May-June 2020
ISSN: 0193-4120 Page No. 4715-4722

Smart Contract Authorization Using Blockchain

[1]U.Sailesh, [2]T.Tharun, [3]U.Aditya Varma, [4]Shilpa V, [5]S.V.Subba Reddy
[4]Assistant Professor
[1,2,3,4]Department of Computer Science and Information Technology, REVA University, Bengaluru,India
[1]saileshuppuluri@gmail.com, [2]tharunkoti1999@gmail.com,
[3]Adithya951@gmail.com, [4]shilpa.v@reva.edu.in, [5]siddireddy578@gmail.com

Article Info
Volume 83
Page Number: 4715-4722
Publication Issue:
May-June 2020

Article History
Article Received:*19 November 2019*
Revised: *27 January 2020*
Accepted: *24 February 2020*
Publication: *16 May 2020*

Abstract

File authorization is a process of either giving or denying access to a system which in order gives the permission for client to access information depending on the client's profile. Most of the security frameworks depend on a advance procedure which consists of two steps. Confirmation: The first stage which guarantees about the user personality. Approval is subsequent step, which grants the user to get to the access dependent on the user's character. Act in the present day frameworks rely upon trusted third party member. We propose using blockchain-based shrewd agreements to encourage secure examination and the board of files without the need of confided in outsider part. Utilizing the Ethereum blockchain, we can store a hash of a private report (an agreement, for instance) alongside an Ethereum Address. This demonstrates in an open and secure manner that the proprietor of the Ethereum Address has marked the archive. Different gatherings to the agreement can sign it too. All they need is a connect to the marking page, which is produced when a client transfers a document.

Keywords: *Blockchain, Ethereum, smart contracts and decentralized management.*

1. Introduction

An ongoing study of more than 500 IT masters internationally directed by Ipswitch and Vanson-Bourne in the U.S., U.K., Germany and France uncovered worries over their association's capacity to ensure information (counting record move) and meet security consistence prerequisites. The outcomes propose that IT groups need document move robotization to stop incidental information misfortune by end-clients, while empowering the association to partake in constant improvement for improved information insurance. Just a single third of all respondents detailed that their capacity to distinguish and relieve hazards in their record move forms is exceptionally productive. The expense of information misfortune and resistance with information protection approaches is high. IT groups need the innovation to empower end-clients from coincidental information misfortune, while engaging them for coordinated upgrades to meet business and security enhancements. There have been numerous endeavors at building a worldwide dispersed document framework. A few frameworks have seen huge achievement, and others flopped totally

Past Work**:** Buterin explained a part of his work in 2013. Despite the reality that presently developed from numerous points of view, the true usefulness of blockchain with a complete turing language and a adequately boundless between exchange stockpiling capacity stays unaltered. The authors Cynthia Dwork and Moni Naor in the year 1992 gave their main work onto Usage of compute consumption cryptographic proof ("verification of-work"). As a means of conveying a worthwhile sign over the Internet. This worth sign is used as spam discouragement instrument as opposed to any sort of money, however basically showed the potential for an essential information channel to convey a solid financial sign, permitting a recipient to cause A physical declaration, without focusing on security. The author A.Back in the year 2002 delivered a comparative Structure. The principal case for using verification of-function as solid financial sign to make sure about a cash. Right now, token was utilized to keep distributed document exchanging check, giving "customers" with the capacity to make miniaturized scale installments to "providers" in reference to their administrations. The designed model for security is maintained by the proof of the work has been expanded with computerized marks

May-June 2020
ISSN: 0193-4120 Page No. 4715-4722

and a database to ensure that the chronic database can not be debased and that malevolent on-screen characters couldn't parody installments or unjustifiably gripe about help conveyance. The author Nakamoto in 2008 presented a proof of the work-made sure about worth token, fairly more extensive in scope. The products of this venture, Bitcoin, turned into the first broadly received worldwide decentralized exchange record. Different activities based on Bitcoin's prosperity; the alt-coins presented various different monetary forms through adjustment to the convention. Lite coin and Prime coin are the completely most common, examined by the author sprankel in the year 2013. Different undertakings also tried to take into account and repurpose the basic material of the convention; In the year 2012 author aron talks about, The Name coin plan, for example, which means giving a decentralized name-goal system.

