International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 5 Issue: 7
ISSN: 2454-4248
28 – 33

A Survey on Block Chain and Bitcoin – Challenges & Applications

Kolluru Venkata Nagendra[1]
Associate Professor,
Department of CSE,
ASCET, Gudur,
kvnagendramtech@gmail.com

G Rajesh[2]
Assistant Professor,
Department of CSE,
ASCET, Gudur,

Arun Prasad Desai[3]
Assistant Professor,
Department of CSE,
ASCET, Gudur,

Abstract: Block chain is as of late presented and changing the advanced world conveying another point of view to security, flexibility and productivity of framework. While at first promoted by Bit Coin, Block chain is significantly more than an establishment for digital money. It offers a safe method to trade any sort of good administration or exchange. This paper exhibits an exhaustive review on Block chain Technology and Bit coin. Bitcoin has emerged as the most successful crypto currency since its appearance back in 2009. Besides its security robustness, two main properties have probably been its key to success: anonymity and decentralization. In this paper, we provide a comprehensive description on the details that make such crypto currency an interesting research topic in the privacy community. We perform an exhaustive review of the bitcoin anonymity research papers that have been published so far and we outline some research challenges on that topic.

Key Words: *Block chain, Bit coin, Trade and Finance, supply chain and e-Voting.*

******

I. INTRODUCTION

Blockchain: A Blockchain is a standout amongst the most famous and dubious syndicated programs among innovation pioneers. In basic words blockchain is a sort of computerized record, a record of exchanges without the control of any focal expert. Every one of the exchanges are put away as squares. Blockchain is the most recent method for putting away information and exchanges. At the end of the day, blockchain is a disseminated record guardian to store exchange information without focal man.

A blockchain is a chain of blocks of that develops as new information is added to the chain. Each "Block" contains a hashed key which joins it to the past block, a timestamp for when it was adjusted, and exchange information. Every exchange is confirmed by the minors and added to the block. Blockchain after accord is come to on the legitimacy of the activity. This enables members to put trust in their exchanges even without a focal specialist, along these lines empowering distinct mediation.

A blockchain is intrinsically unchanging - when recorded, information on the blockchain can't be changed. In a blockchain to refresh an old record, most of the hubs must be consented to change. Blockchain innovation is one of the rising advancements now days. It might bring us more dependable and helpful Services. Blockchain is a group of innovations containing scientific calculation, Cryptography, shared systems, circulated database.

Bitcoin: Bitcoin is an online virtual currency based on public key cryptography, proposed in 2008 in a paper [1] authored by someone behind the Satoshi Nakamoto pseudonym. It became fully functional on January 2009 and its broad adoption, facilitated by the availability of exchange markets allowing easy conversion with tradicional currencies (EUR or USD), has brought it to be the most successful virtual currency. However, in contrast to other virtual payments systems appeared so far, the seminal paper [1] describing the Bitcoin system was not published in the scientific arena but as a forum post on the Internet.

Furthermore, the practical development of the ideas proposed in such paper took place on January 2009, when the same author created the first block of the Blockchain and implemented a fully functional bitcoin wallet which allows to operate with such new cryptocurrency. For this reason, the deployment of bitcoin took of without so much attention from the research community and the first research papers on the topic did not appear until late 2011 in the arXiv repository and later published conferences and journals ([2,3]). During the 2014, there has been an explosion in the publication of bitcoin research papers, and well established conferences included the topic of cryptocurrecies as a“topic of interest”.

II. CHARACTERISTICS OF BLOCKCHAIN

Key Characteristics of Blockchain are as follows

- ✓ Decentralization. In traditional incorporated exchange frameworks, every exchange should be

 ISSN: 2454-4248
28 – 33

approved through the focal confided in organization (e.g., the national bank), unavoidably coming about to the expense and the execution bottlenecks at the focal servers. Complexity to the concentrated mode, outsider is never again required in blockchain. Accord calculations in Block Chain are utilized to keep up information consistency in disseminated organize.

