European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 03, 2020

Blockchain-Based Decentralized Constrained Framework in Secure Transaction using Exodus

K. Berlin Sujo[1], K. Logu[2]

[1]UG Student ,[234]Assistant Professor
Department of Computer Science and Engineering
SAVEETHA SCHOOL OF ENGINEERING
SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCES,
SAVEETHA NAGAR, THANDALAM, CHENNAI - 602105

Abstract: Secure and stable cryptographic cash key affiliation is huge right by and by cash considering how the keys are the most ideal approach to manage find a better than average pace. Despite the way where that Exodus wallet plans have been proposed, some application goals and common security dangers notwithstanding everything exist. At this moment, propose a novel cryptographic cash wallet the administrators plot subject to Decentralized Multi-Constrained Derangement (DMCD) Hybird blockchains to store the keys securely and dependably in a decentralized framework. Filling in as the data stream framework, DMCD has high data dissipating and a staggering comprehension between the pace of additional room use and commitment, which can guarantee the security and nature of the key saving and recovery. In our approach, to adjust to the issue that center centers are as routinely as conceivable on the web and isolated in the decentralized structure, we use a Shamir-Kademlia-Neighbor (SKN) riches procedure to ensure the high openness of set aside key. Then, for achieving puzzling correspondence during DMCD data dispersal, in setting on the Kademlia show up, we change the Client/Server (C/S) framework for Hordes show to a decentralized variation. All the proposed advances can ensure that our arrangement constrains sublimely in a decentralized mode. The evaluations and assessments show that our game-plan is beneficial, stable, and secure in the decentralized framework. Our proposed is Exodus it's not just cryptographic cash is a phase for Decentralized Multi-Constrained Derangement (DMCD) Hybird blockchains(HB). We give modernized trust signature figuring to checked trade. We show that the trade designing time won't be basically influenced considering the structure nonattendance of goliath worth through wide duplicates on a private Exodus sort out.

Keywords: DMCD, HB, SKN, EXODUS.

1. INTRODUCTION

A blockchain is an open record of information amassed through a structure that sits over the web. It is the course by which this information is recorded that gives blockchain its notable potential. Blockchain movement isn't an alliance, nor is it an application, yet rather an altogether better method for chronicling data on the web. The progress can be used to make blockchain applications, for instance, social affiliations, parcels, games, exchanges, taking care of stages, hurling a studying structure structures, check markets, online shops and generously more. At this moment, resembles the web, which is the explanation some have named it "The Internet 3.0". The information recorded on a blockchain can take on any

structure, whether or not it be recommending a trade of money, ownership, a trade, someone's character, a discernment between two social affairs, or even how much effect a light has used. Regardless, to do so requires an approval from a couple of contraptions, for instance, PCs, on the framework. Right when a seeing, moreover called a perception, is come to between these devices to store something on a blockchain it is unquestionably there, it can't be tended to, cleansed or changed, without the data and support of the people who made that record, additionally as the more broad structure. By and large, each square contains the data it is recording, for example a trade like 1 Lisk token being sent from Alice to Bob, in like manner as timestamps of when that information was recorded. It will in like manner join a robotized etch related with the record that made the record and a superb specific join, as a hash (think of it as a moved stand-apart etching), to the past square in the chain. It is this alliance that makes it immense for any of the information to be changed or for a square to be presented between two existing squares. To do so all after squares would ought to be adjusted as well. At the present time, square strengthens the past square and the security of the entire blockchain considering the way where that it prescribes more squares would ought to be changed to disturb any information. Decentralization is the route toward dissipating and scattering power away from a central position. Everything considered cash related and regulatory structures, which are starting at now in closeness, are joined, suggesting that there is a single most critical expert liable for directing them, for instance, a national bank or state mechanical party. There are a few essential burdens to this procedure, starting from the manner by which that any central master in like manner recognize the development of a singular clarification behind disillusionment in the system: any breakdown at the most raised inspiration driving the chain of significance of power, whether or not unplanned or purposeful, unavoidably unfairly impacts the entire structure.