In 1997, the writers Szabo and Miller ended early work on sensitive agreements. It turned out to be certain around the 1990s that algorithmic comprehension specifications could turn into a huge power in human involvement. Given the fact that no concrete mechanism was suggested for the application of such a system, it was expected that these frameworks would actively influence the fate of law. Could be called a general use of such a crypto-law system right now

The spillage of information in electronic paper records (EFRs) may result in trade off the security of information (for example, useful information). Much of the information in EFRs remains unchanged until it is passed to the framework; in this way, blockchain may potentially be used to allow this information to be exchanged. Diverse partnerships and citizens involved. It will then be feasible (for example, healthcare practitioners, emergency departments, development organisations and insurance agencies) to meet EFRs put on the blockchain with a greater degree of certainty.

The authors in [1], proposed Digital marks include some of the scheme, but the fundamental benefits are lost if a believed outsider is still needed to avoid double spending. similarly authors in [2], proposed The aim of Ethereum is to create an elective convention for the construction of decentralized applications, offering an alternative arrangement of trade-offs that we believe to be useful for a vast class of decentralized applications, with special emphasis on circumstances in which quick improvement time, safety for applications used little by little and once in a while and the ability of Various applications are important for proficiently connecting.[7] sent huge document dispersion frameworks supporting more than 100 million synchronous clients. Indeed, even today, Bit Torrent keeps up an enormous organization where a huge number of hubs stir every day. [8] These applications saw more noteworthy quantities of clients and documents dispersed More than their partners in the scholastic record setting. In any case, the programs were not designed as the basis upon which to construct themselves. Although successful repurpositions have not established a comprehensive document structure that provides low-inertness and open dissemination worldwide.

We are suggesting an solution to the double issue of expenditure using a shared framework. The machine timestamps are exchanged by hashing them into a progressive chain of hash-based proof of operation, creating a record that cannot be modified without retrying the operation confirmation., A blockchain-based open encryption conspire is suggested for EFRs. The record for EFRs is created by means of complex logical articulations and put in the blockchain so that an information client can use the articulations to access the file. As only the file is moved to the blockchain to promote generation, the proprietors of the information have complete control over who can see their EFRs information. Using blockchain software ensures that the file of EFRs is straight, against modification and recognizability. Finally, the show of the proposed plot is assessed from two viewpoints, to be precise as to the overhead for separating the archive IDs from EFRs and the overhead associated with directing transactions in Ethereum on brilliant agreement.

Organisation of Paper

This paper follows this format. It starts with Introduction as part I, System overview as part III, Literature survey as part IV, Methodology as part V working as part VI and Results as part VII .The Conclusion and References are in part VIII and IX.

2. System Overview

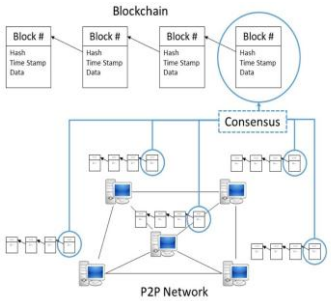
It involves the basics required in order to complete the task at hand and also to gain better understanding of the concepts.

A. What is Block Chain?

```Blockchain innovation has pulled in colossal consideration in both scholarly community and capital market. Be that as it may, overpowering theories on a large number of accessible digital currencies and various beginning coin offering tricks have additionally welcomed famous discussions on this rising innovation.

By nature, a blockchain is an ever-developing chain of obstacles, each of which contains a cryptographic hash of the past square, a time mark, and its transmission of information

Key elements of blockchain are in the below figure:


```

May-June 2020
ISSN: 0193-4120 Page No. 4715-4722

B. Smart Contract

The ongoing improvement of blockchain innovation has resuscitated the thought and encouraged the production of savvy contracts, initially imagined by Szabo in 1994 (e.g., Tapscott and Tapscott (2016)):

"A savvy contract is a modernized exchange convention that executes the particulars of an agreement. The general targets are to fulfill normal legally binding conditions, (for example, installment terms, liens, privacy, and even requirement), limit exemptions both malevolent and unintentional, and limit the requirement for confided in go-betweens. Related financial objectives incorporate bringing down misrepresentation misfortune, mediations and implementation costs, and other exchange costs."

