INTERNATIONAL JOURNAL OF ADVANCE RESEARCH AND DEVELOPMENT

(Volume 3, Issue 10)

Available online at: www.ijarnd.com

A review on challenges and opportunities in Blockchain Technology

Urvi Dilipkumar Rajguru

Student, Raksha Shakti University, Ahmedabad, Gujarat

ABSTRACT

The blockchain is a decentralized exchange and information association improvement grew first for Bitcoin cryptographic money. A Blockchain is basically a passed on database of records, or open record everything considered or motorized occasions that have been executed and shared among taking an interested party. Each exchange the comprehensive network record is certified by the assertion of a greater bit of the people in the structure. Once entered, data can never be deleted. The Blockchain contains a certain and clear record of each and every exchange whenever made. Bitcoin, the decentralized appropriated electronic money, is the most standard blueprint that utilization Blockchain advancement. The modernized cash Bitcoin itself is outstandingly sketchy at any rate the central Blockchain headway has worked consummately and discovered wide grouping of utilization in both monetary and non-budgetary world. The fervor for Blockchain advancement has been developing since the considering was established in 2008. The explanation for the energy for Blockchain is its focal properties that give security, namelessness and information steadfastness with no outcast alliance accountable for the exchanges, and appropriately it makes dazzling examination zones, particularly from the point of view of particular difficulties and repressions. In this examination, we have composed a consider mapping study with the objective of the social event all basic research on Blockchain advancement. We will most likely understand the stream research subjects, inconveniences and future headings with respect to Blockchain progression from the particular point of view.

Keywords— *Bitcoin, Litecoin, Blockchain, Loyalty, Hash, Cryptocurrency, Ethereum, Private Chain, Public Chain*

1. INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

Money exchanges between people or affiliations are as from time to time as conceivable bound together and controlled by an untouchable affiliation. Impacting an impelled segment or money to exchange requires a bank or charge card supplier as an executive to finish the exchange. In like way, an exchange causes a cost from a bank or a MasterCard affiliation. An in every practical sense indistinct framework applies in like the way in a couple of particular spaces, for example, beguilements, music, programming et cetera. The exchange structure is conventionally joined, and all information and data are controlled and facilitated by an untouchable relationship, rather than the two fundamental parts related to the exchange. Blockchain advance has been passed on to regard this issue. The objective of Blockchain progress is to make a decentralized zone where no untouchable is in charge of the exchanges and information.

The blockchain is a coursed database system that keeps up a continually making rundown of information records that take the stand concerning by inside focuses valuing it. The information is recorded in an open record, including data of each exchange at whatever point wrapped up. The blockchain is a decentralized outline which does not require any untouchable relationship in the center. The data about each exchange at whatever point finished in Blockchain is shared and open to all center interests. This trademark makes the structure more clear than bound together exchanges including an outsider. Moreover, the fixations in Blockchain are everything seen as confounding, which makes it more secure for different focus fixations to support the exchanges. Bitcoin was the principal application that demonstrated Blockchain progress. Bitcoin affected a decentralized zone for cryptographic to money, where the all-inclusive community can purchase and trade stock with cutting edge cash.

It is essential to perceive what subjects have been starting at now considered and tended to in Blockchain and what are starting under the most exceptional conditions weights and impediments that need additionally thinks about. To address these request, we used a gainful mapping study system to see fundamental papers related to Blockchain. In the think mapping study, we related a particularly kept research custom to search for material in sensible databases. The affected guide of melodic change to look at on Blockchain will interface with specific managers and experts in watching possible research zones and imperativeness for future research.

2. ARCHITECTURE OF BLOCKCHAIN TECHNOLOGY

Blockchain gives an ordinary record improvement that individuals in a business structure can use to record the true blue establishment of business trades that can't be changed. Blockchain gives a singular reason for truth: a standard, change clear record.

This approach changes trade following from a soloed show up, where differentiating records are seen over wholeheartedly, to one that gives a standard view over the entire framework.

