project specific goal in a defined sequence of actions.

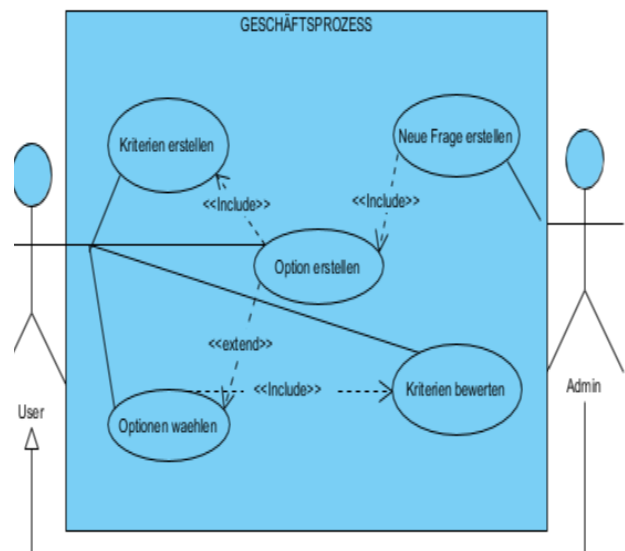


Figure 1: Use Case

4 Implementation

4.1 Practical Implementation

This paragraph defines the implementation of the system:

Structure: The implementation was implemented through JavaScript. Both JavaScript, HTML Framework and CSS Style were used as frontend here. The waves-transactions, waves-api, by Waves were used too. In addition, the NodeJs was installed under Windows.

Login-Admin: The admin uses a string from Keyboard (like seed). The smart contract is working to verify the public Key of the admins before the transaction is validated. If the seed entered from Keyboard matches one of the user existing in the smart contract, then they can save the data transaction containing the question in the blockchain and can be redirected to the next page where options are created, otherwise the redirect fails and there is no data storage in blockchain. After the script is assigned to the account, the project is sent to the

⁵ <https://www.t2informatik.de/wissen-kompakt/use-case>

Blockchain, this happens to block or check the sending of data from the project account. The admin can still additionally create options like the user.

Login-User: Each user individually applies unique seed. If the seed to be entered does not match one of the user in smart contract, it will result in a bad page, otherwise the user can create options, criteria and save them in blockchain. The smartcontract verifies the user's correctness of the publickey before the transaction is validated and completed. It is enough if only one of the users has a correct signature. This will be forwarded to the menu where criteria are located.

Insert Data into Blockchain: The data will be described in a special format when entered in the option, criteria or evaluation fields sent together in a field as JSON objects through the WAVES-TRANSACTIONS_API to the Blockchain.

4.2 Waves

"Waves is an open source blockchain platform that allows the users to launch and release their own Cryptocurrency tokens" (chohan, 2018). The Waves Blockchain is the starting point for the Waves Client and everything that works on Waves. Waves uses "plug-ins" to introduce new types of transactions, instead of attaching token transactions to regular blockchain transactions. These plug-ins are generated on the core software to use these transactions. This plug-in must be set up by the user. Through this system and the ability to create custom tokens, the Waves blockchain can execute a custom token against another custom token. Basically, therefore, tokenizing and trading assets in the blockchain is possible.⁶

4.3 Ride

RIDE is a blockchain scripting language that grants "intelligent" blockchain transactions. The result of the execution is based on a certain logic, realized with the help of RIDE scripts and made available in the blockchain. The purpose

of the RIDE architecture is to create a native on-chain computing layer that is as close as possible to the general blockchain architecture (full data synchronization)⁷. A smart contract should be written applying the ride language. RIDE language has this characteristic that makes it harmless, effective and precise: Non-Turing Complete lazy, Strong typed, statically typed expression-based language, no cycle and recursion capability compared to solidity. RIDE may be complete in composition with a blockchain Turing, since the blockchain is theoretically infinitely long⁸.

