

Blockchain for government fund tracking using Hyperledger

Apoorva Mohite
Department of Computer Science and Engineering
KLS, Gogte Institute of Technology
Belgaum, India
apps.mohite@gmail.com

Ajay Acharya
Department of Computer Science and Engineering
KLS, Gogte Institute of Technology
Belgaum, India
aacharya@git.edu

Abstract— Blockchain is one of the technology that has created a disruptive change in many industries. Currently, Blockchain is being used in several places and there are many more applications of Blockchain yet to be discovered and implemented. Blockchain is characterized by its decentralized nature, integrity of the data stored in the chain and its openness. Due to these characteristics, another place where Blockchain can be used is to release government funds for a project. Usually when a project is allocated funds, there is no knowledge as to how these funds are being used and a large part of it is never shown in records due to corruption. To solve this problem, a system has been proposed using Blockchain to provide the transparency. This paper also gives a description about a prototype which was developed using Hyperledger Composer. It then discusses the future development of this prototype and finally, concludes with the applicability of Blockchain.

Keywords— Blockchain, Hyperledger Composer

I. INTRODUCTION

Today the world is getting digital in all aspects. Blockchain technology is an upcoming technology and said to be one of the most promising technologies which would revolutionize the world. These days blockchains are being used in Supply chains, Identity management, Cross-border payments, Cryptocurrencies and many more places. [1] Blockchain finds a wide range of applications, this is mostly due to its characteristics. Some of the most important characteristics of blockchain include its decentralized nature, transparency, consistency and security of data, immutability, non-corruptibility, low cost and speed. The use of blockchain in Government sector can cause radical changes in the administration and management. It can reduce corruption by providing transparency in every transaction. [2]

In this paper we will be discussing the basics and applicability of blockchain in different domains. More particularly, this paper discusses the use of blockchain technology for tracking the government funds. When the government issues funds for projects, often a large part of it is unutilized and is barely used for the actual project, one of the main cause being corruption. So, if blockchains are introduced here, everyone can track all the amount regarding when and where it is being utilized. This

technology being utilized in the government sector, can have a major impact on the growth and economy of a country. This is especially true in case of developing countries where there is lack of transparency. Thus, tracking of government funds, in a way would reduce corruption.

In the next section we give a brief introduction to Blockchain technology and then a brief description of our proposed system with respect to its working. In the fourth section we have given a description of our prototype for this application of the Blockchain. And finally, we discuss about the future scope of this application and the Blockchain.

II. BLOCKCHAIN

Blockchain was discovered by Satoshi Nakamoto in his paper “Bitcoin: A Peer-to-Peer Electronic Cash System” which was the foundation for the blockchain based bitcoin cryptocurrency. [3] Wikipedia defines blockchain as “A blockchain is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data”. [4] This system is based on the concept of a decentralized ledger which is shared between all the nodes in a network. A transaction is represented as a block which has a hash value and a hash value of the previous block. Every transaction is verified by the peer network. When a transaction is carried out, the block is linked to the previous block using its hash value. This mechanism ensures that integrity of the data is maintained.

Some of the major applications of blockchain are cryptocurrencies and smart contracts. A cryptocurrency is a digital asset as a medium of exchange using cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets. [5] Blockchain-based smart contracts are proposed contracts that could be partially or fully executed or enforced without human interaction. [4] These are some of the popular uses of blockchain. In the next section, we apply the concept of blockchain for fund releasing as discussed earlier.

III. PROPOSED SYSTEM

In the context of government fund releasing, trust in an intermediary and on the transactions that are made is necessary. Therefore, we can implement the fund release system using a blockchain.^[6] Below is a basic block diagram of how the blockchain will work here. The transaction here is paying the supplier to buy raw materials for the project.

The process basically starts with a transaction. This transaction is represented by a block. This block contains details of the transaction like the amount, the payer, the payee and the purpose of the transaction along with a transaction ID.