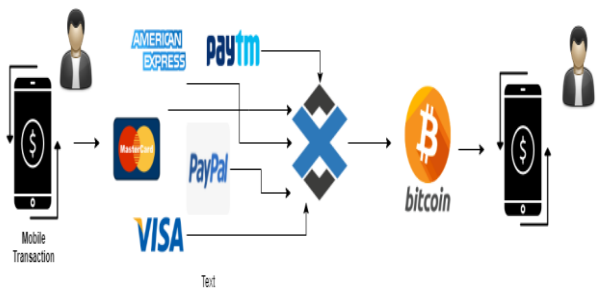

Fig.1 Overall Architecture

Our proposed is Exodus it's not just cryptographic cash is a phase for Decentralized Multi-Constrained Derangement (DMCD) Hybird blockchains(HB). We give modernized trust signature figuring to checked trade. We show that the trade arranging time won't be basically affected considering the structure nonattendance of goliath worth through wide duplicates on a private Exodus sort out.

2. RELATED WORKS

Blockchain is a development making the normal library thought from passed on frameworks a reality for various application spaces, from the modernized money one to possibly any mechanical structure requiring decentralized, solid, trusted, and motorized dynamic in a multi-accomplice circumstance. Notwithstanding, the credible perfect conditions in utilizing blockchain instead of some other standard methodology, (for example, concentrated

databases) are not completely fortifying to date, or maybe there is a solid key for a vademecum directing sketchers toward the correct choice about when to comprehend blockchain or not, which sort of blockchain better meets use-case necessities, and how to utilize it. Right now, target equipping the structure with such a vademecum, while giving a general introduction of blockchain that goes past its usage in Bitcoin and keeping an eye out for an affirmation of the huge making that rose over the most recent couple of years. We draw the key necessities and their headway while going from permissionless to permissioned blockchains, showing the allotments among proposed and attempted accord parts, and depicting existing blockchain stages.

Adaptability issue of blockchain shows has gotten huge idea. Sharding is one of the most encouraging reactions for scale blockchain. The focal thought behind sharding is to portion the blockchain organize into various sheets where each admonishing social affair structures a substitute system of exchanges. As of now, propose a numerical model to gut the security of sharding-based blockchain appears. Similarly, we separate unmistakable sharding shows including RapidChain, OmniLedger, and Zilliga to recognize our model. The key duty of our paper is to bound the goof likelihood for one driving get-together of trustees right now each age utilizing likelihood limits for wholes of upper-compelled hypergeometric and binomial dispersals. In like way, this paper duty responds to the going with critical mentioning: "how to keep the mix-up likelihood, for a surrendered sharding appear, more minor than a predefined limit?". Three likelihood limits are utilized: Chebyshev, Hoeffding, and Chvátal. To layout the abundancy of our proposed model, we direct a numerical and relative evaluation of past what many would consider possible.

Seeing check of Alzheimer's torment (AD) from neuroimaging data, for instance, MRI through AI has been a subject of befuddling assessment starting late. The foreseen achievement of huge learning in PC vision has progressed such research. In any case, standard goals with such counts are reliance on unremitting structure pictures, and the need of cautious improvement of the disengaging through of gigantic structures. Beginning at now, have a go at understanding these issues with move seeing, where the top level VGG technique is instated with pre-segregated through loads from epic benchmark datasets including trademark pictures. The structure is then changed with layer-wise tuning, where only a pre-shown get-together of layers are set up on MRI pictures. To pull back the status data size, we use picture entropy to pick the most basic cuts. Through experimentation on the ADNI dataset, we show that with the structure size of 10 to different occasions humbler than the other contemporary frameworks, we land at the bleeding edge execution in AD versus NC, AD versus MCI, and MCI versus NC request issues, with a 4% and a 7% improvement in exactness vastly level for AD versus MCI and MCI versus NC, self-rulingly. We what's more give a point by point evaluation of the effect of the exceptional coordinating data demand structure, changing the status size, and changing the degree of layers to be adjusted. Finally, we give class starting maps (CAM) that show how the proposed model spotlights on discriminative picture zones that are neuropathologically major and can help the human affiliations skilled in discharging up the model's immense force process.