While an accord definition (no play on words planned) for savvy contracts still can't seem to be reached, their center usefulness is clear — contracting on possibilities on a decentralized agreement, and on ease, algorithmic execution. To accomplish decentralized agreement, a disseminated record is required, which additionally must act naturally executing. Possibilities (counting portion of property and control rights) in a savvy agreement ought to be arranged, with the goal that computerized execution is attainable, decreasing implementation cost. The previously mentioned realities lead to a characteristic practical meaning of brilliant agreements:

Keen agreements are computerized contracts permitting terms dependent upon decentralized accord that are self-upholding and carefully designed through robotized execution.

C. Ethereum

Ethereum is an undertaking which endeavors to fabricate the summed up innovation; innovation on which all exchange based state machine ideas might be manufactured. In addition it means to give to the end-engineer a firmly incorporated start to finish framework for building programming on an up to this point unexplored register worldview in the standard: a trustful article informing process structure.

3. Literature Survey

As sited in paper [1], Advanced marks include some of the scheme, but the fundamental benefits are lost if a believed outsider is still expected to prevent double spending. We are suggesting an solution to the double problem of expenditure using a shared framework. The device exchanges timestamps by hashing them to advance chain of hash-based verification of-work, shaping a record that can't be changed without re-trying the evidence of-work.

As sited in paper [2], The expectation of Ethereum is to make an elective convention for building decentralized applications, giving an alternate arrangement of tradeoffs that we accept will be helpful for a huge class of decentralized applications, with specific accentuation on circumstances where quick advancement time, security for little and once in a while utilized applications, and the capacity of various applications to proficiently cooperate, are significant.

As sited in paper [3], bitcoin paper was distributed by Satoshi Nakamoto, whose personality despite everything stays a secret. The objective of Bitcoin was to make a shared (P2P) money that would evacuate the requirement for a confided in outsider, for example, a bank. From that point forward, the media progressively revealed about Bitcoin because of the ascent of the Bitcoin value, the progressive idea of the fundamental blockchain innovation and its maltreatment by lawbreakers to move bitcoins out in the open without leaving physical follows. Exchanges are just combined with a Bitcoin address, which isn't really connected with a character. In May 2017, the ransomware WannaCry, made by the NSA got free and utilized an endeavor in old Windows variants to taint PCs all around the world. The ransomware had the option to secure just 50 Bitcoins up to finish of May 2017 [2] while another crypto malware Erebus gained even a Million US$ [3].

As sited in paper [7] Large file storage systems were deployed that served over 100 million simultaneous users. Also now, Bit Torrent maintains a large deployment in which tens of millions of nodes churn every day.

As sited in paper [8] these applications saw more noteworthy quantities of clients and documents circulated than their scholastic record framework partners. Be that as it may, Frameworks were not designed as the foundation upon which to construct themselves. Although successful repurposings1 have occurred, no large record system has been created that offers global, low-dormancy, and decentralized dispersal.

As sited in paper [5] this venture targets observing medicinal services utilizing shrewd agreement as follows the crude information is sent to an ace "savvy gadget," normally a cell phone or tablet, for accumulation and organizing by the application. When complete, the designed data is sent to the important savvy contract for full investigation alongside redid limit esteems. In the Ethereum convention, the hotspot for the data took care of to the keen agreements is known as the "Prophet". Right now, Oracle is the savvy gadget, which imparts straightforwardly to the brilliant agreements. The keen agreement will at that point assess the gave information and issue alarms to both the patient and human services supplier, just as mechanized treatment guidelines for the actuator hubs whenever wanted.