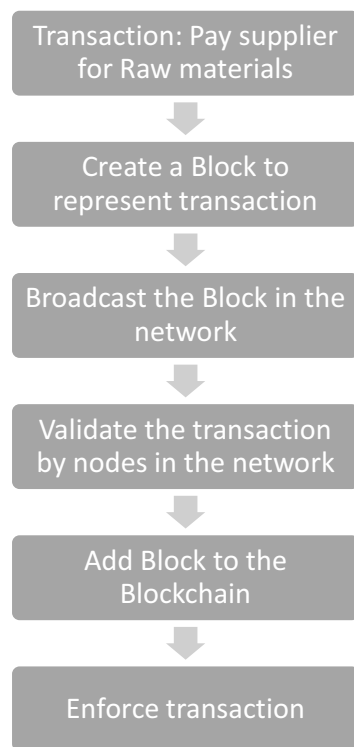


Fig 1: Blockchain Process

Now a block containing the information mentioned, is broadcasted into the network. The nodes (people in real) involved in the network, validate the transaction. After this validation, the block along with a timestamp is added to the blockchain. The transaction can then be enforced. All of the transactions thus submitted will be recorded in the decentralized ledger and will be visible to everyone publicly.

IV. PROTOTYPE

A prototype was implemented for this system using the Hyperledger Composer from the Linux Foundation. Hyperledger Composer set of collaboration tools for building blockchain business networks to create blockchain applications for business problems. It is a rapid prototyping tool, running on top of Hyperledger Fabric.^[7]

Hyperledger Composer uses a modelling language called CTO. It has a user interface called playground which is used for creating and testing our prototype.^[8] We can define our assets, participants, transactions and access control. The logic behind transactions is written in JavaScript as a transaction processor function. The resources that must be defined are Asset, Participant and Transaction.^[9]

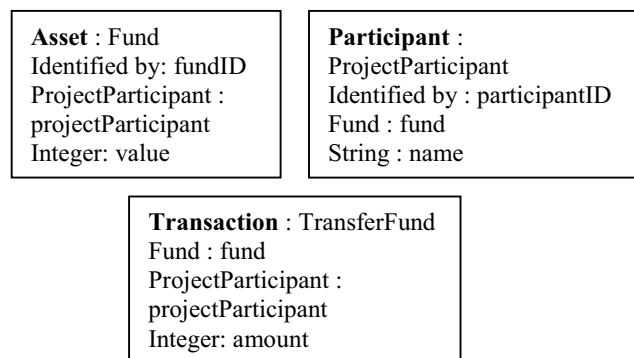


Fig 2: Prototype Model

In this context, the asset is Fund, participants are the people involved in the project, here ProjectParticipant and transaction is paying money for different commodities required for the project, here FundTransaction. We have an initial Total Fund from which other funds are withdrawn by project participants. Each of the participant has a relationship of Fund. An asset (Fund) is created for every participant. The transaction processor function is called every time a FundTransaction is submitted. The function is passed a transaction instance which specifies the involved participant and the amount of fund to be transferred. If the transaction parameters satisfy all the constraints, the transaction is ledged in the registry. This transaction entry also contains a transaction ID along with a timestamp when the transaction was submitted. The logic here is straightforward. Whenever a transaction is submitted, the specified amount of funds is withdrawn from the total fund. The assets registry and participants registry are updated after the submission, so that the data is consistent.

The prototype was tested in the Hyperledger playground by submitting two transactions. Two participants Ali and Bob and three

Assets, Total fund (value=1000), fund available with Ali (value=0) and Bob (value=0) were instantiated. One transaction was by participant Ali who withdrew 500 from the Total fund. In the other transaction Bob withdrew 250 from Ali. This withdrawal can be analogous to a contractor withdrawing money from the total and a supplier being paid from the contractor.

Thus, all the transactions made can be clearly visible to anyone and everyone publicly. There can be many improvements made to this model like the access control, users and so on which will be discussed later.

```

1  {
2    "$class": "org.example.basic.FundTransaction",
3    "fund": "resource:org.example.basic.Fund#total",
4    "projectParticipant":
5      "resource:org.example.basic.ProjectParticipant#ali",
6    "purpose": "Contract for design"
7    "amount": 500
8  }

```

Fig 3: Screenshot of a transaction to be submitted

Date, Time	Entry Type	Participant	
2018-10-19, 10:42:36	FundTransaction	admin (NetworkAdmin)	view record
2018-10-19, 10:42:06	FundTransaction	admin (NetworkAdmin)	view record
2018-10-19, 10:38:36	UpdateAsset	admin (NetworkAdmin)	view record