- ✓ Persistency. Exchanges can be approved rapidly and invalid exchanges would not be conceded by legit diggers. It is about difficult to erase or rollback exchanges once they are incorporated into the Block Chain. Hinders that contain invalid exchanges could be found promptly.
- ✓ Anonymity. Every client can collaborate with the Block Chain with a produced location, which does not uncover the genuine character of the client. Note that Block Chain can't ensure the ideal security protection because of the inherent requirement.
- ✓ Auditability. Bitcoin Block Chain stores information about client adjusts dependent on the Unspent Transaction Output (UTXO) show: Any exchange needs to allude to some past unspent exchanges. When the present exchange is recorded into the Block Chain, the condition of those alluded unspent exchanges change from unspent to spent. So exchanges could be effectively verified and followed.
- ✓

III. APPLICATIONS OF BLOCKCHAIN

Blockchain is a technology used for most of the digital currencies as a platform. Blockchain is not only for Bitcoin, it can be used to develop an application that can be used as a shared distributed database. Some of the applications are discussed as:

APPLICATION	DESCRIPTION
Block Chain in Real estate :	In the real estate market there are various individual angles that are to be kept mystery to make a focused market. Blockchain innovation could empower the land advertise more straightforward and free from arbiter. Utilization of blockchain in land makes the work quicker, less demanding, riskless, lessening extortion and giving more straightforwardness. Blockchain as keen contracts can assume a major job in land, particularly in activities, for example, property exchanges (buy, deal, financing, renting, and administration).
Blockchain in Supply Chain :	Traditional supply chains need straightforwardness in view of their multifaceted nature. Blockchain innovation is greatly affecting business to make straightforwardness. Presently days associations are tolerating advanced method for supply chains. New advances, having extraordinary effect in transit of business. These strategies are on a very basic level changing the manner in which things are delivered and disseminated. In store network blockchain is being acknowledged step by step.
Blockchain for e-voting :	Innovation is getting advance step by step. Electronic casting a ballot framework is the most recent creation of this specialized world. Just in the couple of years e-casting a ballot framework turn out to be excessively famous due to its straightforwardness, high security and protection. Cryptography is utilized to make the framework more secure. In e-casting a ballot framework all capacities are on the web and result is tallied consequently. Contrasted and customary casting a ballot, electronic casting a ballot is less tedious and rate of exactness is more. Utilization of blockchain makes it more straightforward and secure.
Blockchain in Education :	Blockchain is endeavor to have a place in every single field. The utilization of blockchain to instruction is somewhat new. Blockchain can be utilized to join the records of expansive colleges, little foundations, schools and online instructive stages to shape a freely obvious chain.
Blockchain in Medical :	Blockchain innovation can likewise assume an essential job in medicinal services moreover. Blockchain has transformative potential for our wellbeing and care frameworks. There are various utilize instances of blockchain in medicinal services, for

 ISSN: 2454-4248
28 – 33

example, repayment of social insurance administrations, trade of wellbeing information, clinical preliminaries and supply chains. In spite of the fact that having an extraordinary effect in therapeutic, this innovation yet confronting various difficulties that are keeping the usage of this innovation in restorative, for example, information protection and clinical preliminaries.

IV. BITCOIN PAYMENTS

Payments in the bitcoin system are performed through transactions between bitcoin accounts. A bitcoin transaction indicates a bitcoin movement from source addresses to destination addresses. Source addresses are referred as input addresses in a transaction and destination addresses are named output addresses. A transaction details the exact amount of bitcoins to be transfered from each input address. The same applies to the output addresses, indicating the total amount of bitcoins that would be transfered at each account. For consistency, the total amount of the input addresses (source of the money) must be greater or equal than the total amount of the output addresses (destination of the money) [4]. Furthermore, the bitcoin protocol forces that input addresses must spend the exact amount of a previous received transaction [5] and for that reason, in a transaction, each input address can unambiguously indicate the index [6] of the transaction in which the bitcoins were received. Finally, the owner of the input addresses should perform a digital signature using his private keys, proving that he is the real owner of such accounts.

