A Survey on Blockchain for Enabling Transparency in transactions of Government Direct Benefit Transfers (DBT)

Mansi Borole
Computer Engineering
Pune Vidyarthi Griha's College of Engineering and Technology
Pune, India

Abhishek Nilange
Computer Engineering
Pune Vidyarthi Griha's College of Engineering and Technology
Pune, India

Karan Velhal
Computer Engineering
Pune Vidyarthi Griha's College of Engineering and Technology
Pune, India

Tanmay Joshi
Computer Engineering
Pune Vidyarthi Griha's College of Engineering and Technology
Pune, India

ABSTRACT
Blockchain has a great potential in distributed shared peer to peer ledger like spreadsheets that record any transaction. A copy of ledger is shared between all stakeholders. Blockchain plays an important role for secure decentralization and brings more transparency to the system. Traditionally, within the society, people have created trust through intermediaries. They use these third party entities because they trust that they will store and protect their goods and send the right amount when they request it, and to the right person. In Government sector, there is a critical need to have more transparency in transactions and so this system has been designed as an effective mechanism to avoid the corruption. Blockchain technology provides the transparency so that actors present in this use case can track the flow of any transaction. Any transaction pertaining to DBT (Direct Benefit Transfer) is recorded. Blockchain replaces the need for intermediaries by redirecting the trust to decentralized systems.

General Terms
Blockchain

Keywords
Blockchain, Distributed Ledger Technology, Transparency, Hyperledger, Cryptography

1. INTRODUCTION
In current scenario, Indian Government provides scholarship to minority students who cannot afford to pay their University fee. Students have to fill out forms in order to be eligible for the scholarship. The government's scholarship fund is then transferred to the student's bank account whose application has been approved. The amount disbursed might vary from student to student depending on their caste/category or the minority they belong to. Another way in which the fee is disbursed by the government is in fractions. Consider, for example, an OBC (Backward Class) category student pays 50% amount of his fees to the college and the college awaits the remainder 50% fee from the government scholarship department. For the college to retrieve its remaining 50% fees, it has to file its entire summed up amount of all registered candidates and pass the bill to the scholarship department. The scholarship department is branched upon the districts and states in India. The scholarship amount is returned to the college from treasury via scholarship department. Currently, the treasury amount is not distributed evenly to all the institutes. Some colleges do not get their entire scholarship amount although the government has passed the funds causing the system to become less transparent and giving a way to various forms of corruption and delay inconveniences for the college. The colleges might have to bribe the scholarship department officers get their pending fees cleared. Also, students don't have information about their scholarship transactions in detail.To curb this menace, we propose a new method to perform transactions related to Direct Benefit Transfers (such as Scholarship retrieval from government) to be done with the assistance of blockchain. This system will be able to track all fee deposit transactions for each and every student would be receiving a scholarship form the Government of India. Using platforms like Ethereum or Hyperledger blockchain to maintain a ledger of all the verified and valid transactions.

2. PROBLEM STATEMENT
Due to non-transparent and untimely disbursement of Direct Benefit Transfers (DBT) by the government, there is a need to make the system more transparent to ensure that there is equal distribution to institutions and/or individuals. This gives a way to blockchain technology as it promises to radically transform the way individuals and companies exchange of digital assets and track transactions securely. Its distributed nature guarantees the persistence of the ledger data. Its public key crypto-system offers the capabilities for a user to sign transactions that transfer.

3. LITERATURE SURVEY

3.1 Blockchain fundamentals
Blockchain technology emerged in 2008 as a core component of the bitcoin cryptocurrency (Bhardwaj and Kaushik, 2018). Blockchains provide transactional, distributed ledger functionality that can operate without the need for a centralized, trusted authority. Ledger recorded updates are immutable and cryptographic time stamping affords serial recording. The robust, decentralized functionality of blockchains is very attractive for use with global financial systems but can easily be expanded to contracts or operations such as tracking of the global supply chain. Three papers from the 1960s established specific principles that subsequently materialized in the blockchain concept. Thus, Haberand Stornetta (1991) described how to use crypto-signatures to time-stamp documents; Ross Anderson (1996) proposed a decentralized storage system from which recorded updates could not be deleted; and Schneier and Kelsey (1998) described how to encrypt sensitive information in order to protect log files on untrusted machines.