The abundant improvement of cryptographic sorts of money and their covered up blockchain development has restored Szabo's uncommon thought of sharp understandings, i.e., PC shows that are proposed to thusly sponsorship, check, and grasp the exchange and execution of motorized understandings without focal virtuosos. Astonishing understandings can locate a wide level of potential application conditions in the moved economy and savvy endeavors, including money related affiliations, the authorities, strong affiliations, and Internet of Things, among others, and besides have been stimulated into the standard blockchain-based improvement stages, for example, Ethereum and Hyperledger. In any case, brilliant

understandings are as yet a long way from make, and fundamental express difficulties, for example, security and certification issues are so far imagining further research attempts. For example, the most acclaimed case may be "The DAO Attack" in June 2016, which provoked more than $50 million Ether moved into a foe's record. Right now, endeavor to introduce a capable and complete chart of blockchain-related sharp understandings, concentrating on vitalizing further research toward this rising appraisal zone. We from the earliest starting point demonstrated the working instrument and standard foundation of blockchain-connected with critical understandings, and proposed an appraisal structure for tricky understandings subject to a novel six-layer building. Second, both the particular and authentic difficulties, also as the pushing appraisal drives, are recorded. Third, we indicated a couple of run of the mill application conditions. Close to the end, we examined the future headway instances of canny understandings. This paper is made game courses of action for give unsurprising direction and reference to future research attempts.

The electronic law based has made after some time as a substitution to the paper-based vote based to diminish the redundancies and varieties from the standard. The unquestionable viewpoint appeared over the most recent two decades endorses that it has not been so gainful in perspective on the security and confirmation gives up observed after some time. This paper proposes a system by utilizing persuading hashing procedures to guarantee the security of the information. Square creation and square fixing is exhibited right now. The presentation of a square fixing idea helps in making the blockchain adaptable to address the issue of the analyzing structure. The utilization of consortium blockchain is upheld, which guarantees that the blockchain is obliged by a directing body (e.g., political race commission), and no unapproved access can be made using outside. The structure proposed right now the trustworthiness of the watching out for framework, hashing tallies' utility, square creation and fixing, information variety, and result assertion by utilizing the adaptable blockchain technique. This paper reports to get the security and information the board difficulties in blockchain and gives an improved appearance of the electronic vote based system.

3. CRYPTOCURRENCY SYSTEM

A cryptographic cash is a progressed or virtual money that is guaranteed by cryptography, which looks extraordinary difficult to phony or twofold spend. Away from sorts of cash are decentralized frameworks in peril to blockchain progress—a scattered record wrapped up by a pivotal procedure of PCs. A portraying feature of electronic sorts of cash is that they are all around not gave by any central force, rendering them theoretically safe to government impedance or control Cryptocurrencies are structures that consider the guaranteed parts online which are picked in like manner as virtual "tokens," which are would with everything considered by record zones inside to the system. "Crypto" attire the apparent encryption checks and cryptographic structures that shield these segments, for instance, atypical breeze encryption, open private key matches, and hashing limits.

Blockchain, a trustless and appropriated accord structure, licenses you to send correspondingly as get money from someone without going to hard to land at affiliations. By making an appropriated approach of records that work together to keep all trades, understandings and records open, they take out the necessity for intercession to epic degree by procedures for a thought named as Proof of work. Underwriting of work is a need to layout a senseless PC figuring, other than called mining, that ought to be acted in order to make another social event of trustless trades (the alleged square) on a disseminated record called blockchain. All the structure's excavators battle to be the first to find a response for the canny issue that stacks the contender cripple, an issue that can't be comprehended in upsetting affinities then again with through creature power, on an exceptionally fundamental level

requiring impossible endeavors. Unequivocally when an excavator finally finds the right framework, he/she verbalizes it to the whole structure all the while, getting a cryptographic cash prize (the prize) gave by the show.

