A Novel Framework for Automating Land Registrations through Blockchain Technology

L. Haritha[1] and K. Vani[2*]
[1] Assistant Professor, Department of CSE, CVR College of Engineering
*[2] Associate Professor, Department of CSE, CVR College of Engineering

ABSTRACT

Bitcoins are currently gaining popularity among the internet users with their novel approach of dominating the third-party validation like the involvement of banks or trusted third parties in financial transactions. The main technology enabling the rampant rise in the implementation of cryptocurrencies like Bitcoins is Block Chain Technology. Though the block chain technology is much older in its conceptualization and realization, bitcoins popularized it. Block chain technology is an enabling solution for the next generation security issues across different domains. However, the potential of block chain is not yet unleashed with respect to several other problems pertaining to domains like Healthcare, Insurance, remains to be tapped. The whole offline system could completely be automated with the help of block chain technology. An endeavor to propose a novel strategy to automate registration of lands using block chain technology to avoid the typical problems associated with offline registrations is made here.

KEYWORDS: Bitcoins, block-chain Technology, double spending, distributed, peer-to-peer, electronic currency, applications of block chain

I. INTRODUCTION

A block chain is a chain of blocks that contains data. This technique was originally proposed in 1971 to timestamp digital documents. A block chain is a distributed ledger that is completely accessible to anyone. Data stored in a block chain is difficult to tamper with. Each block consists of data, hash of the block and the hash of the previous block. The initial block would contain the previous hash set to all 0's indicating that it is the first block in the chain. If any intruder tries to tamper with the data, the hash of this data gets changed due to which authentication fails. However with the advancement in hardware and computing capabilities generation of hashes for the tampered data and changing the previous hash values in the subsequent blocks is not quite impossible. This is counterfeited with the timestamp of transaction wherein regenerating the hashes of tampered data certainly takes a few seconds more than the original transaction which gets published in the distributed ledger across all the participants in the network who would subsequently vote for the first published transaction which is naturally the original transaction initiated by authentic personnel. This technique of validating a transaction in block chain technology is called as proof of work.

II. APPLICATIONS OF BLOCK CHAIN

Bitcoins

Bitcoins are electronic crypto currencies which are translated using distributed peer-to-peer transactions [1,3, 4]. Bitcoins initiated a radical change in the process of financial transactions by eliminating a need for central authority like a bank or a trusted third party. Instead a distributed ledger is implemented and transactions are validated using block-chain technology. The origin of bitcoins is by Satoshi Nakamoto, an invisible and unknown source who conceived the idea of Bitcoins[4]. Originally, complex mathematical problems are solved to release bitcoins, there are a total of 2 million bitcoins. The process of solving the complex mathematical problems to release bitcoins is called mining and the people who do mining are called miners. The Miners could be hired by companies or individuals to buy bitcoins or miners themselves could trade the bitcoins. A recent trend in the mining and trading of bitcoins can be seen in figure 1[2]. The number of companies which have started and thriving on this technology year wise is shown in Table 1.

Once the mined bitcoins are released, a trading of these bitcoins could be done. In the typical banking phenomena where a centralized ledger is maintained pertaining to all the coins minted where authenticity of a coin is validated based on its first entry into the mint, contrary to this Bitcoins rely on a distributed ledger[7,8].

Table 1. Companies based out on bitcoins over years

Year	No. Of Companies Using Technology
2003	1
2010	1
2011	7
2012	3
2013	26
2014	11
2015	5

A graph plotted against the number of companies established on bitcoins is showing an increasing trend and is seen in Figure 1[2]

A Bitcoin can broadly be defined as a sequence of digitally signed transactions. Every bitcoin is appended with an encrypted of the earlier transactions along with attaching the public key of this mint owner [12]. This chain of transactions marks the basis for mutual trust thus enabling a peer to peer transaction model encouraging a seamless transactions between different parties.

Proof-of-work # method of working

For the purpose of validation of a bitcoin transaction, block-chain technology is used. Block-chain Technology relies on publish model, where a transaction is appended to the bitcoin[6]. The modus operandi is that whenever a transaction occurs an announcement is published across the entire group of bitcoin participants who can later endorse the first occurrence of a particular transaction thus thwarting the chances of a double spending attack[9,10,11]. To check the trading of bitcoins websites like unicorn, Beycoin, Zebpay, coin secure and local Bitcoins may be accessed. They could be purchased in units like milli bitcoin and micro bitcoin as well along with multiples of one whole Bitcoin [5].