Since Blockchain uses consent to submit trades to the record, the results are last. Each part has a copy of a proportional record, so asset provenance and tractability are clear and trusted. Blockchain can be related to any industry.

The blockchain is a plan of squares, which holds an entire once-finished of exchange records like a standard open record. Figure 1 portrays an occasion of a Blockchain. With a past square hash contained in the square header, a square has just a single parent square. It is basic that uncle squares hashes would in like way be moored in Ethereum Blockchain. The essential square of a Blockchain is called beginning square which has no parent square. We by then clear up the internals of Blockchain in unassuming parts.

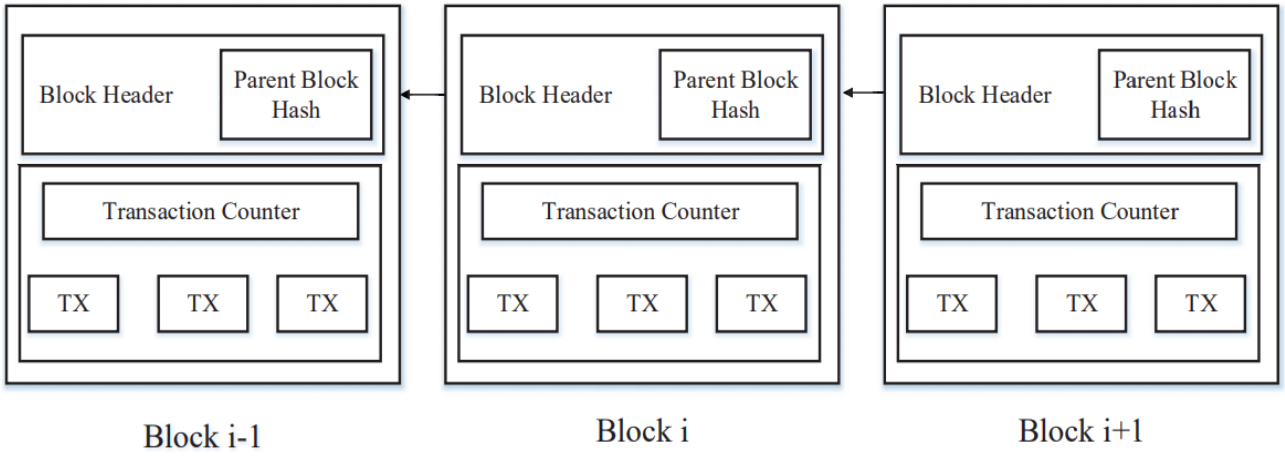

Fig. 1: An example of Blockchain

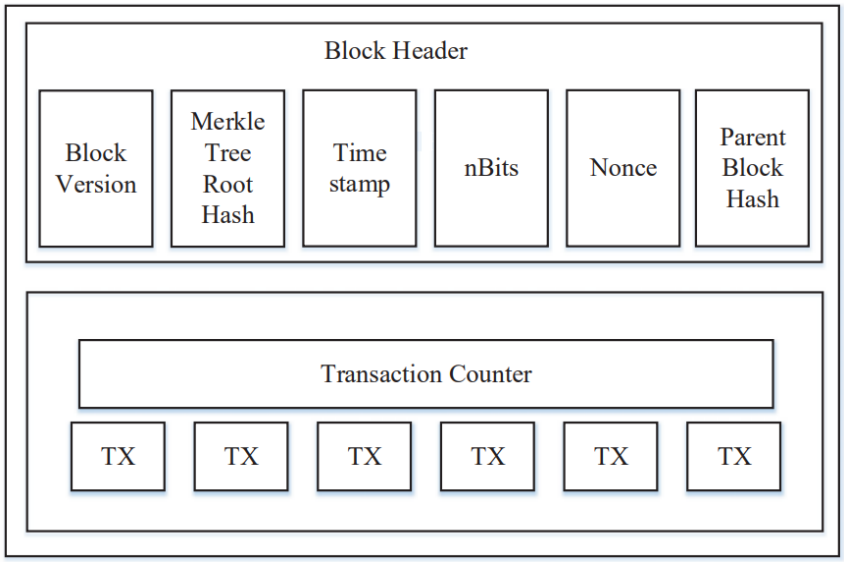

Fig. 2: Block architecture

2.1 Block

A square contains the square header and the square body as appeared in Figure 2. Specifically, the square header wires following parts as described in the figure above.