5 Evaluation

The generated software project is now being examined with a small web application. The web application was implemented in NodeJS and consists of several graphical user interfaces which after filling in the field store the option or criteria information in the blockchain. Starting point of this example application is a testnet/wavesexplorer in which all necessary data are stored. After all fields (Options or Criteria) are filled in, a script was written in JavaScript that reads all data stored in Blockchain and all mathematical calculations for each option, then it decided which option is best (maximum of calculated options). The result of the best option calculated on the platform is displayed.

$$\text{Option_weight} = \sum_{i=0}^n BK^{(i)} * E^{(i)}$$

(Equation 1)

$BK^{(i)}$ is the evaluation of the i-th criterion und $E^{(i)}$ ist die i-th connexion

6 Conclusions

It was shown in this paper that a decision can be made on the basis of various options or criteria concerning a business process in a web platform.

Different user interfaces were used for the interaction. We have designed for the rating a small self-written web application named "server.js".

⁶Tehmoonwalker(Jul 21, 2018)

<https://medium.com/@tehMoonwalker/all-you-need-to-know-about-waves-7a07556e13d8c>

⁷ <https://blog.wavesplatform.com/waves-dapps-roadmap-for-2019-dc481445439c>

⁸ <https://docs.wavesplatform.com/en/smart-contracts/ride-language/ride-language.html>

At the end of the process, one could be able through the website result, which shows the best option after complete calculation over all options and criteria, to make a decision.

7 Outlook & Future

For many major industries, politics and individuals, Blockchain technology has significant implications for the future. It is not a phenomenon that the big companies secure their place in the Blockchain industry. And DApp, one of the key applications of the blockchain, is bringing more and more interesting applications of blockchain. During work, an employee can be paid in real time with a demanding contract. Programs can easily track keystrokes, recognize that they do not play around on Facebook, and measure the wealth of ideas. Then company pay in real time during the work. This is a positive aspect for both the company and the employee. Many companies already use services like Upwork. These services make the monitoring of the work of remote employees in real time. It is easy to duplicate this and just change the payment system⁹. Blockchain could be a great tool to get a lot of important documents in industries like Logistics, copyright and many others to save. Blockchain could make an intermediary superfluous when it comes to the legalization of contracts. Smart contract platforms are still being completed when it comes to usability and are expected to be used vigorously over the next 5 years¹⁰.

References

1. Mohanta, B.K., Panda, S.S., Jena, D., (July 2018): “*An overview of smart contract and use case in blockchain technology*”, Bengaluru, India
2. Cognizant, (2016):” *Block chain’s smart contract: Driving the next wave of Innovation across Manufacturing Value chains* “. <https://www.cognizant.com/whitepapers/block-chains-smart-contracts-driving-the-next-waves-of-innovation-across-manufacturing-value-chain-codex2113.pdf> (2017).
3. Chohan, U.W., (March 2018): “*The Waves platform and the Dissemination of new Cryptocurrencies*”, University of new south Wales, Canberra
4. Prusty, N., (April 2017):” *building Blockchain Projects*”, Birmingham, UK, www.packtpub.com, ISBN 978-1-7812-214-7,
5. <https://www.wavesplatform.com>
6. Tehmoonwalker, (Jul 21, 2018) <https://medium.com/@tehMoonwalker/all-you-need-to-know-about-waves-7a07556e13d8>
8. T2informatik, <https://www.t2informatik.de/wissen-kompakt/use-case>, Berlin
9. Naerland, K., Müller-Bloch, C., Beck, R., Palmund, S., (December 2017): „*Blockchain to rule the waves-Nascent Design principles for Reducing Risk and uncertainty in Decentralized Environments*”
10. Nick Szabo (1997): “*the idea of smart contract*”
11. Calvin Christopher., (2018): „*8 Experts on the future of Blockchain Technology & Applications*”, <https://www.newgenapps.com/blog/future-of-blockchain-technology-applications>
12. <https://blog.qsc.de/2018/09/blockchain-welche-vorteile-bieten-smart-contracts/>
13. <https://blog.wavesplatform.com/waves-dapps-roadmap-for-2019-dc481445439c>
14. <https://docs.wavesplatform.com/en/smart-contracts/ride-language/ride-language.html>
15. <https://cryptodigestnews.com/what-you-should-know-about-waves-platform>

⁹ <https://www.newgenapps.com/blog/future-of-blockchain-technology-applications>

¹⁰ <https://www.newgenapps.com/blog/future-of-blockchain-technology-applications>