Bitcoin has a cryptographic security feature to ensure that specific the owner of a Bitcoin can spend it. The idea is that the owner makes two numbers—a private key that is puzzle and an open key that is passed on. The open key can be successfully made utilizing the private key, at any rate not the a substitute way. A pulling in can be used to watch that the owner holds the private key, without revealing the private key, using a system known as an elliptic turn signature plot. Starting at now, recipient can watch that the owner has the private key and right now the bit of slack to spend the Bitcoin.

A .Bitcoin

Lets start with Bitcoin. The major pushed money to make was Bitcoin (BTC), it relies on the SHA-256 count. This moved thing was conceptualized at a whitepaper written in 2009 by a pseudonymous writer who passed by the name Satoshi Nakamoto. Over the range Bitcoin's key four decades, the market cost of one Bitcoin has contracted from under $0.01USD to over $250USD. The staggeringly flawed cost has passed on Bitcoin a join with try choice for sellers endeavoring to profit by advance speculation, while at verifiably an indistinguishable time the business weakness has gotten focal pack money related directors and a little piece at a time customers hesitant to take a force for freeing degrees from time. A single Bitcoin can be spent at lacking develops that Can be as spurned as 0.00000001 BTC per trade. The humblest improvement of a Bitcoin is obviously known as a Satoshi, called after the first whitepaper maker. The show thinks about steady trades the event the estimation of BTC to moves to where little scale trades will become standard spot. The development in the estimation of BTC is customary considering the course that there's a tremendous to the whole degree of Bitcoin will ever be made. Decidedly when the Bitcoin blockchain is done, customers can on a fundamental level stream the coin that paying little mind to everything exists on the structure.

B. Litecoin (LTC)

Litecoin (LTC) uses the Scrypt encryption check, instead of SHA-256. One of the goals of Litecoin is have trades state at a snappier speed stood segregated from Bitcoin make, about as use an estimation that has been secured to vivified contraption mining degrees of progress like ASIC. The entire degree of Litecoin that is open for mining and course is on various occasions the level of Bitcoin, which interprets there will be fourfold the level of Litecoin accessible to Bitcoin.

C. Ethereum (ETH)

Stage that interfaces sharp understandings and scattered applications (DApps) to be made and work with no huge time, winding, impedance or control from a pariah. All through Ethereum had developed a pre-can filter for after ether that had gotten a surprising response. The applications on Ethereum are kept up with no other individual sort out express cryptographic token, Ether. Ether appears, apparently, to be a vehicle for moving around on the Ethereum structure, and is filtered for all around structures attempting to make and work programs inside Ethereum.

D. Zcash

A decentralized and open-source cryptographic cash incited in the second bit of 2016, and it truly looks verifies. In case Bitcoin looks like http for money, Zcash is https, this is in a general sense the course by which Zcash depicts. Zcash offers security and watching straightforwardness of trades. At the present time, https, Zcash cases to give extra verification

or security where all trades are recorded and printed inside a blockchain, yet nuances, for instance, the sender, recipient, and whole stay private. Zcash offers its customers the decision of 'authenticated' trades, which see substance to be mixed using advanced cryptographic system or zero-data check structure called a zk-SNARK made by its gathering.

E. Run

Run (from the most convenient beginning stage known as Darkcoin) is an extremely incredible social gathering of Bitcoin. Run offers feasibly boss request as it deals with a decentralized mastercode structure which produces trades untraceably. Influenced in January 2014, Dash experienced a creation fan after in a short degree of time. This mechanized cash was made and passed on by Evan Duffield and could be mined using a CPU or GPU. The rebranding didn't change any of its innovative features, for instance, Darksend, InstantX.