- **Block alteration:** shows which set of square validation rules to take after.
- **Root hash:** the hash estimation of all the transactions in the square.
- **Timestamp:** current time as seconds in the complete time since January 1, 1970.
- **nBits:** target limit of a true blue square hash.
- **Nonce:** a 4-byte field, which by and large begins with 0 and enlargements for each hash estimation
- **Parent square hash:** a 256-piece hash respect that fixations to the past square

The square body is made out of a trade counter and trades. The most outrageous number of trades that square can contain depends upon the square size and the proportion of each trade. Blockchain uses a cryptography segment to affirm the check of transactions. Digital signature in light of unequal cryptography is used futile scheming condition.

2.2 Digital signature

Every client ensures several private key and open key. The private key that will be kept in confidentiality is utilized to sign the exchanges. The modernized checked exchanges supporter all through the entire structure. The standard induced check is joined with

two stages: stamping stage and demand manage. For example, a client Alice needs to send another client Bob a message. In the checking stage, Alice scrambles her information with her private key and sends Bob the encoded result and amazing information. In the verification phase, Bob bolsters the inspiration with Alice's open key. The run of the mill electronic stamp joins utilized Blockchain is the elliptic twist moved stamp estimation.

3. TYPES OF BLOCKCHAIN TECHNOLOGY

It required an essential stretch of time to comprehend Blockchain. Before long there are particular structures. Until the point that further notice, there are three sorts of Blockchain, since then two or three affiliations, governments, and banks have been attempting to utilize the Blockchain. Regardless, what is the multifaceted nature between various purposes of truth comprehended Blockchain in the setting of their makes as given underneath?

3.1 Public Blockchain

An open Blockchain as its name proposes is the Blockchain of open, which suggests a sort of Blockchain which is-' for the general open, by the comprehensive network and of the comprehensive network'. Here nobody is in control and anybody can value examining/framing/taking a gander at the Blockchain. Something extraordinary is that these sorts of Blockchain are open and clear from this time forward anybody can examine anything at a given explanation behind time on an open Blockchain. Regardless, a trademark asks for that motivates a passionate reaction is that when nobody is in control here then how the choices are gone up against these sorts of the Blockchain. So the correct response is that fundamental expert occurs by different decentralized assentation instruments, for example, proof of work (POW) and proof of stake (POS) etc. Bitcoin, Litecoin is the best case of open Blockchain Technology.

On Bitcoin and Litecoin Blockchain systems, anybody can do the running with things that make it to a great degree open Blockchain.

- Anyone can run BTC/LTC full focus and begin mining.
- Anyone can make exchanges on BTC/LTC chain.
- Anyone can think about/review the Blockchain in a Blockchain voyager.

3.2 Private Blockchain

Private Blockchain as its name underpins is a private property of an individual or an affiliation. Not under any condition like open Blockchain here, there is an in control who organizes enormous things, for example, read/make or whom to unequivocally offer access to investigate or the substitute way. Here the comprehension is refined on the focal clarifications behind the focal in-control that can give mining rights to anybody or not give by any stretch of the creative centrality.

That is the thing that makes it reevaluated where particular rights are sharpened and vested in a focal confided in the party yet it is cryptographically moored from the affiliation's perspective and fundamentally more monetarily sharp for them. In any case, it is 'in the not to an extraordinary degree far away past far from being obviously veritable if such a private thing can be known as a 'Blockchain' in light of the path by which that it generally invalidates the all-around beneficial of Blockchain that Bitcoin OK with us. Bank chain is an occasion of private Blockchain change.

In this kind of Blockchain:

- Anyone can't run a full focus point and begin mining.
- Anyone can't make exchanges on the chain.
- Anyone can't plot/review the Blockchain in a Blockchain voyager.

