# Application of Blockchain to prevent benami transactions

Abhishek S Patil
Department of Electronics and Communication
JSS Science and Technology University (formerly SJCE)
Mysuru, India
abhishekspatil92@gmail.com

Bharath S
Department of Electronics and Communication
JSS Science and Technology University (formerly SJCE)
Mysuru, India
sbharath534@gmail.com

*Abstract*— **Blockchain is a decentralized, distributed ledger which is immutable. Ledger is a collection of transactions which are immutable i.e. once created cannot be updated. It is one of the ways to remove the central Servers or third parties. The third parties facilitate the (interactions) transactions between two different parties which can be eliminated by Blockchain. It provides high level of security since the transactions remain anonymous. This technology can be used in different areas and one of them is in real estate industry to avoid benami transactions. This paper will give the outline or an idea of the underlining concepts about this new technology and the different ways it can be used in real estate industry.**

***Keywords— Blockchain, decentralize, immutable, ledger, benami transaction.***

## I. Introduction

Blockchain technology is a distributed ledger technology which acts as a data structure. The value of each block is referred by the block prior to them. After creating the Blockchain and the information is fed, it is not possible to tamper the network and fetch the details since it is shared to all the members across the network. All the users in a Blockchain are aware of all the transactions that take place. A Blockchain contains blocks, wherein every block is the successor of the previous block. It uses the nonce and signature of the previous block as a key to go forward to the next block. A digital signature plays a major role as the transactions are broadcasted across the public network. As the public network is not safe and the details can be easily tampered, the digital signature contains a signing phase and a verification phase to prevent fraud using private key and public key. The private key is a confidential key which is known only to the user to sign the transactions and the public key is known to all the users. The Blockchain is categorized into private, public and federated. In public Blockchain every one can read and write data to the ledger. Anyone can be part of it. Private Blockchain is company specific. Only authorized users can access the Blockchain. Federated Blockchain is for a group of people or companies and only those people have the authority to access. Figure 1 represents the basic flow of Blockchain wherein it contains a genesis block which is the first block that contains the genesis transaction details and the very first hash value. This block is referred as i-1th Block. The second block i.e. the ith Block contains transaction details and the hash value of the previous block i.e. the genesis block. The third block is referred as i+1th Block, which is the consecutive block containing the transaction details and the previous hash value. Sequence of blocks is constructed in the similar manner to form a Blockchain. A Blockchain can contain only one genesis block. The size of the block and size of each transaction is used to determine the maximum number of transaction that a block can contain within itself.

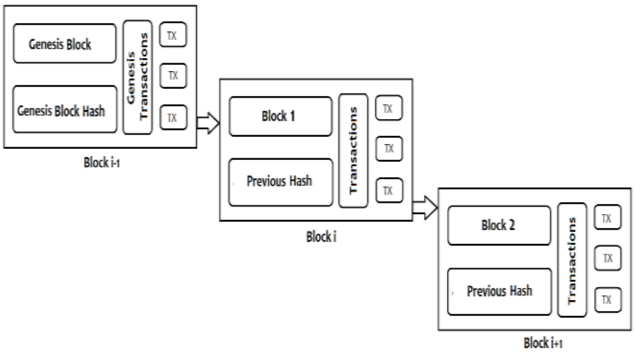

Fig 1: Block diagram of Blockchain

The term “Benami” basically means “without a name”. According to The Benami Transaction Prohibition Act, 1988, which is currently known as Benami Transaction Prohibition Amendment Act, 2016 (the “ACT”) “Benami transaction” is defined as an act of transaction or arrangement of property. The property will be transferred to a person but the payment for such a property is done by another person. This is done for future benefit of the person who paid for the property. It can also be a transaction carried by a fictitious name, or a transaction where the owner is unaware of the property or denies it. It can also be a transaction where the person who pays money is not traceable or uses a fictitious name. Real estate sector in India is expected to reach US$ 650 billion and its share in India’s Gross Domestic Product (GDP) is projected increase to 17 per cent by 2040. A lot of such benami transactions take place in real estate sector. A number of benami transactions acts were introduced to prevent the benami transactions. Digitalization was also implemented. But none could give a stop to benami transactions which hinders the growth of Indian Economy. This paper provides a solution to eradicate benami transactions. The main objective is to implement this architecture into real estate industry where all the transactions will be transparent and secure. The implementation of Blockchain will eliminate the benami transactions and thus improves the Indian Economy.

