International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 7 Issue 1 Series I ǁ 2019 ǁ PP. 26-28

A Review on Funding Using Blockchain

Amruth V, S Srikanth, Prajwal K M, Sourav B S, Anitha Ananda Rao
Assistant Professor,Information Science and Engineering Maharaja Institute of Engineering Mysore, India
Information Science and Engineering Maharaja Institute of Engineering Mysore, India
Information Science and Engineering Maharaja Institute of Engineering Mysore, India
Information Science and Engineering Maharaja Institute of Engineering Mysore, India
Information Science and Engineering Maharaja Institute of Engineering Mysore, India
Corresponding author: Amruth V (amruthv_ise@mitmysore.in)

ABSTRACT: *There are many fundraising and donation platforms worldwide and yet issues related to extra fees, accountability, corruption and processing delay still exist. Since there is no transparency of each transaction that happens after the amount is paid to organization, causing chaos and mistrust issues in the society. In this paper, we present a succinct survey on blockchain technologies, smart contracts used and covering its problem and research gap.*
KEYWORDS: *blockchain, smart contracts, consensus, cryptocurrency*

Date of Submission: 08-03-2019 Date of acceptance: 28-03-2019

I. INTRODUCTION

- **Blockchain**

A blockchain is an open distributed database (a distributed ledger) that monitors cash, merchandise traded or transactions on an open decentralized manner. In a conceptual view, the block-chain is a data structure that consists of time ordered, linked blocks that contain a number of transactions, and each transaction in the public ledger is verified by consensus from a majority of the participants in the system. Once information is entered into the blockchain, it cannot be erased.[1] The blockchain allows trust less network, whereby two strangers can perform secure electronic transactions without trusting each other. In conclusion blockchain technology is very attractive and useful to overcome the financial also the nonfinancial industry dilemma.

- **Smart Contracts**

The concepts of smart contract was established by Szabo (1997) 20 years ago[2,3]. The industries have already moved on to the second generation of blockchain applications which incorporates smart contract, intellectual property and digitizing asset ownership. The blockchain smart contracts contains scripts that are stored on the blockchain with a unique address enabling us to easily trace. Decentralized smart contracts has its own advantages compared to the traditional cryptocurrencies. The advantages like fair exchange, to minimized interaction among parties and efficiency.

II. BACKGROUND ON BLOCKCHAIN

- **Proof Methods**

A blockchain is a replicated state machine [4] where a reversed link between blocks is a pointer from a state to its previous state. [5] Consensus is necessary to totally order the blocks, hence maintaining the chain structure. To reach consensus, traditional blockchain systems adopted a technique based on proof-of work, requiring a proof of computation [6]. Miners solve a hashcash crypto puzzle [7] to append a new block to the chain. Given a block and a threshold, a miner repeatedly(mines) selects a nonce and substitutes a pseudo-random function to this block and the selected nonce until the obtained result is lower than the threshold. This restricts or limits the rate at which new blocks can be generated by the network.

However, solving proof-of-work puzzles wastes a significant amount of electricity, i.e., the huge computing power used to solve the puzzle is wasted unproductively[8]. To save energy, therefore, an alternative method called the proof-of-stake method was proposed within the Bitcoin community as early as 2011 and Peercoin [3]was the first cryptocurrency to implement it. In proof-of-work, the probability of mining a block depends on the work done by the miner. Conversely, the resource of the proof-of-stake is the amount of coins that are held. In order to successfully complete an attack on the blockchain, an attacker has to control more than 50 percent of the resources of the entire network (known as a 51% attack). In proof-of-stake, if an attacker tries to gain(monopolize) coins to control the network, participants will detect it and the value of the coins held will be significantly reduced. This works as a deterrence against attacks.

The Ripple consensus algorithm starts with a known set of nodes known to be participating in the consensus[10]. The Unique Node List, (UNL) is a list of public keys meant to be associated with those active (validating) nodes, the node operator believes are "unique". [11] Ripple Labs suggests that UNL's "should have 100+ nodes on them."