3.3 Consortium Blockchain or federated Blockchain

This kind of Blockchain endeavors to clear the sole self-lead which gets vested in just a specific substance by using private block chains. So here instead of one in charge, you have more than one in charge. On an essentially key level, you have a social unlawful relationship of affiliations or expert individuals getting together and settling on decisions for the best exceptional position of the whole structure. Such social affairs are likewise called consortiums or an interest that is the reason the name consortium or joined Blockchain. For example, let recall you have a consortium of the world's control 20 cash related relationship. So it is a framework for achieving thing on a to a superb degree focal level speedier and you other than have more than one single illuminating behind dissatisfactions which in a way remains the whole customary structure against a specific motivation driving blocked want. r3, EWF is a pinch of the instance of this kind of Blockchain.

In such kind Blockchain:

- Members of the consortium can run a full concentration and start mining.
- Members of the consortium can make trades/decisions on the chain.
- Members of the consortium can consider/outline the Blockchain in a Blockchain voyager.

4. CHALLENGES IN BLOCKCHAIN TECHNOLOGY

Blockchain headway use is being investigated in interminable, interfacing from stock structure to budgetary affiliations. While there is all the more than likely that circumnavigated record change is extraordinary diverged from different advancement starting late events, it is likely that it will require a fundamental degree of speculation before the progress is gotten all around. That is by the greatness of there are a couple of troubles related to Blockchain plan that must first be facilitated before wide coordination can happen.

4.1 Scalability

Blockchain are experiencing bother enough supporting a fundamental number of clients on the system. Both Bitcoin and Ethereum, the major Blockchain systems, have encountered squashed exchange speeds and higher costs charged per exchange light of a liberal change in users. While this reality has affected all around look at about how to help both these structures and Blockchain everything considered, relative, the dialogs around the proposals are to an amazing degree moved and are undoubtedly going to take a gigantic proportion of time. In like way, scaling methodology should be checked and completely screened before execution into the records. Adaptability concerns must be sensibly tended to before the Blockchain can be comprehended a wide scale.

4.2 The criminal connection

Since its dispatch, Bitcoin has for quite a while been connected with the shadowy dealings of the things advance and the dull web. Since this is the chief joint exertion of general society with Blockchain change, this intrigue has continued with Bitcoin, Altcoins, and the tech key it too. A social occasion of powerful events found that best in class sorts of money are utilized by foot raise territories to interface with buys of constrained materials on online business centers, as a contraption for unlawful cost keeping up a vital separation from, what's more, bundle structures for Ransomware. While these exercises are unlawful, they are a surrendered unavoidable conceded result of individuals' relationship of bleeding edge money related structures and ought to be conceivable with fiat money other than. In any case, for Blockchain movement to be seen by people as a last resort, it must shake this shadowy association.

4.3 Inefficient technological design

The Ethereum questionable contract oversees licenses engineers for a changed show of affiliations. While Bitcoin is the critical cryptographic cash, the Ethereum make connects with customers to trade the purpose behind the control of the Blockchain to true blue applications. Regardless, get some information about has demonstrated that a noteworthy number of sharp contracts passed on the stage have vulnerabilities in the setting of their coding. Also, the Bitcoin supervise is proposed to join a fundamental level of data with each trade. While a piece of this information is central, only a particular out of each odd last piece of it is essential. This makes the Bitcoin Blockchain liberal and rather enthusiastic. Blockchain setup must be streamlined and progressed to constrain these inefficient edges to result in wide choice.

4.4 Privacy

The Bitcoin Blockchain is ought to have been quick self-evident. Every single one of the information identifying with a trade is open for anyone to see. Adjacent to security, this is the same with unlimited Blockchain starting at now in closeness. While this part may be major in two or three settings, it changes into a peril if scattered records are to be used in delicate conditions. For instance, private patient data should not be open for all on an extremely fundamental level like the case with restrictive business data. This is in addition colossal to government data or cash related data. For Blockchain advancement to be gotten on a wide scale, the records ought to be balanced with a particular legitimate focus to oblige access to the data contained in that to only the general open who have the essential breathing space.