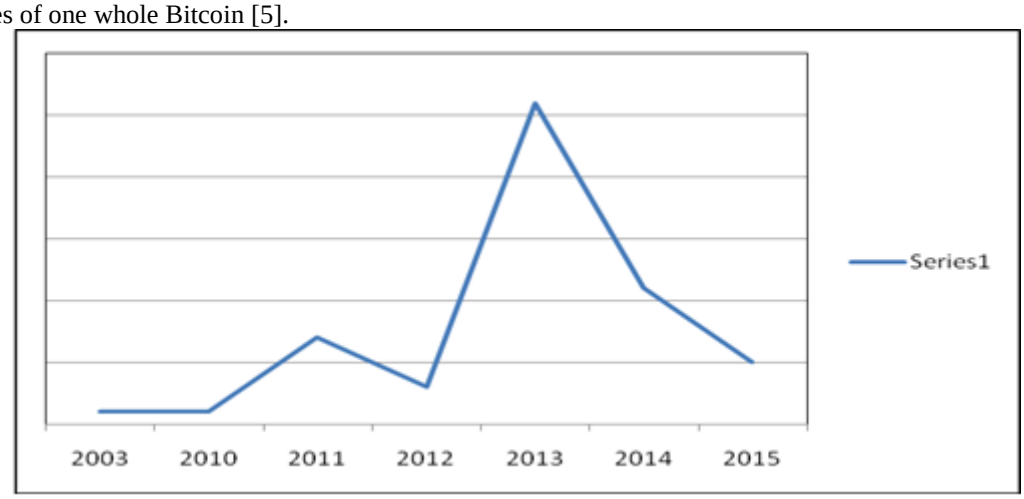

Figure 1. Graph showing trends in Bitcoins usage

III. PROPOSED WORK

Existing System

Current land registrations suffer the drawbacks of double registrations, due to lack of authentication of a registration for a particular land. This is one of the major contributing factors for the rise in the number of civil cases in the jurisdiction of the country. The land registrations currently are being carried based out on a clear title of the land. Clear title refers to possession of encumbrance certificate by a particular owner of the land. The encumbrance certificate is issued by the registrar after due verification of the land's ownership back to quite a few

generations prior to the current ownership. All these details are documented in the "pattadar" book of the land owner. Once an encumbrance certificate is issued to a person, the person is entitled to become the legal owner for the land which is identified by a unique survey number. However, the chances of duplicating the original documents and claiming ownership of a particular land owned by another person is quite possible in which case, it is treated as a double registration case. Such contentions are to be resolved in the court of law.

Proposed System

In the current work, an endeavor to thwart the double registrations of lands using block chain technology is proposed. A unique code comprising of 16 digit number used to uniquely identify a piece of land is allotted. This number along with the seller and buyer information is stored as a data block along with a hash of this data and hash of previous block is stored. In the 16 digit code the first 2 digits specify whether it is a land registration or land lease, next 2 digits signify the state, next 2 digits the district, then the next 2 digits represent the mandal, followed by the 2 digits identifying the village code. This 16 digit number along with the seller's and buyers's information is encrypted using the SHA 256 algorithm. Every transaction thereof is also appended to the previous transaction thus making a trailing list of transactions to every survey number registered within the network. This information however is broadcasted to all the nodes in the network, who would participate in authenticating the next legal transaction by voting. A sample block chain for land registrations is shown in figure 2.

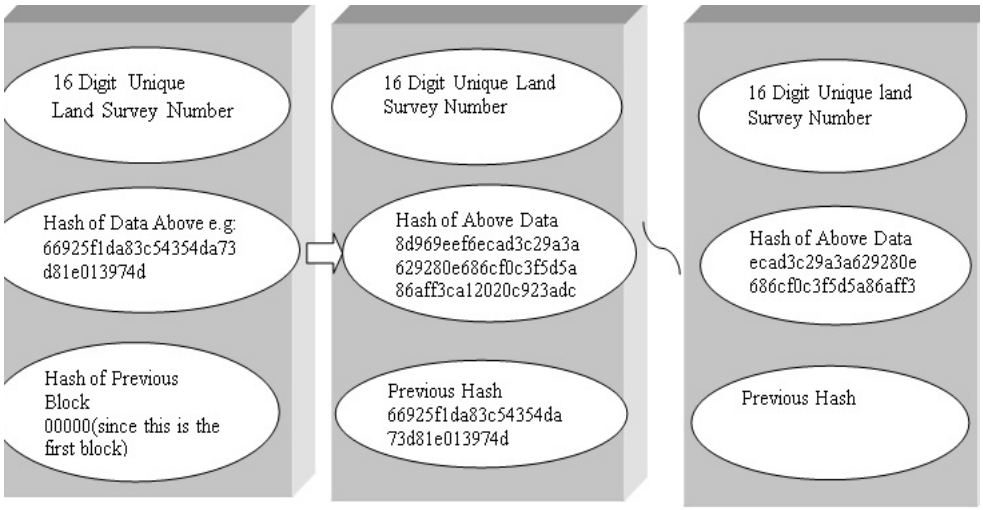

Figure 2.Sample block chain for Land Registrations

IV. CONCLUSION

Block chain technology still remains with a potential unleashed offering solutions to suit the needs of contemporary societal problems. In the current work, a system has been proposed for land transactions, which would use a framework to create a hash of a data pertaining to a land. But this would not serve the purpose as long as the double registration attack persists. As a solution, a peer – to- peer distributed network using proof of work to record public history of land transactions that is difficult to simulate quickly computationally if honest nodes dominate the CPU power. The nodes vote with their CPU power by exercising valid blocks and extending them while the invalid blocks are straightaway rejected.

The vulnerability of existing clients to double-spending might severely harm the motivation towards automation of land registrations, and impact its financial and economic standing.

V. ACKNOWLEDGEMENTS

The authors would like to express their sincere thanks to Satoshi Nakamoto for inspiring them into understanding the concepts underlying the bit coins.

VI. REFERENCES

[1] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan and Joshua A. Kroll, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies", IEEE Symposium on Security and Privacy, IEEE Computer Society, 2015.

[2] https://en.wikipedia.org/wiki/List_of_bitcoin_companies

[3] Anton Badev and Matthew Chen, “Bitcoin: Technical Background and Data Analysis”, Finance and Economics Discussion Series Divisions of Research & Statistics and Monetary Affairs Federal Reserve Board, Washington, D.C.
[4] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”
[5] Nishith Desai, “Beyond Bitcoin: Exploring the Block Chain”, Nithish Desai Associates, 2016.
[6] Alex Biryukov, Dmitry Khovratovich, “Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem”
[7] Malte Möser, “Anonymity of Bitcoin Transactions”, Münster Bitcoin Conference (MBC), 17–18 July ’13, Münster, Germany.
[8] Ghassan O. Karame, Elli Androulaki and Srdjan Capkun, “Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin”
[9] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.
[10] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.
[11] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.
[12] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.