V. BITCOIN NETWORK

The bitcoin system needs to disseminate different kinds of information, essentially, transactions and blocks. Since both data are generated in a distributed way, the system transmits such information over the Internet through a distributed peer to peer (P2P) network. Such distributed network is created by bitcoin users in a dynamic way, and nodes of the bitcoin P2P network [5] are computers running the software of the bitcoin network node. This software is included by default into bitcoin's full-client wallets, but it is not usually incorporated in light wallet versions, such as those running in mobile devices. It is important to stress such distinction in case to perform network analysis, because when discovering nodes in the P2P bitcoin network, depending on the scanning techniques, not all bitcoin users are identified, but only those running a full-client and those running a special purpose bitcoin P2P node. Furthermore, online bitcoin accounts, provided by major bitcoin Internet sites, can also be considered as a light weight bitcoin clients, so they do not represent a full bitcoin P2P node neither.

Bitcoin Anonymity: Anonymity is probably one of the properties that has been key for the success of the currency deployment. Anonymity in the bitcoin network is based on the fact that users can create any number of anonymous bitcoin addresses that will be used in their bitcoin transactions. This basic approach is a good starting point, but the underlaying non-anonymous Internet infrastructure, together with the availability of all bitcoin transactions in the blockchain, has proven to be an anonymity threat.

VI. TRAFFIC ANALYSIS

Traffic analysis: The anonymity degree of users in the bitcoin system is also bounded by the underlying technologies used. Transactions in the bitcoin system are transmitted through a P2P network, so, as it was first pointed out in [2], the TCP/IP information obtained from that network can be used to reduce the anonymity of the system. Although it is true that most wallets are able to work over anonymous networks (TOR11 or I2P12) a high number of bitcoin users do not use such services, and then, there is still room for network analysis. Koshy et alter [6] perform an anonymity study based on real-time transaction traffic collected during 5 month. For that purpose, authors develop CoinSeer, a bitcoin client designed exclusively for data collection. For more than 5 million transactions, they collected information on the IP address from where the CoinSeer received such transaction and, in the general case, they assigned as the IP corresponding to the transaction the one that broadcast the transaction for the first time. In order to perform a pure network analysis, authors do not apply any address clustering process, so only single input transactions (almost four million) are taken into account in the analyzed data set. Then, to match an IP with a bitcoin address, they consider a vote on the link between IPi and addressj if a transaction first broadcasted form an IPi contains the bitcoin addressj as input address. Authors also perform a similar analysis for output addresses and model the problem as an evaluation of association rules, identifying the corresponding confidence scores and the support counts for the rule. After their analysis, authors conclude that it is difficult to map IP addresses with bitcoin addresses by performing traffic analysis if bitcoin peers act properly, since the bindings authors could obtain between IP addresses and bitcoin addresses mainly come from anomalous transactions patterns. Furthermore, authors also indicate that some network configuration, like mixing services or eWallets, might conduct to erroneous assumptions when linking IP and bitcoin addresses.

In contrast to blockchain analysis, traffic analysis has received less attention from the researches probably due

 ISSN: 2454-4248
28 – 33

to the fact that the blockchain is ready available for analysis and network data has to be gathered. In fact, bitcoin network analysis is a hard topic due to the dynamism and size of such P2P network. The anonymity analysis performed by Koshy et alter seems to show that no information can be derived with this technique, but it is difficult to completely discard such approach since in their work authors do not provide any estimation regarding which part of the bitcoin P2P network represent the 2,678 peers they were able to monitor, and for the period of the analysis, no data of the size of the network is available from other sources. So, with only one work performed, whether or not network analysis can reveal private information from bitcoin users still remains an open problem. Furthermore, network analysis can be performed to identify not only the owner of an address but also the identity of other actors in the bitcoin community.