A blockchain is essentially a distributed database of records in the form of encrypted "blocks" (smaller datasets), or a public ledger of all transactions or digital events that have been executed and shared among participating parties, and can be

verified at any time in the future. Each transaction in the public ledger is verified by consensus of a majority of participants in the system. Once entered, information can never be erased. The blockchain contains a certain, verifiable record of every single transaction ever made and its blocks can be used to coordinate an action or verify an event. This is accomplished without compromising the privacy of the digital assets or parties involved. In order to prevent third party sources such as banks, governs or social networks from being hacked, manipulated or compromised, this technology uses mathematical problems that require substantial computational power to solve (Nakomoto, 2009)[1].

This protective measure makes it harder for potential attackers to corrupt a shared database with false information unless the attacker owns most of the computational power of the overall network. Consensus within the network is achieved through different voting mechanisms; the most common of which requires certain computers on the network, colloquially referred as "miners", to solve a computationally intensive mathematical problem, and other computers to verify that the solution to the problem does not correspond to a previous transaction. This mechanism is called "Proof of Work". Every computer(node) in the network stores a copy of the blockchain, and the nodes are periodically synchronized to ensure that all are sharing the same database. In this way, blockchain protocols ensure that transactions are valid and never recorded to the shared repository more than once; thus enabling people to coordinate individual transactions in a decentralized manner without the need to rely on a trusted authority to verify all transactions (Bonneau et al., 2015; Wright and De Filippi, 2017). Bitcoin is the most popular example intrinsically tied to blockchain technology. However, the blockchain concept can be applied to any online repository where a certain trusted authority is needed (Crosby et al., 2016).

Across ecosystems, business model changes enabled by blockchain technology can bring strengthened trust and transparency, and a new link to value exchange. Whether it is individuals seeking to complete transactions involving many parties, or enterprises collaborating across multiple organizational silos —wherever any documents or transactions must be confirmed, settled, exchanged, signed or validated—, there are usually frictions that can be avoided by using blockchain technology to unlock greater economic value. One of the greatest challenges in implementing a blockchain system is its usual complexity (Iansiti and Lakhani, 2017). Thus, all stakeholders in the chain must collaborate to adopt and implement the technology in order to make it fruitful. Because blockchain technology is still at an incipient stage of development, there is a general lack of standards for implementation. A blockchain should be universal and adaptable to specific situations (**Hyperledger**, 2016, 2017).[2]

3.2 Security in Blockchain

Hash

The hash function is a mathematical algorithm that takes any data as an input and generates a hash value as an output (value with a certain number of digits). The function generates completely different hash even if the input data is slightly changed. It is difficult to revert the original data by having the hash value only. This hash function is used in Blockchain for hashing the transaction message, and it is also used for the consensus algorithm such as Proof-of-Work. Miners need this algorithm to generate a hash value of all the transactions that is under a specific threshold.[3]

Public-Key Cryptography:

Public-key cryptography uses public and private keys for encryption and decryption of messages. The sender can use the receiver's public key to encrypt the message, and only the receiver can decrypt the message using the private key (Nakamoto, 2008). This mechanism eliminates the need to share the keys between parties to encrypt and decrypt the message, known as symmetric-key cryptography. The public private keys are also used for the digital signature.

Digital Signature

The cryptographic digital signature is used to prove authenticity of the data using the public-private key pairs. In digital signature, the sender encrypts the hash of the message using his/her private key, which then can be sent to the receiver along with the message. The receiver in this case also generates the hash value of the original message, and the authenticity can be verified against the hash value generated from decrypting the hash values that was sent by the sender using his/her public key

3.3 Consensus

Synchronized Records The blockchain maintains a single history of blocks using the consensus algorithms, which synchronize the records within the Blockchain to ensure blocks do not contain contradicting/invalid transactions. The consensus is known as mining in Bitcoin. There are multiple consensus algorithms used for Blockchain depending on its type and applications, this section discusses Proof-of-work and Proof-of-Stake.