4. EXODUCS

Mass advancement is a multi-resource modernized money wallet as it underpins more than 80+ coins and tokens. It has a central interface which can be utilized enough even by the understudy brokers. Utilizing the joined Exodus Exchange, you can't purchase/sell cryptographic sorts of money utilizing fiat cash at any rate can essentially trade between the modernized resources. Mass headway isn't viewed as the best choice to store huge degrees of bleeding edge money as it isn't as strong as a mechanical gathering wallet. That is the clarification it supports the clients to go for gear wallets like Trezor, KeepKey or Ledger for overseeing gigantic level of cutting edge resources. The Exodus wallet has a worked in exchanging highlight. This is given by the trade sort out Shapeshift. It makes swapping one cash for another fast and essential. It in actuality won't offer as low costs as you will discover on trades like CoinBase and Bittrex, yet it is shocking for non-fit shippers needing to purchase evolving cryptos. Mass improvement doesn't offer two-factor attestation. This makes it less perplexing for originators to utilize a keylogger to break into a wallet. All that certifies the wallet is a solitary question key. Once in, a thing engineer pushes toward the mechanized sorts of money put aside there. It's unmitigated expected to have a multi-signature wallet on a PC and a phone. Both of these contraptions must validate an exchange before it is given to the structure. This makes it essentially intelligently hard for planners to take spares since they should locate a reasonable pace instead of one. two security gives up that Exodus themselves don't get a handle on dealing with a monstrous proportion of mechanized money on their thing. The Exodus wallet is liberally intensely reasonable for use as a standard wallet.

A. Web Wallet

The Exodus wallet is all around more secure than a web wallet. Web wallets, similar to those found at trades, (for example, Coinbase), are the most simple to lose assets from. They have security hazards that relative wallets have. These wire the threat of the trade's focal servers being hacked and the danger of the partnership itself missing the mark. eb wallets are not fitting for overseeing cryptographic money. On the off chance that you are a working expert, you ought to go confronting the test. This is pondering the way in which that exchanging requires your coins to be open at short notice, so you can mishandle upgrades in the cost of certain pushed sorts of money. For one another individual, it's simply not worth overseeing benefits on a web wallet alliance.

B. Mechanical gets together Wallet

The Exodus wallet is totally less secure than either a paper or gadget wallet. Neither of these are constantly associated with the web like most programming wallets are. This lessens the odds of them being hacked. On the off chance that your thing wallet is on a PC that you utilize each day, the odds of you downloading malware or keyloggers are a lot higher. On the off chance that you need to store your cryptographic money for an essential stretch of time, paper or contraption wallets are the best other choice. Wallets like the Exodus wallet are radiant for individuals who utilize compelled extents of cryptographic money continually. They are in like way great in the event that you need to swap one induced money for another. In any case, Exodus isn't the best decision for skilled vendors. The Exodus wallet costs make it hard to get cash exchanging, regardless of whether it's more secure than keeping cash on a trade.

C. Segment Currencies

As the name proposes, these perfect conditions are generally for sections and are starting now and into the not all that far off called Payment Currencies. For instance, you could utilize fragment financial structures to pay for things or affiliations, manage your tabs, money out from front line cash related benchmarks to way to deal with fiat budgetary structures like the dollar, and so forth. While each motorized resource can hypothetically be utilized to pay for things, shipper get-together or approval by suppliers of thing and tries is reasonably paying little notice to what you look like at it for Payment Currencies. Specifically, cryptographic sorts of money like Bitcoin (BTC), Litecoin (LTC), Bitcoin Cash (BCH), and others are renowned and undeniable Payment Currencies

D. Blockchain Economies

Blockchain Economies, regardless called blockchain stages, take the comfort of blockchain movement more remote than just bits. These stages award you to make your own induced resources (consistently recommended as tokens), decentralized applications (Dapps, and so forth on their foundation. At this moment, stages become their own "Blockchain Economies" with various resources, applications, no two ways about it. Some Blockchain Economies you may have considered union Ethereum (ETH), Ethereum Classic (ETC), (EOS), (NEO), and Tron (TRX)

E. Security Coins

Some actuated resources are made with an element on security. In Privacy Coin exchanges, just the sender and recipient know the extent of coins executed. In addition, the evening out of a Privacy Coin wallet address is on a very basic level known by the proprietor of the wallet. This is rather than blockchains like those of Bitcoin, which show exchange wholes for each exchange besides as wallet address alters. Crypto resources like ZCash (ZEC), Monero (XMR), (PIVX, etc are events of Privacy Coins.