VII. CHALLENGES &RECENT ADVANCES

Despite the great potential of blockchain, it faces numerous challenges, which limit the wide usage of blockchain. We enumerate some major challenges and recent advances as follows.[7]

A. Scalability With the amount of transactions increasing day by day, the blockchain becomes bulky. Each node has to store all transactions to validate them on the blockchain because they have to check if the source of the current transaction is unspent or not. Besides, due to the original restriction of block size and the time interval used to generate a new block, the Bitcoin blockchain can only process nearly 7 transactions per second, which cannot fulfill the requirement of processing millions of transactions in real-time fashion. Meanwhile, as the capacityof blocks is very small, many small transactions might be delayed since miners prefer those transactions with high transaction fee. There are a number of efforts proposed to address the scalability problem of blockchain, which could be categorized into two types:

- Storage optimization of blockchain.
- Redesigning blockchain.

B. Privacy Leakage

Blockchaincanpreserveacertainamountofprivacythrough the public key and private key. Users transact with their private key and public key without any real identity exposure. However, it is shown in [8], [9] that blockchain cannot guarantee the transactional privacy since the values of all transactions and balances for each public key are publicly visible. Besides, the recent study [10] has shown that a user's Bitcoin transactions can be linked to reveal user's information. Moreover, Biryukov et al. [11] presented an method to link user pseudonyms to IP addresses even when users are behind Network Address Translation (NAT) or firewalls. In [11], each client can be uniquely identified by a set of nodes it connects to. However, this set can be learned and used to find the origin of a transaction. Multiple methods have been proposed to improve anonymity of blockchain, which could be roughly categorized into two types:

- Mixing
- Anonymous.

C. Selfish Mining

Blockchain is susceptible to attacks of colluding selfish miners. In particular, Eyal and Sirer [12] showed that the network is vulnerable even if only a small portion of the hashing power is used to cheat. In selfish mining strategy, selfish miners keep their mined blocks without broadcasting and the private branch would be revealed to the public only if some requirements are satisfied. As the private branch is longer than the current public chain, it would be admitted by all miners. Before the private blockchain publishment, honest miners are wasting their resources on an useless branch while selfish miners are mining their private chain without competitors. So selfish miners tend to get more revenue. Based on selfish mining, many other attacks have been proposed to show that blockchain is not so secure. In stubborn mining [13], miners could amplify its gain by non-trivially composing mining attacks with network-level eclipse attacks. The trail-stubbornness is one of the stubborn strategy that miners still mine the blocks even if the private chain is left behind. Yet in some cases, it can result in 13% gains in comparison with a non-trail-stubborn counterpart. [14] shows that there are selfish mining strategies that earn more money and are profitable for smaller miners compared to simple selfish mining. But the gains are relatively small. Furthermore, it shows that attackers with less than 25% of the computational resources can still gain from selfish mining. To help fix the selfish mining problem, Heilman [15] presented an novel approach for honest miners to choose which branch to follow. With random beacons and timestamps, honest miners would select more fresh blocks. However, [17] is vulnerable to forgeable timestamps. ZeroBlock [16] builds on the simple scheme: Each block must be generated and accepted by the network within a maximum time interval. Within ZeroBlock, selfish miners cannot achieve more than its expected reward.

VIII. CONCLUSIONS

The assessment shows BlockChain can accept a basic employment in changing the digitalization of endeavors and applications by engaging secure trust frameworks and all the more firmly joining with headways, for instance, conveyed processing and IOT. The Block chain

 ISSN: 2454-4248
28 – 33

is an advancement that makes it possible to store information without giving off on an inside man. The closures are that the Block chain is amazingly useful and appropriate in different locales where the plan is mentioning safty, straightforwardness and ampleness.