Proof-of-Work (PoW)

Proof of Work (PoW) is a mechanism to approve the distribution of ledger where it is used to confirm a block creation in Bitcoin. The block is created after the successful generation of a hash value for a set of transactions from the unconfirmed transactions pool with a nonce. Nonce is arbitrary number, like a counter, that is used at most once within a session [4]. The participants in the network shall guess the nonce in order to be able to get a hash value that is smaller than a certain value set by the network. The network adjusts this value with the required level of complexity to keep the average processing time to 10 minutes. All network participants confirm and validate the block once a participant obtain the hash value, and the used transactions are at this stage are considered confirmed transactions. The participant that guessed the nonce value and created the block gets rewards of bitcoins. The use of PoW proves that significant effort is spent in creating new blocks to prevent forgery of data, and it prevents double spending of bitcoins, and it makes modifications of confirmed transactions impossible.[5]

Proof of Stake (PoS)

Proof of Stake (PoS) is a consensus algorithm alternative to PoW, in which the created block is chosen based on the wealth of the participant, hence the name Proof of Stake is given. The selection of the participant is based on the randomized block selection or the coin age based selection [6]. In the randomized block selection, the selection is predicted in a random manner using a formula that uses the stack size (publicly known) and the lowest hash value. In the coin age based selection, the selection is based on the age of the coin in which participants holding coins for more than 30 days can start trying to sign a block. This selection method also uses the randomized block selection. Compared to PoW, it was shown that PoS has lower latency, requires less

computational power, wastes fewer resources, and improves security for smaller chains [7].

4. BLOCKCHAIN IN DBT

All stakeholders involved the DBT (Government, banks, students, colleges) are driven by a need to make transparent transactions. Blockchain simplifies this challenging task by providing for one-to-many data integration and process orchestration among participants. This in turn facilitates establishment of a data structure that can be used by smart contracts to automate assertions, certifications and market operations.

There are three elements to explain why DBT can benefit from the blockchain concept:

4.1 Transparency

Transparency will no doubt be of future value, especially in connection with sustainability and the environment. Although one can use a centralized system to be transparent simply by disclosing information, blockchain technology is superior in this respect.

The strength of blockchain transparency lies in trust; thus, no transaction can be changed or manipulated after it has been recorded —with a centralized system, outsiders cannot assess the trustworthiness of disclosed information. The idea behind blockchain technology is that, once data have been chronologically stored and verified, they cannot be manipulated without altering the entire history of the blockchain.

4.2 Efficiency

Smart contracts are instructions that interface with the blockchain protocol in order to automatically evaluate and possibly post transactions in the blockchain. Similarly, smart libraries are specialized sets of blockchain-aware functionality that can be used locally or privately, or shared and licensed to other blockchain participants and agents. All participants come together in the blockchain, can evaluate the assertions made, and notify their account holders when matches in quality, timing, quantity, etc., are found.

4.3 Security and safety

Blockchains can also be used to issue and manage the creation of unique cryptographic tokens. The strategy around the issuance of these crypto-tokens, which need not be implemented in the initial system, is still being defined, however.

In other words, once a transaction is made it is irreversible. This is one other advantage of blockchain technology over centralized systems in terms of trustworthiness. Blockchains can be of help to address social concerns(corruption). This is a result of blockchain technology supporting traceability and transparency, which can be further strengthened by integrating smart contracts.

5. BLOCKCHAIN DEVELOPMENT PLATFORM

5.1 Hyperledger

The Hyperledger Project (www.hyperledger.org) is a collaborative effort to create an enterprise-grade, open-source distributed ledger framework and code base. It aims to advance blockchain technology by identifying and realizing a cross-industry open standard platform for distributed ledgers, which can transform the way business transactions are conducted globally. Established as a project of the Linux Foundation in early 2016, the Hyperledger Project currently has more than 50 members.

5.2 Hyperledger Fabric

Hyperledger Fabric (github.com/hyperledger/fabric) is an implementation of a distributed ledger platform for running smart contracts, leveraging familiar and proven technologies, with a modular architecture allowing pluggable implementations of various functions. The distributed ledger protocol of the fabric is run by peers. The fabric distinguishes between two kinds of peers: A validating peer is a node on the network responsible for running consensus, validating transactions, and maintaining the ledger. On the other hand, a non-validating peer is a node that functions as a proxy to connect clients (issuing transactions) to validating peers. A non-validating peer does not execute transactions but it may verify them.