## II. Literature Survey

The paper [1] mentions different technologies that are emerging with the Blockchain as base such as, colored coins are the protocols which permit other digital assets to be transferred in the Blockchain but not Bitcoin itself by using Bitcoin as tokens. Another example is the alternative Blockchain wherein we can shift the Bitcoin of a particular Blockchain to a new Blockchain. There is a new Blockchain called the Ethereum Blockchain which is carried out by a set of contracts called the smart contracts which are nothing but a deal between the client and the receiver. Further they have explained the working of Blockchain and given a statistics on how fast the Blockchain industry is growing by studying the upward trend where there are a lot of research papers on Blockchain being written.

The paper [3] depicts the different areas where there should be more security and privacy in certain areas of Blockchain like the smart contracts etc., they have also discussed about different companies who have increased security through certain schemes. On a whole all the aspects of security and privacy for Blockchain and crypto currencies are being highlighted in this paper

## III. Methodology

### *3.1 Data collection*

The main of the paper is to eliminate the benami transactions which exist in the current Indian market. Blockchain technology is used to achieve this. The entire process can be divided into two phases. One of the phases is associated with collecting details regarding seller. A decentralized application is the core system. The seller will be asked to enter his details. The details to be entered are name of the person who owns the property, property details such as area in square feet, location and Identity proof of the owner. If the property details are entered for the first time it will be stored in a new block in Blockchain. If the Blockchain already has the information regarding the property then it will be used to verify the entered details. If the validation stage is successful it enters the next part called amount decision. A suitable amount will be decided according to the location and many other factors. An ID will be generated for each of the selling property. The entire information regarding the property can be fetched using the ID. The block diagram of the entire process is shown in figure 2. The method of storing the required user documents and addition of new Blockchain are explained in the upcoming sections. Smart Contracts are the method by which it is possible to add new Blockchain. Blockchain is a distributed network in which information is spread across many users rather than storing in single central server. Corrupting the information or modifying the information could be avoided. It requires 51% of the total computing power to change or modify any previously stored data. Hence the information stored in Blockchain is secure. Proof of Work or Proof of Stake are the two main algorithms which decide on who adds new Blockchain to the list. Proof of Work is based on the computing power where as Proof of Stake is based on the total investment in the list.