TABLE I. BLOCKCHAIN PLATFORMS [20]

Blockchain platform	**Consensus model**	**Proof method**	**Support smart contracts**	**Permissioned or permission less blockchain**	**Built in crypto-currency**
NEM	Eigen trust	Proof of stake	No	Permissioned Blockchain	None
ERIS (FOSS)	Byzantine fault tolerance	Proof of work	Yes	Permission less	None
ERIS	Byzantine fault tolerance	Proof of work	Yes	Permission less	None
(MONA)	PBFT, others can be implemented	Proof of work and proof of stake	Yes	Both can be set up	None
Bluemix hyper-ledger	Byzantine fault tolerance	Proof of work	No	Permission less	Bitcoin
Bitcoin	Ripple consensus Algorithm	Unique nodes list	No	Permissioned	Ripple (XRP)
Ripple	Byzantine fault tolerant	Proof of Work	Yes	Permission less	Ether

- Permissioned and Permissionless blockchain

Distributed Ledger Technologies can be alienated between permission-less and permissioned networks. A permissioned network limits the number of peers who can access the blockchain and participate in the validation in contrary to a permission-less network where everyone can contribute in the canonical chain. For instance, Bitcoin and Ethereum are permission-less blockchains that rely on a Proof-of Work (PoW) consensus[18].

III. BLOCKCHAIN CONSENSUS MODELS

- Eigen trust

An algorithm to decrease the number of downloads of inauthentic files in a peer-to-peer file-sharing network that assigns each peer a unique global trust value [12], based on the peer's history of uploads. It's a distributed and secure method to compute global trust values, based on Power iteration. By having nodes or peers use these global trust values to choose the peers from whom they download, the network effectively identifies corrupt and malicious peers and thus isolates them from the network. In simulations, this reputation system is called Eigen Trust and has been shown to significantly decrease the number of inauthentic files on the network, even under a variety of conditions where malicious peers cooperate in an attempt to deliberately monopolize or subvert the system.

- Byzantine fault tolerance

A reliable computer system must be able to cope with the failure of one or more of its components[13]. A failed component or node may exhibit a type of behaviour that is often overlooked--namely, sending conflicting or wrong information to different parts of the system. The problems associated with this type of failure is expressed abstractly as the Byzantine Generals Problem.

Byzantine-fault-tolerant [BFT], state machine replication algorithm that is safe in distributed asynchronous systems such as the Internet [14]. It does not rely on any synchrony assumption to provide safety. In particular, it can work well even in the presence of denial-of-service attacks. Moreover, it guarantees liveness provided message delays are bounded eventually. The service may temporarily be unable to return replies when a denial-of-service attack is active but clients are guaranteed to receive replies when the attack ends.

- Practical Byzantine fault tolerance

Practical Byzantine Fault Tolerance (PBFT) as a practical and improved algorithm on BFT works in asynchronous environments [15] to improve the response time of previous algorithms by more than an order of magnitude [16] and reduces message complexity on BFT algorithm from the exponential level to polynomial level for the first time [17]. PBFT as a practical algorithm for state machine replication could tolerate Byzantine faults and offer both liveness and safety.

IV. FINDINGS

Table I gives the summary of various trending blockchain platforms and their capabilities. After studying these blockchain platforms, we concluded that Ethereum blockchain is most suitable for our platform because Ethereum can be seen as a transaction-based state machine which can transition between states using

cryptographically secured transactions. When creating a new state machine node encode rules or criteria that must be met in order for valid state transition to happen, this information is then merged into blocks and gets uploaded on the blockchain. This functionality of Ethereum allows us to create automated contracts to be enforced between our system actors.

V. CONCLUSION AND FUTURE WORK

To conclude, we have proposed a system of philanthropic donation platform that is distributed, transparent and secure by storing all transaction details on a public blockchain and by creating smart contracts which is programmed to interact with actors within the blockchain system. By doing this we can help donors, vendors and donation receivers from all over the world to transact money in a decentralized, transparent, trusted and secure environment. Furthermore, because the system does not rely on an intermediary to transfer funds, the speed and cost for handling aid is reduced. In the future, we hope to explore on methods that could verify transactions much faster. For example, instead of using proof of work we could experiment with other methods of consensus algorithms such as proof of stake or proof of importance to achieve faster verifications of transactions.

REFERENCES

[1]. Stefan Seebacher and Ronny Schüritz.:" Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review" © Springer International Publishing AG 2017 S. Za et al. (Eds.): IESS 2017, LNBIP 279, pp. 12–23, 2017. DOI: 10.1007/978-3-319-56925-3_2.