5.3 Architecture

The validating peers run a BFT consensus protocol for executing a replicated state machine that accepts three types of transactions as operations:

1. **Deploy transaction**: Takes a chaincode (representing a smart contract) written in Go as a parameter; the chaincode is installed on the peers and ready to be invoked.
2. **Invoke transaction**: Invokes a transaction of a particular chaincode that has been installed earlier through a deploy transaction; the arguments are specific to the type of transaction; the chaincode executes the transaction, may read and write entries in its state accordingly, and indicates whether it succeeded or failed.
3. **Query transaction**: Returns an entry of the state directly from reading the peer's persistent state; this may not ensure linearizability. Each chaincode may define its own persistent entries in the state. [8]

The blockchain's hash chain is computed over the executed transactions and the resulting persistent state. Validation of transactions occurs through the replicated execution of the chaincode and given the fault assumption underlying BFT consensus, i.e., that among the n validating peers at most $f < n/3$ may "lie" and behave arbitrarily, but all others execute the chaincode correctly. When executed on top of PBFT consensus, it is important that chaincode transactions are deterministic, otherwise the state of the peers might diverge. Membership among the validating nodes running BFT consensus is currently static and the setup requires manual intervention. Support for dynamically changing the set of nodes running consensus is planned for a future version. As the fabric implements a permissioned ledger, it contains a security infrastructure for authentication and authorization. It supports enrollment and transaction authorization through public-key certificates, and confidentiality for chaincode realized through in-band encryption.

More precisely, for connecting to the network every peer needs to obtain an enrollment certificate from an enrollment CA that is part of the membership services. It authorizes a peer to connect to the network and to acquire transaction certificates, which are needed to submit transactions. Transaction certificates are issued by a transaction CA and support pseudonymous authorization for the peers submitting transactions, in the sense that multiple transaction certificates issued to the same peer (that is, to the same enrollment certificate) cannot be linked with each other.

Unlike Bitcoin and Ethereum, Hyperledger Fabric does not have any cryptocurrency, where the access to the network is restricted to the network members only, and not anyone can join the network. The transactions are controlled in Hyperledger Fabric using chaincode (smart contract), which is a program code that provides the ability to write and design the applications to interact with the network. The privacy of the transactions between the participant in the network can be obtained using an isolation mechanism known as channel. The channel ensures that the transaction and data are available only to the nodes that are members in the channel.

According to the official documentation of Hyperledger Fabric, a transaction is an invoke or an instantiate request that is submitted by the peer for ordering and validation.

The instantiate request initializes a chaincode in a particular channel, while the invoke transactions execute read/write operation on the ledger.[9]