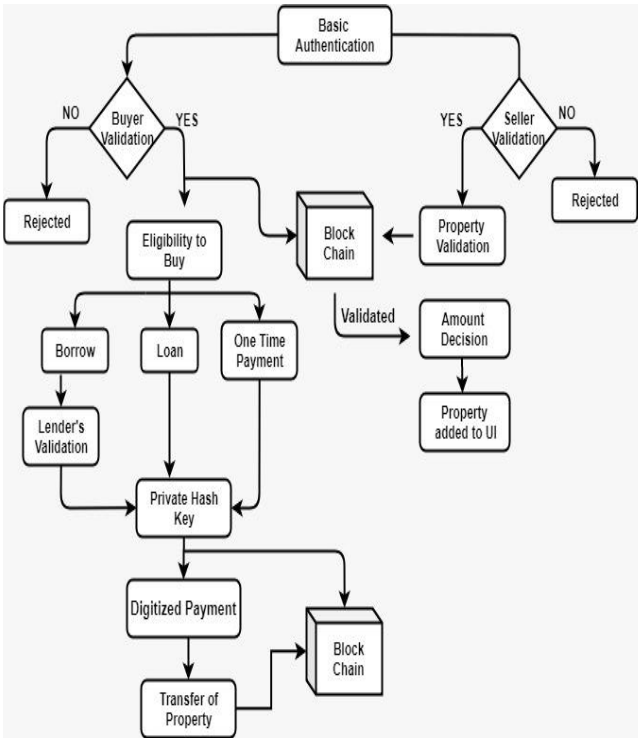

Fig 2: Flow diagram of the entire process

### *3.2 Buyer validation*

The next import phase in the entire process is the buyer validation. It forms the core of the system. It concludes many things such as whether the person is alive or not, his ability to buy certain property and so on. As shown in the figure first step is validating the buyer. Buyer will be asked to enter details such as name, properties under his name, source of income and identity proof if he is buying for the first time else the details already saved in Blockchain will be used and upgraded. The source of income is the key parameter. Only financially strong people can buy the property. The basic three modes of achieving this capability is either by his income which reflects as his bank balance or borrow money from a financially strong person who may be a friend or relative of the buyer or getting a loan from any Financial organization. Each and every method has to be verified in its own way. Since source of income has to be entered by the buyer an average bank balance could be calculated. Hence it could be calculated whether a person with a job with ‘x’ lakhs per annum could afford to buy a property worth ‘y’ lakhs after working for certain years. Since he submits his identity proof like Aadhar his bank balance could be found out. Suppose if the buyer wishes to borrow amount from a financially strong person the details of the money lender has to be entered. All the details such as source of income, properties under his name identity proof will be collected. It then follows same procedure as mentioned above to validate the money lender. Another possibility is that the buyer takes loan from any financial organization. Then the loan details have to be entered in order to buy the property.

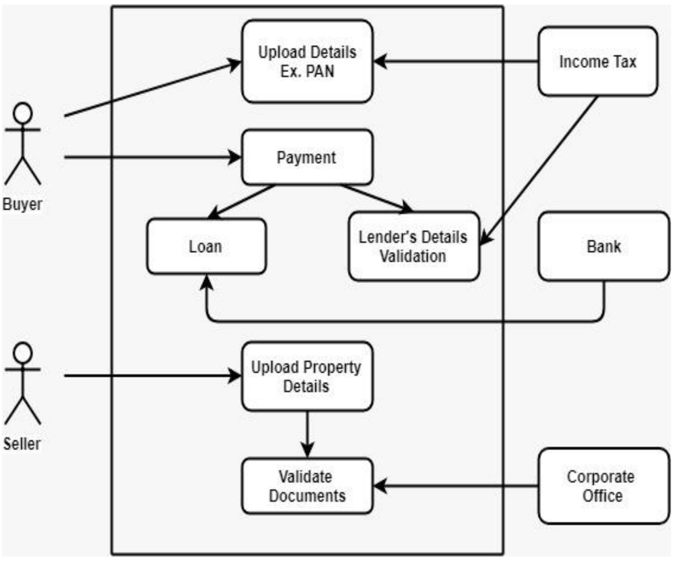

Fig 3: Flow diagram of the validation process

After validating the method by which the buyer wishes to buy the property, he will be taken to the next stage. The second stage displays all those properties in a certain location which the buyer will be able to afford. All the other properties of the same area which are above his level won't be displayed. All the ID's generated in the seller validation phase will be displayed. It contains all the necessary information regarding the property such as location, owner details, photos etc. The buyer decides whether to buy or not. If he wishes to buy then he will be asked to press the buy option. He will be then taken to the digital payment mode where he transfers the required amount to buy the property. After the purchase a new Blockchain will be created indicating the new owner of the property and his details attached to it. In the future if he wishes to buy or sell any property then his details could be fetched directly from the existing Blockchain and then upgrade as necessary. Since all the details are stored in Blockchain it remains secured. The second major advantage is avoiding black money. There is no offline transactions involved in the proposed system. Only online payments are allowed. Hence the entire amount involved in the transaction is taxable. The block diagram shown in figure 3 depicts method of validation.

### *3.3 Storage of user documents*

The user documents such as PAN, Bank balance, identity proof and other details are stored using a method called Smart Contracts. Smart Contracts are lines of codes which does the process of storing information in Blockchain. Consider an example of buying car to understand Smart Contracts in a better way. There are several steps involved and can be a tiring process. If the payment cannot be done instantly then financing has to be done. Along with credit check several forms with the personal information of the person have to be filled to verify the identity. It might be needed to interact with several different people salesperson, finance broker and lender. Hence as a compensation for their work, various commissions and fees are added to the base price of the car. This complex process involves several intermediaries because of lack of trust among participants in the transaction. Smart Contracts can streamline this process. The identity of a person will be stored in Blockchain; hence lenders can quickly make a decision about credit. A Smart Contract would be then created between the dealer, your bank and the lender. When the funds will be released to dealer then the car's title will be held by lender and the repayment will be initiated based on the agreement policy. The transaction gets recorded in Blockchain and ownership will be transferred automatically. This will be shared among the participants and can be checked at any time. IPFS (Interplanetary File System) is a content addressable distributed file system which stores file. Unlike of HTTP it is a peer to peer method of storing file. IPFS thus overcomes the major drawbacks of HTTP. IPFS is a method which provides permanent web and reduce latency. IPFS uses a distributed hash table to store data and MerkleDag gives it a structure. MerkleDag is process of repeated hashing until a root key is obtained. The data is transferred using bit swap. The data will be taken from the nearest peer who has the data and not from a server kept miles away. This reduces bandwidth consumption. Hence Smart Contracts is used as a method to store the user documents in IPFS. Hence it ensures security. Figure 4 depicts the storage process.