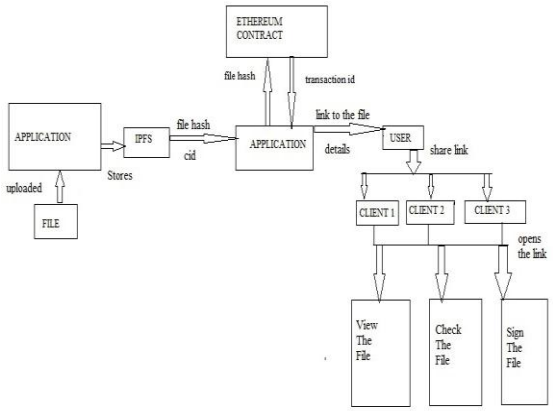
As sited in paper [6] A frontend, a web application method, HTML and Java interface dialects were used to build the frontend. An Ethereum private blockchain was based on a hubs network. To test EMR, electrocardiogram (ECG) information was put away on IPFS hubs associated with the Ethereum hubs, and produced occasionally by a nearby programming. A few shrewd agreements were additionally conveyed for warning age and hubs association.

May-June 2020
ISSN: 0193-4120 Page No. 4715-4722

4. Methodology

The methodology consists of Architecture design, modules and the stepwise process performed during the usage of technology.

Architecture Design



The concept of the application developed is as follows:

a) The application works on the basis of private network technology instead of third party users
b) The file will be uploaded into the application using a basic web application
c) The application then stores it into the IPFS(Inter planetary file system)
d) The IPFS then produces the content identifier and file hash back to the application
e) The application moves towards the Ethereum contract using the file hash which in further provides the transaction id to the application
f) The application then shares a link for the file details to user for access
g) The user shares the link over the clients and they will be given access over viewing ,checking and signing the file

IPFS:

IPFS is a disseminated document framework which incorporates fruitful thoughts from past shared Systems that include DHTs, BitTorrent, Git, SFS. IPFS 'dedication is to disentangle, build and associate demonstrated procedures into a single firm system, which is more remarkable than its parts aggregate. IPFS provides another stage for the composition and dissemination of applications, as well as another process for the dispersal and creation of huge information. IPFS could also push the network forward.

IPFS is distributed; there are no benefits for the hubs. IPFS hubs store Community storage IPFS queries. Connection hubs with each other and transfer objects. Such articles refer to records and other systems of knowledge. The IPFS Protocol is divided into a heap of sub-conventions which are accountable for specific usefulness:

a) Characters - oversee hub personality age and confirmation.
b) System - oversees associations with different friends, utilizes different hidden system conventions.
c) Steering - Keeps data up for specific friends and things to search. Responds to local and distant enquiries. Defaults to a DHT but is exchangeable.
d) Trade - a novel square trade convention (BitSwap) that administers productive square appropriation. Demonstrated as a market, feebly boosts information replication. Exchange Strategies swappable.
e) Items - a Merkle DAG of substance tended to changeless articles with joins. Used to speak to subjective data structures, for example record chains of command and correspondence frameworks.
f) Records - formed document framework chain of command enlivened by Git.
g) Naming - A self-confirming changeable name framework.

Solidity:

Solidity is an organized document, an essential language of the level for the actualization of keen agreements. Brilliant agreements are systems that manage record keeping within the Ethereum State. This has been impacted by C++, Python and JavaScript and is designed to concentrate on the Ethereum Virtual Machine (EVM) and is dynamically constructed, underpins legacy, libraries and complex client types characterized among various highlights.

With Solidity you can make contracts for utilizations, for example, casting a ballot, crowd funding, dazzle barters, and multi-signature wallets. When sending contracts, you should utilize the most recent discharged form of Solidity. This is on the grounds that breaking changes just as new highlights and bug fixes are presented normally.

REACT: REACT (otherwise called React.js or ReactJS) is a JavaScript library for building UIs. It is kept up by Facebook and a network of individual designers and organizations. Respond can be utilized as a base in the advancement of single-page or portable applications. Be that as it may, React is just worried about rendering information to the DOM, thus making React applications for the most part requires the utilization of extra libraries for state the executives and routing. Redux and React Router are individual instances of such libraries.