6. Developing A Conceptual Blockchain Application

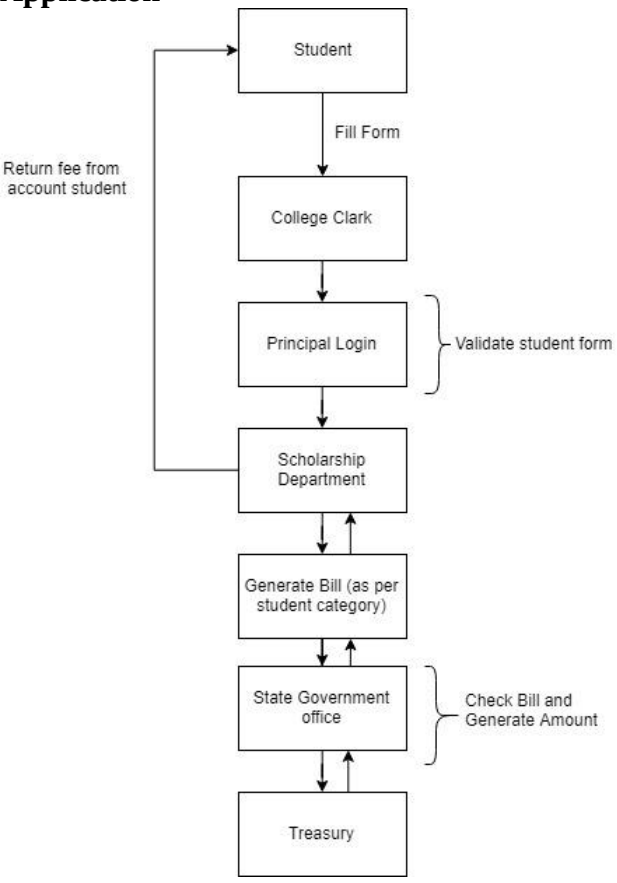

Figure 1: Normal procedure for Fee Disbursement

To develop a solution first a study of current work flow of fee disbursement is conducted as shown in Fig 1. A student fills and submits the form with all documents. Then college clerk will check all the documents verify and validate it and send it for next verification. College principal is going to check and finally send it to social welfare center then social welfare center generates the total bill and submit it to state government office then it will sanction the bill and give an order to a treasury department for distributing the scholarship fairly.

Main aspects of the required system are as follows:

Web Interface:
Client Side Interface: clients use this interface to interact with system and read get required result.

DB Module:
DB is used to store all personal information about clients. And clients can perform Add/Update/Delete/Modify operations on documents.

Blockchain Interaction:
Blockchain is used to record transactions. Ethereum is used as a platform and performing transaction related operations securely.

Document Verification:
It is used to sign client documents using cryptographic algorithms.

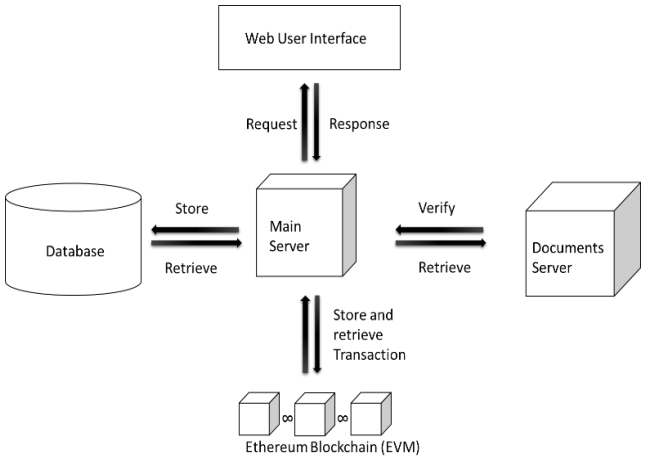

Figure 1: System Architecture

Use case diagram for fair distribution of the scholarship system is shown in Fig 3.

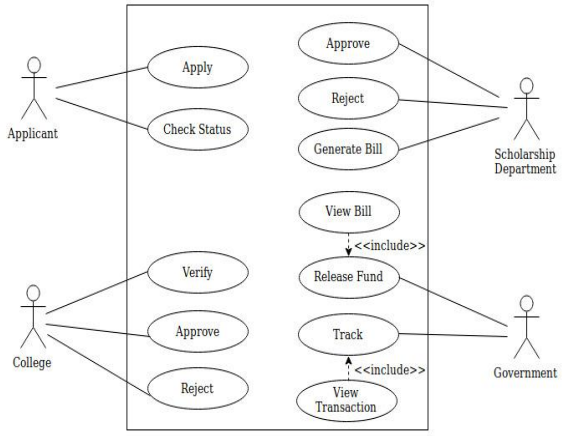

Figure 4: Use Case Diagram

Description of actors in the scene:
Applicant: Can apply, fill & submit the form as well as check the status of next verification.
College clerk: Can verify and validate forms which were applied by the applicant as well as form is approved and rejected by college clerk

Social welfare center (Scholarship dept.):
a form is approved & rejected by this department after verifying all documents. finally, the total bill is generated.