Fig 4: Transaction registry after submitting transaction

```

1  {
2    "$class": "org.example.basic.FundTransaction",
3    "fund": "resource:org.example.basic.Fund#total",
4    "projectParticipant":
5      "resource:org.example.basic.ProjectParticipant#ali",
6    "amount": 500,
7    "transactionId": "e3b98b16-ddd6-45b7-a741-af16007f6a6b",
8    "timestamp": "2018-10-19T05:12:06.893Z"
9  }

```

Fig 5: Historian record with transactionID and timestamp

ID	Data	
aliFund	<pre> { "\$class": "org.example.basic.Fund", "fundId": "aliFund", "owner": "resource:org.example.basic.ProjectParticipant#ali", "value": 250 } </pre>	 
bobFund	<pre> { "\$class": "org.example.basic.Fund", "fundId": "bobFund", "owner": "resource:org.example.basic.ProjectParticipant#ali", "value": 250 } </pre>	 
total	<pre> { "\$class": "org.example.basic.Fund", "fundId": "total", "value": 500 } </pre>	 

Fig 6: Screenshot of the asset registry after transaction

V. FUTURE WORK

Since this is a bare minimum prototype of a blockchain application developed using Hyperledger Composer, there is a lot of scope for further improvement in this. In this sense we can control the access to the resources by the participants. Any transaction to be submitted can be made to verify digitally. This model can be exported as a .bna (Business Network Archive) file and run on the Hyperledger Fabric on the cloud where the blockchain would be stored. Further we can generate a REST interface and a GUI for interaction. ^[4] We can come up with a policy where the wallet address of the people involved in the project is made public, which will make it very easy to trace the route of the fund. ^[2] This can then be put to use in a real-world situation like the government fund releasing as mentioned earlier.

VI. CONCLUSION

The Hyperledger Composer tool allows us to rapidly prototype blockchain applications by defining a business model and deploying it on the Hyperledger fabric.

While we considered about building blockchain applications, we even have to consider the access and privacy challenges though. Even then, with further enhancements, this blockchain model can provide a transparency in all the government transactions. There will be no discrepancies of any kind. Because of the decentralized ledger all the transactions can be verified and cannot be altered. The money that is released can be tracked, anyone and everyone can find out how the money is being used. Such a blockchain will surely reduce the ongoing

corruption. It will create a huge impact on the economic development of a country.

Finally, blockchain technology has a huge potential. Storing data across a peer-to-peer network, the blockchain removes a number of risks that come with data being held centrally. As the definition of blockchain states that every block has a cryptographic hash of the previous block, it confirms the integrity of the previous block all the way to the starting block. ^[5] Thus, the blockchain technology has the power to disrupt many such industries requiring transparency.

VII. REFERENCES

- [1] Massimo Di Pierro, "What Is the Blockchain?"; Computing in Science & Engineering, Issue No. 05 - September/October (2017 vol. 19) pp: 92-95.
- [2] Toshendra Kumar Sharma (2018). "HOW CAN BLOCKCHAIN REDUCE CORRUPTION?" [Online] Available: <https://www.blockchain-council.org/blockchain/how-can-blockchain-reduce-corruption/>
- [3] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", <https://bitcoin.org/bitcoin.pdf>
- [4] Wikipedia, "Blockchain", <https://en.wikipedia.org/wiki/Blockchain>
- [5] Wikipedia, "Cryptocurrency", <https://en.wikipedia.org/wiki/Cryptocurrency>
- [6] Gideon Greenspan (2015). "Avoiding the pointless blockchain project" [Online] Available: <https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/>
- [7] Wikipedia, "Hyperledger", <https://en.wikipedia.org/wiki/Hyperledger>
- [8] Hyperledger, "AboutHyperledger", <https://www.hyperledger.org/about>.
- [9] J Steven Perry (2017). [Online] Available: <https://www.ibm.com/developerworks/cloud/library/cl-model-test-your-blockchain-network-with-hyperledger-composer-playground/index.html>