The steps wise usage is a following:

- The user is asked to upload a file.
- The document is transferred to ipfs and it restores the hash of the record which is a CID.
- This CID (hash) is put away in the Ethereum keen agreements conveyed in the rinkeby test organize.
- The user on visiting the home page with metamask logged in to rinkeby network, shows a list of documents he has previously uploaded into the

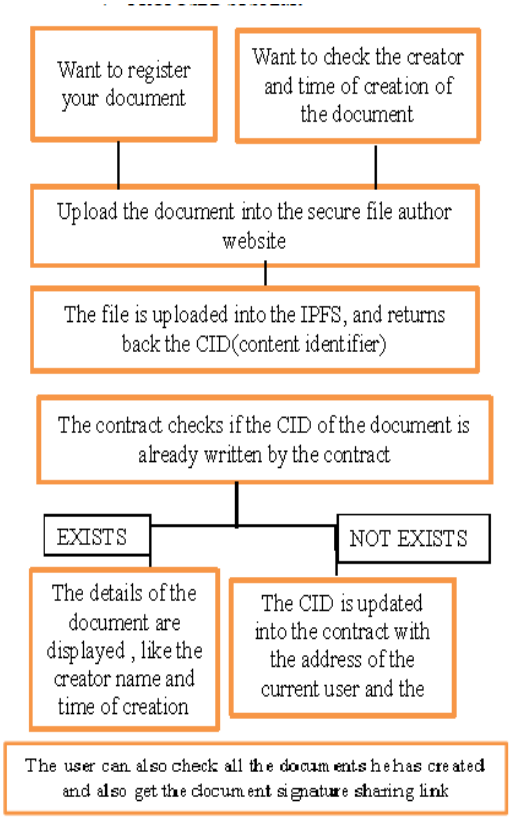
May-June 2020
ISSN: 0193-4120 Page No. 4715-4722

network, he also gets a link to docsign page, which can be shared with the fellow members who are required to sign the document.

- In docsign page, given the file hash we can check who signed the document, view the document and also if agreed to what document says to sign.
- When the same file is uploaded again by the other user, he is notified that there is a specific file which generates the same hash already in the network**.**

5. Implementation

Proposed System:



The Digital notary is the first stage of the document where the user will be asked whether to register the document or to check the creator and time of creation.

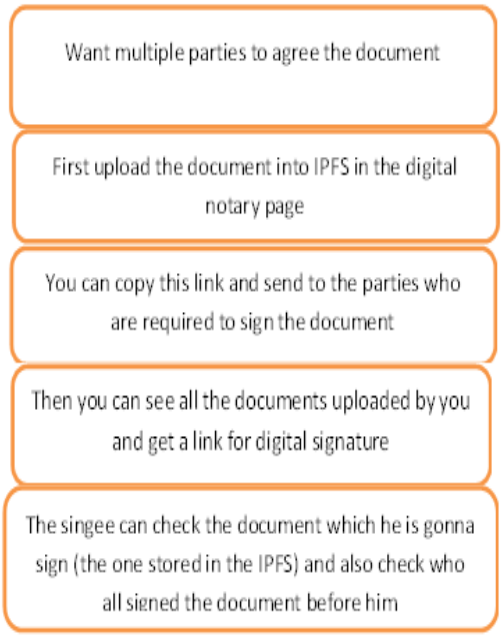
In case of registering the document it will be uploaded over a Secure file author website then the contract checks the cid of the document whether the document is already written on the document.

The file is uploaded into the IPFS only if there are no duplicates of the file and then generates a cid.

There are two cases with CID there if the cid generated is present the it returns the creator name and time of its creation

Else the cid is updated under the current user and current time is assigned to the document.

The user can check all the documents created and also retrieve the document signature sharing link for the files.



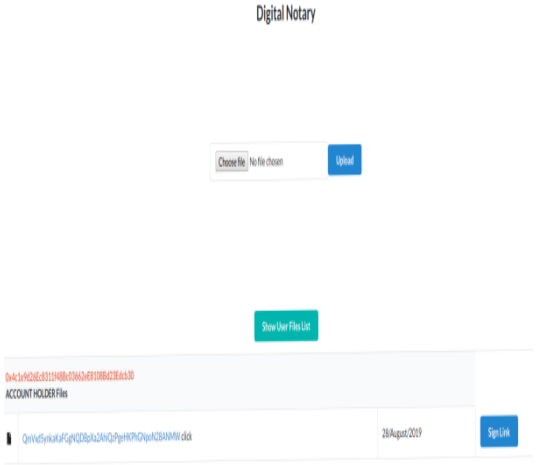
This is the second stage of the application if the user want multiple parties to agree over a single document the creator has to upload the file over the IPFS which is the first stage.