Government + treasury dept
The generated bill is viewed by this department and according to that fund is released and after releasing it, a transaction is tracked by this department.Sequence diagram for fair distribution of the scholarship system is as follows:

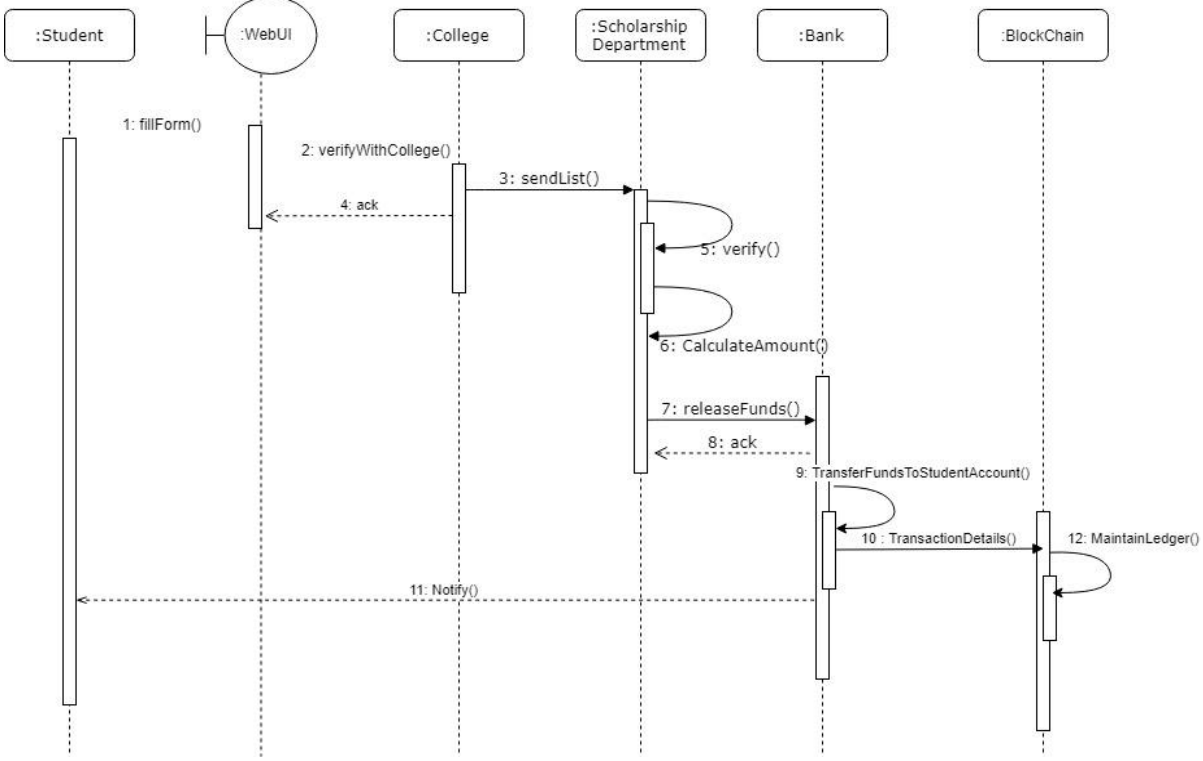

Figure 5: Sequence Diagram

7. CONCLUSION

Blockchain has been the subject of intensive research lately and in this paper a solution is proposed that uses blockchain to a major problem faced by Indian administration. Hyperledger Fabric was found to be the best fit for development of this use-case as it gives us high customizability, private network and confidential transactions

8. ACKNOWLEDGEMENT

We are grateful to Chaitanya Kulkarni and Sagar Deshmukh for their kind support. Their valuable time and suggestions were very helpful. We would like to take this opportunity to also thank my internal guide Prof. A. M. Bhadgale for giving me all the help and guidance that was needed.

9. REFERENCES

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”

[2] Paneljuan F, Galvezaj.C, Mejutobj, Simal-Gandara , “Future Challenges on the use of Blockchain for Food Tracability Analysis”

[3] Pilkington, Marc. (2016). Blockchain Technology: Principles and Applications.

[4] P. Rogaway, "Nonce-Based Symmetric Encryption," in International Workshop on Fast Software Encryption, Delhi, India, 2004.

[5] J. Mattila, "The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures," ETLA Working Papers, 2016

[6] Sunny King, Scott Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake" 2012.

[7] P. Rogaway, "Nonce-Based Symmetric Encryption," in International Workshop on Fast Software Encryption, Delhi, India, 2004

[8] Christian Cachin, “Architecture of the Hyperledger Blockchain Fabric” IBM Research - Zurich CH-8803 Ruschlikon, Switzerland, July 2016.

[9] “Hyperledger Fabric Project,” https://hyperledger-fabric.readthedocs.io/en/release/