4.5 Security

While it is to a brilliant degree difficult to happen to wide Blockchain structures, Blockchain is slight against a 45% strike. This dress a condition where a digger or a gathering of excavators control in excess of 50 percent of the mining power. In such a condition, the excavators would be able to control the request of new exchanges, particularly those by different diggers. Besides, they would be able to switch the exchanges they ensured and in this way twofold spend tokens. While the controlling diggers would not be able to change old wrecks, this would to a stunning degree affect the dauntlessness of the token with the impacted Blockchain and it would need to recoup in people everything thought about the eye. Luckily, the likelihood of this strike is lessened as more individuals share in the structure as excavators.

4.6 Costs

Blockchain change is an impacting instrument for decreasing costs. It diminishes the lacks related for exchanging respect and can streamline the operational system. Notwithstanding, in light of how it is an all-around new movement, it is hard to help it with inheritance structures. Such a structure is likely going to be a senseless issue that particular affiliations and governments will be unwilling to get it.

5. FUTURE AND OPPORTUNITIES IN BLOCKCHAIN TECHNOLOGY

Blockchain as a headway can on an especially key level impact a wide system of structures and sorts of advancement. At its inside, the Blockchain is a structure for discarding the key for trust in trades. While that may appear like a key recommendation, a creature bit of the best foundations on the planet exist today to fill in as trusted in untouchables, for example, SWIFT and the Depository Trust Clearing Company. Corporate open zones copy for affiliations that can increment related Blockchain degrees of ground concentrating on specific trades, for example, the home drive industry.

The centrality scene of home advances requires an amazing web of title looks, title affirmation, and on edge minor trade charges that are major to keep the structure running. These structures exist in light of the way that, clearly, the trading of land has been a system that requires a mammoth level of trust in dated records. In any case, the Blockchain would address these weights, and a specific property's record can contain certain and kept up the history of trades, obliging the major for foundations to give a chance aiding and trust affiliations, rather the trade can exist in its own specific right. The result would close home advances for really level of the cost, in to some degree level of the time, with wide higher degrees of trust.

The most key bit of Blockchain is that it gives staggering security in an unsecured Internet where phishing, malware, spam and hacks put in the chance the course by which business is done all around. One of the pick benefits that Blockchain gives over other

record making PC programs is that it depends upon cryptography and is familiar with last, one can't return to a specific point on the Blockchain and change data. For the 10 wide stretches of Blockchain's substance, it has never been hacked. Another fundamental ideal position of Blockchain is it's passed on completed distinctive structures, making it to an amazing degree difficult to bring down for a condition of despot government or unlawful business hones. For instance, a land got uncovered and can't be executed or covered up by any master, making the proprietor shielded from shows of dismissal.

Considering, Blockchain is a grand device to use to store gigantic degrees of basic documentation in turns, for example, fulfilling affiliations, surrounded undertakings, copyright and some more. Blockchain discharges the basic for a keep running between concerning legitimizing contracts. Sharp contract stages are 'beginning at starting late being complimented reasonably of utilization and are required to see wide use in the running with 3 years.

6. CONCLUSION

Blockchain change could be to a confounding degree basic in a likelihood space for the future world that circuits both thought and decentralized models. Like any new change, the Blockchain is a perceived that at first bewilderments and after sometimes it could push the refinement in a more obvious ordinary structure that joins both the old way and the new movement. Some confirmed plans are that the approach of the radio in sureness incited broadened record structures, and peruses, for instance, the Kindle have extended book bargains. As time goes on, we get news from the New York Times, district, Twitter, and repair float channels alike. We cripple media from both essential redirection affiliations and YouTube. Therefore, after some time, Blockchain change could exist in a simply clearer trademark structure with both joined and decentralized models.