There you can copy the link provided and share it over parties whom the user wants to provide access and sign the document

The user will be able to see all the documents uploaded and get link for the digital signature

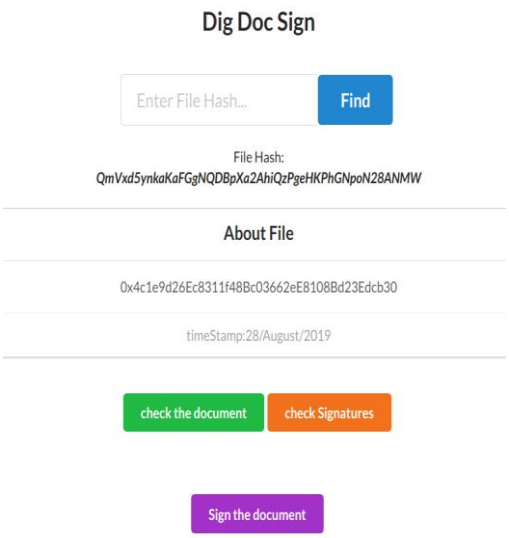
The parties who is signing the document has the access for checking the signatures done before the user which is stored on the IPFS

6. Results and Discussions



Here we can upload the file (or) you can check the files of the user who is trying to upload.

May-June 2020
ISSN: 0193-4120 Page No. 4715-4722



Here in this stage we can check for the hash of the file and who signed the document and the document can also be viewed.

7. Conclusion

This paper expresses the importance of Block Chain Technology Applications and impact of Smart contract. Modules such as IPFS, React, Ethereum, Solidity, Block chain are used for file authorization.

The application is developed for a secured access for a file on the blockchain network and helps in viewing the content like who has signed the document and who has the viewed the document. This helps sensitive data from data leakage and tampering. In case of a similar file which is already on the network is uploaded by another user the application notifies the user and most importantly helps in the removal of the middleman who is responsible for the contract between the parties.

References

[1] Nakamoto, Satoshi. *Bitcoin: A peer-to-peer electronic cash system*.Manubot, 2019.

[2] Buterin, Vitalik. "Ethereum white paper: a next generation smartcontract & decentralized application platform.

[3] Nakamoto, Satoshi. "Re: Bitcoin P2P e-cash paper." *The Cryptography Mailing List* (2008).

[4] Hasan, Haya R., and et al. "Proof of delivery of digital assets using blockchain and smart contracts." *IEEE Access* 6 (2018): 65439-65448.

[5] Griggs., et al. "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring." *Journal of medical systems* 42.7 (2018): 130.

[6] Rifi, Nabil, et al. "Towards using blockchain technology for eHealth data access management." *2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME)*. IEEE, 2017.

[7] Carvalho, David Alexandre Milheiro de. *Towards the detection of encrypted peer-to-peer file Sharing Traffic and peer-to-peer TV traffic using deep packet inspection methods*. Diss. 2009.

[8] Wang L, Kangasharju J. Measuring large-scale distributed systems: case of bittorrent mainline dht. InIEEE P2P 2013 Proceedings 2013 Sep 9 (pp. 1-10). IEEE.

[9] Cohen, Bram. "Incentives build robustness in BitTorrent." *Workshop on Economics of Peer-to-Peer systems*. Vol. 6. 2003.

[10] J. H. Howard,M. J. West, et al. Scale and performance in a distributed file system. ACM Transactions on Computer Systems (TOCS), 6(1):51–81, 1988.

[11] J. Kubiatowicz, W. Weimer, et al. Oceanstore: An architecture for global-scale persistent storage. ACM Sigplan Notices, 35(11):190–201, 2000.

[12] D. Levin,B. Bhattacharjee, et al. Bittorrent is an auction: analyzing and improving bittorrent's incentives. In ACM SIGCOMM Computer Communication Review, volume 38, pages 243–254. ACM, 2008.

[13] Benet, Juan. "Ipfs-content addressed, versioned, p2p file system." *arXiv preprint arXiv:1407.3561* (2014).

[14] Szabo, Nick. "The idea of smart contracts." *Nick Szabo's Papers and Concise Tutorials* 6 (1997).