[2].] Bin-Yu Zan, Yuan R, Xia YB, Chen HB.: "ShadowEth: Private smart contract on public blockchain". JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 33(3): 542–556 May 2018. DOI 10.1007/s11390-018-1839-y.

[3]. TonChanhLe, LeiXu, LinChen, WeidongShi.:" Proving Conditional Termination for Smart Contracts" ©2018 Association for Computing Machinery. ACMISBN978-1-4503-5758 6/18/06. https://doi.org/10.1145/3205230.3205239

[4]. X. Xu, C. Pautasso, L. Zhu, V. Gramoli, S. Chen, A. Ponomarev, and A. B. Tran, "The blockchain as a software connector," in Proceedings of the 13th Working IEEE/IFIP Conference on Software Architecture (WICSA), 2016.

[5]. Christopher Natoli, Vincent Gramoli.:" The Blockchain Anomaly". 2016 IEEE 15th International Symposium on Network Computing and Applications. DOI 978-1-5090-3216-7/16/ ©2016 IEEE.

[6]. C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology, ser. CRYPTO '92, 1993, pp. 139–147.

[7]. A. Black, "Hashcash - a denial of service counter-measure," Cypherspace, Tech. Rep., 2002. [Online]. Available: http://www.hashcash.org/papers/hashcash.pdf

[8]. Hiroki Watanabe, Shigeru Fujimura, Atsushi Nakadaira, Yasuhiko Miyazaki, Akihito Akutsu, and Jay Kishigami.:" Blockchain Contract: Securing a Blockchain Applied to Smart Contracts". 2016 IEEE International Conference on Consumer Electronics (ICCE). DOI 978-1-4673-8364-6/16/ ©2016 IEEE.

[9]. S. King, S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof of-Stake", http://peercoin.net/assets/paper/peercoin-paper.pdf, 2012.

[10]. Peter Todd.:" Ripple Protocol Consensus Algorithm Review". May 11th 2015. git commit 92812fe7239ffa3ba91649 b2ece1e892b866ec2a from https://github.com/ ripple/rippled.

[11]. Ripple Labs Inc. Unique node list, 2015. [Online; accessed 24-April-2015].

[12]. Sepandar D. Kamvar, Mario T. Schlosser, Hector Garcia-Molina.:" The EigenTrust Algorithm for Reputation Management in P2P Networks". May 20–24, 2003, Budapest, Hungary. ACM 1-58113-680-3/03/0005.

[13]. LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE.:" The Byzantine Generals Problem". © 1982 ACM 0164-0925/82/0700-0382 ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, July 1982, Pages 382-401.

[14]. MIGUEL CASTRO and BARBARA LISKOV.:" Practical Byzantine Fault Tolerance and Proactive Recovery". ° 2002 ACM 0734-2071/02/1100-0398 ACM Transactions on Computer Systems, Vol. 20, No. 4, November 2002, Pages 398–461.

[15]. Li Zhang, Qinwei Li.:" Research on Consensus Efficiency Based on Practical Byzantine Fault Tolerance". 10th International Conference on Modelling, Identification and Control (ICMIC), July, 2-4, 2018, Guiyang, China.

[16]. N. Chondros, K. Kokordeelis and M. Roussopoulos, "On the Practicality of Practical Byzantine Fault Tolerance," Springer Berlin Heidelberg, vol. 7662, pp. 436-455, 2011.

[17]. J. Fan, LT. Yi and JW. Shu, "Research on the technologies of Byzantine system," Journal of Software, vol. 24, no. 6, pp. 1346-1360, 2013.

[18]. Joanna Moubarak, Eric filiol, Maroun Chamoun.:" On Blockchain Security and Relevant Attacks". 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM). DOI 978-1-5386-1254-5/18/ ©2018 IEEE.

[19]. G. Zyskind and A. S. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," 2015.

[20]. Rizal Mohd Nor, M.M Hafizur Rahman, Towfiqur Rahman and Adam Abdullah, "Blockchian sadaqa mechanism for disaster aid crowd funding" Proceedings of the 6th International Conference on Computing and Informatics, ICOCI 2017 25-27April, 2017 Kuala Lumpur. Universiti Utara Malaysia.

Amruth V" A Review on Funding Using Blockchain" International Journal of Research in Engineering and Science (IJRES), vol. 07, no. 1, 2019, pp. 26-28