It is basic to understand Blockchain concerning Bitcoin, regardless you should not see that all Blockchain trademark structures require Bitcoin instruments, for instance, proof of work, longest chain run, and so on. Bitcoin is an essential undertaking at keeping up a decentralized, open record with no formal control or affiliation together. There are massive exasperates included. Of course, private appropriated records and Blockchain can be sent to arrange to change approaches of issues. As ever, there are tradeoffs and upsides and hindrances to every system, and you need to consider these vivaciously for each individual use case.

7. REFERENCES

[1] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends" 2017 IEEE 6th International Congress on Big Data, June 2017

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

[3] G. W. Peters, E. Panayi, and A. Chapelle, "Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective," 2015. [Online]. Available: http://dx.doi.org/10.2139/ssrn.2646618

[4] G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain, "2015.

[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, pp. 839–858

[6] B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the bitcoin economy," 2013. [Online]. Available: https://ssrn.com/abstract=2394738

[7] 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, pp. 184–191

[8] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for the educational record, reputation and reward," in Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), Lyon, France, 2015, pp. 490–496.

[9] Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park, Kyung-Hyune Rhee" A Critical Review of Blockchain and Its Current Applications" International Conference on Electrical Engineering and Computer Science (ICECOS) 2017 - 19 March 2018.

[10] A. S. Tanenbaum and M. Van Steen, Distributed systems: principles and paradigms. Prentice-Hall, 2007.

[11] D. Drescher, "Blockchain basics," Springer, Tech. Rep.

[12] L. Lamport, R. Shostak, and M. Pease, "The byzantine general's problem," ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382–401, 1982.

[13] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," URL: http://www.bitcoin.org/bitcoin.pdf, 2008.

[14] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[15] Elyes Ben Hamida, Kei Leo Brousmiche, Hugo Levard. "Blockchain for Enterprise: Overview, Opportunities, and Challenges" The Thirteenth International Conference on Wireless and Mobile Communications, ICWMC 2017

[16] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," International Journal of Web and Grid Services, 2017, pp. 1–23.

[17] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, 2016, pp. 2292–2303.

[18] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Sept 2016, pp. 1– 3.

[19] "Stampd.io: A document blockchain stamping notary app," accessed: 2017-07-01. [Online]. Available: https://stampd.io/

[20] A. Yasin and L. Liu, "An online identity and smart contract management system," in 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), vol. 2, June 2016, pp. 192–198.

[21] Shiv Raj Sharma, "Blockchain Technology Review and Its Scope" International Research Journal of Engineering and Technology (IRJET) Volume: 04 Issue: 12 | Dec-2017

[22] N. Anderson, "Blockchain Technology A game-changer in accounting?" unpublished. Admin. (2015, Nov 30). [Online]. Available: https://symbiont.io/uncategorized/distributed-ledgers-vs-centralized-databases/
[23] P. Stafford. (2015, Jul 14). [Online]. Available: https://www.ft.com/content/454be1c8-2577-11e5-9c4e-a775d2b173ca
[24] A. Lewis. (2017, Feb 20). [Online]. Available: https://bitsonblocks.net/2017/02/20/whats-the-difference-between-a-distributed-ledger-and-a-blockchain/
[25] Distributed Ledgers, Internet: http://www.investopedia.com/terms/d/distributed-ledgers.asp [Mar.01, 2017].
[26] J. Walent.(2016, July) , "Blockchain: A Case for General Ledger." Payments Journal [on-line]. Available:http://www.paymentsjournal.com/Content/Featured_Stories/31920/, [Mar.01, 2017].
[27] "Know More About Blockchain: Overview, Technology, Application Areas and Use Cases," Let's Talk Payments, http://letstalkpayments.com/an-overview-of-blockchain-technology/.
[28] "Financial Institutions: Blockchain Activity Analysis," Let's Talk Payments, Sept. 7, 2015, http://letstalkpayments.com/financial-institutions-blockchain-activity-analysis/.
[29] "What is Blockchain Technology? A Step-by-Step Guide For Beginners," Block Geeks,
[30] http://blockgeeks.com/guides/what-is-blockchain-technology/.