Bitcoin is an installment framework dependent on a decentralized design that gives a component to get numerous mysterious accreditations, bitcoin addresses that can be utilized to perform and get installments. In any case, inquire about performed so far has demonstrated that the manner in which the framework uses such locations may reveal some data from their proprietors. Since all exchanges performed by the framework are unreservedly accessible in the blockchain for investigation, it permits to group different addresses of a similar client and describe a few employments. Moreover, on the off chance that one of the addresses of the bunch can be mapped to a genuine personality, at that point the installment history of the whole group may reveal pertinent data of that client. Albeit intriguing exploration has been performed in this theme, the dynamism of the bitcoin environment that always modifies and improves the bitcoin utilization infers that a portion of the speculations expected for those blockchain examination may not totally hold and, hence, blockchain investigation still introduces fascinating open inquiries.

Aside from the blockchain investigation, obscurity of the bitcoin framework can be broke down by social affair data from the P2P system utilized for installment correspondence. Since the P2P system utilizes the TCP/IP convention, traffic examination may uncover private data from clients. Be that as it may, such investigation is considerably more difficult to perform than the blockchain examination since the bitcoin P2P system is very powerful.

Finally, it is worth notice that examination in the bitcoin biological system can be performed in different points than obscurities, as for example cryptography, organize security or P2P system to give some examples. Then again, other than the examination lines that can be performed straightforwardly on the investigation of the bitcoin framework itself, different methodologies perform research utilizing the bitcoin framework as an instrument. Instances of such methodology are the plan of secure multiparty calculation or coin hurl conventions. Moreover, some basic pieces of the bitcoin framework, similar to the blochchain approach as an attach just record, may open fascinating difficulties for future advancements on secure decentralized frameworks.

IX. REFERENCES

[1] Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. (2008)

[2] Reid, F., Harrigan, M.: An analysis of anonymity in the bitcoin system. In Altshuler, Y., Elovici, Y., Cremers, A.B., Aharony, N., Pentland, A., eds.: Security and Privacy in Social Networks. Springer New York (2013) 197–223

[3] Babaioff, M., Dobzinski, S., Oren, S., Zohar, A.: On bitcoin and red balloons. In: Proceedings of the 13th Association for Computing Machinery (ACM) Conference on Electronic Commerce. EC ’12, New York, NY, USA, ACM (2012) 56–73

[4] Antonopoulos, A.M.: Mastering Bitcoins. O’Reilly Media (December 2014)

[5] Donet, J.A., P´erez-Sola, C., Herrera-Joancomart´ı, J.: The bitcoin P2P network. In Bo¨hme, R., Brenner, M., Moore, T., Smith, M., eds.: Financial Cryptography and Data Security. Volume 8438 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2014) 87–102

[6] Koshy, P., Koshy, D., McDaniel, P.: An analysis of anonymity in bitcoin using p2p network traffic. In Christin, N., Safavi-Naini, R., eds.: Financial Cryptography and Data Security. Volume 8437 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2014) 469–485

[7] “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends “ , Zibin Zheng, Shaoan Xie, Hongning Dai,, 2017 IEEE 6th International Congress on Big Data.

[8] S.Meiklejohn,M.Pomarole,G.Jordan,K.Levchenko,D.McCoy,G.M. Voelker, and S. Savage, “A fistful of bitcoins: Characterizing payments among men with no names,” in Proceedings of the 2013 Conference on Internet Measurement Conference (IMC’13), New York, NY, USA, 2013.

[9] 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, pp. 839–858.

[10] J. Barcelo, “User privacy in the public bitcoin blockchain,” 2014.

[11] A. Biryukov, D. Khovratovich, and I. Pustogarov, “Deanonymisation of clients in bitcoin p2p network,” in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014, pp. 15–29.

[12] I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436– 454.