[15] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things. Ieee Access. 2016 May 10;4:2292-303.

[16] Mettler, M., 2016, September. Blockchain technology in healthcare: The revolution starts here. In *2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom)* (pp. 1-3). IEEE.

[17] Asaph Azaria, Ariel Ekblaw, Thiago Vieira and Andrew Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management", , International Conference on Open and Big Data (OBD), 2016

[18] Jie Zhang, Nian Xue, and Xin Huang, "A Secure System For Pervasive Social Network-Based Healthcare", IEEE Access (Volume: 4), 2016

[19] Sayed Hadi Hashemi, Faraz Faghri, Paul Rauschy and Roy H Campbell, "World of Empowered IoT Users", 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), 2016

[20] Trent McConaghy, Rodolphe Marques, Andreas Muller, Dimitri De Jonghe, T. Troy McConaghy, Greg McMullen, Ryan Henderson, Sylvain Bellemare, and Alberto Granzotto, "BigchainDB: A Scalable Blockchain Database", [Online], Available: bigchaindb.com/whitepaper

[21] Kyle Croman, Christian Decker, Ittay Eyal,

May-June 2020
ISSN: 0193-4120 Page No. 4715-4722

Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi1, Emin Gun Sirer, Dawn Song, and Roger Wattenhofer, ”On Scaling Decentralized Blockchains”, Initiative for CryptoCurrencies and Contracts (IC3), 2016

[22] Deloitte UK, Blockchain Key Challenges, [Online], Available: deloitte.com/content/dam/Deloitte/uk/Documents

[23] Ben Dickson, Blockchain could completely transform the music industry, TechTalks, [Online], Available: venturebeat.com/2017/01/07/blockchaincould-completely-transform-the-music-industry/

[24] Don Tapscott and Alex Tapscott, How Blockchain Technology Can Reinvent The Power Grid, 2016, [Online], Available: http://fortune.com/2016/05/15/blockchain-reinvents-power-grid/

[25] Application-specificintegratedcircuit,a.URL https://en.wikipedia.org/wiki/Application-specific_integrated_circuit.https://web.archive.org/web/20170929032958/https://en.wikipedia.org /wiki/Application-specific_integrated_circuit.

[26] ASIC,b.URL{https://en.bitcoin.it/wiki/ASIC}. https://web.archive.org/web/20170929042224/https://en.bitcoin.it/wiki/ASIC. Elliptic Curve Digital SignatureAlgorithm.URLhttps://en.wikipedia.org/wiki/

[27] Elliptic_Curve_Digital_Signature_Algorithm.https: //web.archive.org/web/20170916033830/https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm.

[28] Lattice (order). URL https://en.wikipedia.org/wiki/Lattice_(order).https://web.archive.org/save/https://en.wikipedia.org/wiki/Lattice_(order). Secp256k1.URLhttps://en.bitcoin.it/wiki/Secp256k1.https://web.archive.org/web/20170916032105/https://en.bitcoin.it/wiki/Secp256k1.

[29] Pierre Arnaud, Mathieu Schroeter, and Sam Le Barbare. Electrum, 2017. URL https://www.npmjs.com/package/electrum.https://web.archive.org/save/https://www.npmjs.com/package/electrum.

[30] Jacob Aron. BitCoin software finds new life. New Scientist, 213(2847):20, 2012. URL http://www.sciencedirect.com/science/article/pii/S0262407912601055.

[31] Adam Back. Hashcash - Amortizable Publicly Auditable Cost-Functions. 2002. URL http://www.hashcash.org/papers/amortizable.pdf .https://web.archive.org/web/20170810043047/ht tp://www.hashcash.org/papers/amortizable.pdf.

[32] Roman Boutellier and Mareike Heinzen. Pirates, Pioneers, Innovators and Imitators. In Growth Through Innovation, pages 85–96. Springer, 2014. URLhttps://www.springer.com/gb/book/9783319040158.URLavailableathttp://wiki.erights.org/wiki/Documentation.https://web.archive.org/web/20170810040208/https://www.springer.com/gb/book/9783319040158.