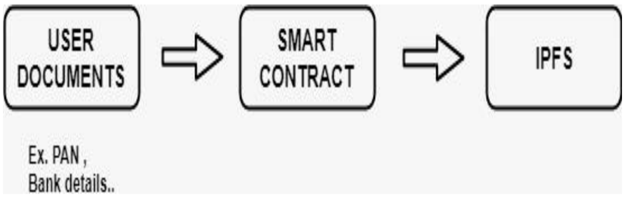

Fig 4: Flow diagram of the storage process

### *3.4 Addition of new Blockchain*

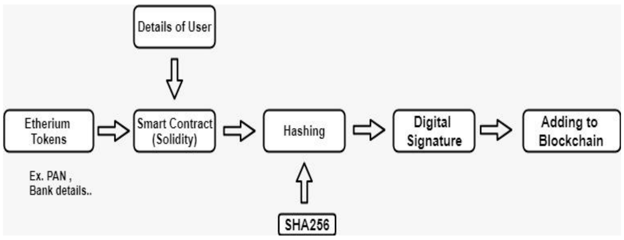

Fig 5: Addition of new Blockchain

The user details are stored using Smart Contracts. Smart Contracts is the only way to add new Blockchain. The entered user details will be encrypted using Hashing. Hashing is a technique which gives encrypted output when an input of any length is given to the hash function. SHA256 is a hashing algorithm which encrypts the data to a fixed length of 256 characters. The input can be of any size. This is one directional and cannot be traced back. A digital code which is generated and authenticated by public key encryption is a Digital signature. It is attached to an electronically transmitted document to verify its contents and the sender's identity. It establishes the proof of ownership for each transaction in the Blockchain. While sending a document the Person A encrypts his document with private key and public key of Person B and sends it over the network. It has to be decrypted first using Private key of B and Public key of A i.e. public key is known to everyone and it can only be encrypted using Private key. The public key is generated using ECDSA one way algorithm then this public key is hashed with SHA256 to give public key hash which on further hashing using Base58Check gives the wallet address of user. Wallet address is a unique identifier for a wallet which can be shared with users to send and receive digital currencies. After the hashing and digital signature process the data will be added to Blockchain. Figure 5 depicts the addition of new Blockchain.

## REFERENCES

[1] Rishav Chatterjee and Rajdeep Chatterjee, “An Overview of the Emerging Technology: Blockchain” in 2017 International Conference on Computational Intelligence and Networks.

[2] Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends” in 2017 IEEE 6th International Congress on Big Data.

[3] Harry Halpin, Marta Piekarska, “Introduction to Security and Privacy on the Blockchain” in 2017 IEEE European Symposium on Security and Privacy Workshops.

[4] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran, Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from bitcoin in Security and Privacy (SP), 2014 IEEE Symposium on, pages 459–474. IEEE, 2014.

[5] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: “The blockchain model of cryptography and privacy-preserving smart contracts,” in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016.

[6] Y. Zhang and J. Wen, “An iot electric business model based on the protocol of bitcoin,” in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015.

[7] S.Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[8] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In Annual International Conference on the Theory and Applications of Cryptographic Techniques Springer, 2015.

[9] Open Source Blockchain Effort for the Enterprise Elects Leadership Positions and Gains New Investments, 2016.

[10] F. K. Maurer, “A survey on approaches to anonymity in Bitcoin and other cryptocurrencies,” Lecture Notes in Informatics (LNI), 2016.

[11] https://en.wikipedia.org/wiki/Blockchain

[12] https://en.wikipedia.org/wiki/Cryptocurrency