[13] K.Nayak,S.Kumar,A.Miller,andE.Shi,“Stubbornmining:Generalizing selfish mining and combining with an eclipse attack,” in Proceedings of 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, Germany, 2016, pp. 305–320.

[14] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, “Optimal selfish mining strategies in bitcoin,” arXiv preprint arXiv:1507.06183, 2015.

[15] S. Billah, “One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner,” 2015.

[16] S. Solat and M. Potop-Butucaru, “ZeroBlock: Timestamp-Free Prevention of Block-Withholding Attack in Bitcoin,” Sorbonne Universites, UPMC University of Paris 6,

Technical Report, May 2016. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01310088

[17] Androulaki, E., Karame, G., Roeschlin, M., Scherer, T., Capkun, S.: Evaluating user privacy in bitcoin. In Sadeghi, A.R., ed.: Financial Cryptography and Data Security. Volume 7859 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2013) 34–51

[18] Ron, D., Shamir, A.: Quantitative analysis of the full bitcoin transaction graph. In Sadeghi, A.R., ed.: Financial Cryptography and Data Security. Volume 7859 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2013) 6–24

[19] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S.: A fistful of bitcoins: Characterizing payments among men with no names. In: Proceedings of the 2013 Conference on Internet Measurement Conference. IMC '13, New York, NY, USA, ACM (2013) 127–140

[20] Ober, M., Katzenbeisser, S., Hamacher, K.: Structure and anonymity of the bitcoin transaction graph. Future Internet 5(2) (2013) 237–250

[21] Spagnuolo, M., Maggi, F., Zanero, S.: Bitiodine: Extracting intelligence from the bitcoin network. In Christin, N., Safavi-Naini, R., eds.: Financial Cryptography and Data Security. Volume 8437. Springer Berlin Heidelberg (2014) 457–468

[22] Maxwell, G.: Coinjoin: Bitcoin privacy for the real world. post on bitcoin forum https://bitcointalk.org/index.php?topic=279249.

[23] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Www.Bitcoin.Org, p. 9, 2008.

[24] S. Sargolzaei, B. Amaba, M. Abdelghani, and A. Sargolzaei, "Cloudbased Smart Health-care Platform to tackle Chronic Disease," vol. 4863, no. August, pp. 30–32, 2016.

[25] S. Underwood, "Blockchain beyond bitcoin," Commun. ACM, vol. 59, no. 11, pp. 15–17, 2016.

[26] "Crypto-currency market capitalizations," 2017. [Online]. Available: https://coinmarketcap.com

[27] G. Engaged, J. Tobe, G. Your, C. Computing, C. Dellorso, E. Apps, E. Reggie, R. Coughlan, and M. S. Fernandes, "Annual Conference – May 6-7 , 2013 – Kingsmill Resort ' The Value of Values : Linking Strategy and Decision Making ' – 2013 Annual Conference Educational Sessions," 2013.

[28] W. E. Summary and S. Plants, "Power and the Industrial Internet of Things (IIoT)," no. January, pp. 1–14, 2015.

[29] U. S. D. of H. and H. Services, "Standards for privacy of individually identifiable health information; proposed rule.," Fed. Regist., vol. 64, no. 212, p. 59917, 1999.

[30] Centers for Medicare and Medicaid Services, "Security Standards: Technical Safeguards," HIPAA Secur. Ser., vol. 2, pp. 1–17, 2007. [10] M. Modahl, "Tablets set to change medical practice," Quantia MD, 2011.

[31] White paper on "Applications of Blockchain Technology to Banking and Financial Sector in India" by IDRBT, January 2017

[32] G. Wood. Ethereum: A Secure Decentralised Generalised Transaction Ledger – Homestead Revision. Jan. 2016. [7]. EU. (2016). Blockchain applications & services. Case study.

[33] A. Kiayias, I. Konstantinou, A. Russell, B. David, R. Oliynykov. : Ouroboros: A provably secure proof-of-stake blockchain protocol.