[33] T. Rightmesh. (Mar. 2018). Rightmesh is Starting a Revolution With Blockchain and Mesh Networks. [Online]. Available: https://yourstory.com/2018/03/rightmesh-blockchain-mesh-networks

[34] P. Anderson, ‘‘BOINC: A system for public-resource computing and storage,’’ in Proc. 5th IEEE/ACM Int. Workshop Grid Comput., Nov. 2004, pp. 4–10.

[35] L. Beberg, D. L. Ensign, G. Jayachandran, S. Khaliq, and V. S. Pande, ‘‘Folding home: Lessons from eight years of volunteer distributed computing,’’ in Proc. IEEE Int. Symp. Parallel Distrib. Process., May 2009, pp. 1–8.

[36] Dickson. (Dec. 2016). How Blockchain Can Create the World’s Biggest Supercomputer. [Online]. Available: https://techcrunch.com/2016/12/27/ how-blockchain-can-create-the-worlds-biggest-supercomputer

[37] Z. Hong, Z. Wang, W. Cai, and V. C. M. Leung, ‘‘Connectivity-aware task outsourcing and scheduling in D2D networks,’’ in Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN), Jul./Aug. 2017, pp. 1–9.

[38] I. Baumgart and S. Mies. S/kademlia: A practicable approach towards secure key-based routing. In Parallel and Distributed Systems, 2007 International Conference on, volume 2, pages 1–8. IEEE, 2007..

[39] Beikverdi and J. S. Song, ‘‘Trend of centralization in bitcoin’s distributed network,’’ in Proc. IEEE/ACIS 16th Int. Conf. Softw. Eng., Artif. Intell., Netw. Parallel/Distrib. Comput. (SNPD), Jun. 2015, pp. 1–6.

[40] Natoli and V. Gramoli, ‘‘The blockchain anomaly,’’ in Proc. IEEE 15th Int. Symp. Netw. Comput. Appl. (NCA), Oct./Nov. 2016, pp. 310–317.

[41] K. O’Hara, ‘‘Smart contracts–dumb idea,’’ IEEE Internet Comput., vol. 21, no. 2, pp. 97–101, Mar./Apr. 2017.

[42] N. Atzei, M. Bartoletti, and T. Cimoli, ‘‘A survey of attacks on Ethereum smart contracts (SoK),’’ in Proc. 6th Int. Conf. Princ. Secur. Trust, vol. 10204. New York, NY, USA: Springer-Verlag, 2017, pp. 164–186.

[43] M. Wohrer and U. Zdun, ‘‘Smart contracts: Security patterns in the Ethereum ecosystem and solidity,’’ in Proc. Int. Workshop Blockchain Oriented Softw. Eng. (IWBOSE), Mar. 2018, pp.

May-June 2020
ISSN: 0193-4120 Page No. 4715-4722

2–8.

[44] K. Bhaskaran et al., ‘‘Double-blind consent-driven data sharing on blockchain,’’ in Proc. IEEE Int. Conf. Cloud Eng. (IC2E), Apr. 2018, pp. 385–391.

[45] K. Croman et al., ‘‘On scaling decentralized blockchains,’’ in Proc. Int. Conf. Financial Cryptogr. Data Secur. Berlin, Germany: Springer-Verlag, 2016, pp. 106–125.

[46] S. Rouhani and R. Deters, ‘‘Performance analysis of Ethereum transactions in private blockchain,’’ in Proc. 8th IEEE Int. Conf. Softw. Eng. Service Sci. (ICSESS), Nov. 2017, pp. 70–74.

[47] Rosic. (Oct. 2017). Proof of Work Vs Proof of Stake: Basic MiningGuide.[Online].Available: https://blockgeeks.com/guides/proof-of-workvs-proof-of-stake

[48] G. Greenspan. (2015). Multichain Private Blockchain–White Paper. [Online].Available:https://www.multichain.com/download/MultiChainWhite-Paper.pdf

[49] J. R. Douceur, ‘‘The sybil attack,’’ in Peer-to-Peer Systems. Berlin, Germany: Springer, 2002, pp. 251–260.

[50] A.Back. (Aug. 2002). Hashcash—A Denial of Service Counter-Measure.[Online].Available: http://www.hashcash.org/papers/hashcash.pdf