F. Utility Tokens

Utility tokens are provoked tokens that are utilized for a blockchain-based thing or alliance. They run on a blockchain arrange, or ceaselessly end, are somewhat a Blockchain Economy. Most utility tokens are ERC20 tokens that sudden spike looked for after for the Ethereum blockchain yet with the proceeded with appearance of other blockchain stages, other token sorts like TRC10 and TRC20 tokens have developed also.

G. Stable Coins

These central focuses are incredibly standard among typical focus people, as they generally have an equivalent cost (or mean to), rather than other electronic resources, which can change amazingly in respect. For instance, if a vendor imagines that a touch of breathing space will lose respect soon, they could sell the extraordinary circumstance for a stablecoin to forestall budgetary accident.

5. SIMULATION AND ANALYSIS

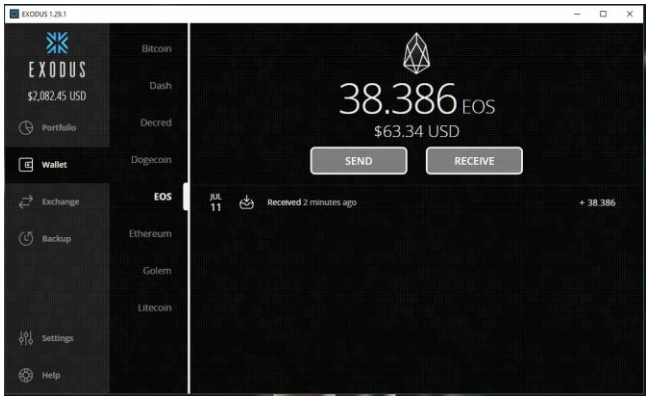

Fig.2 Exodus Simulator

Fig.2 shows the Exodus wallet you also now have the ability to exchange other assets for EOS tokens directly, very easily and with a simple process from their GUI

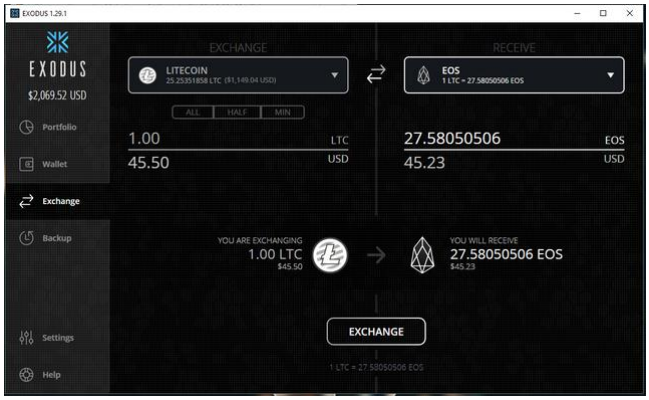

Fig.3 EOS Tokens

Fig.3 shows EOS Tokens currently valued less than 2.00 USD, I felt this was a great opportunity to pick up some more of these tokens

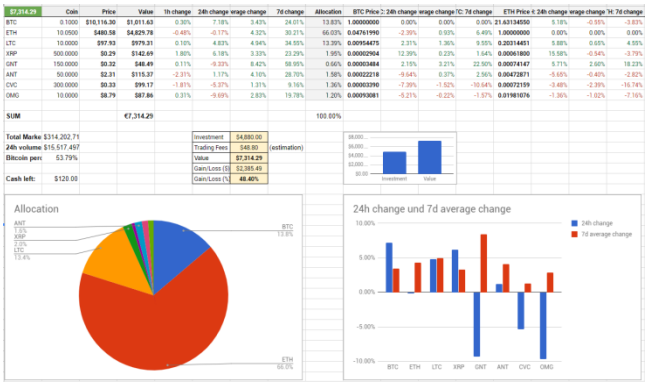

Fig.4 Exodus Comparsion

Fig.3 Shows the Bitcoin comparison between Exodus and Ethereum

Fig.5 Ethereum exodus wallet vs coinbase

Fig.5 shows the comparison between Ethereum exodus wallet vs coinbase

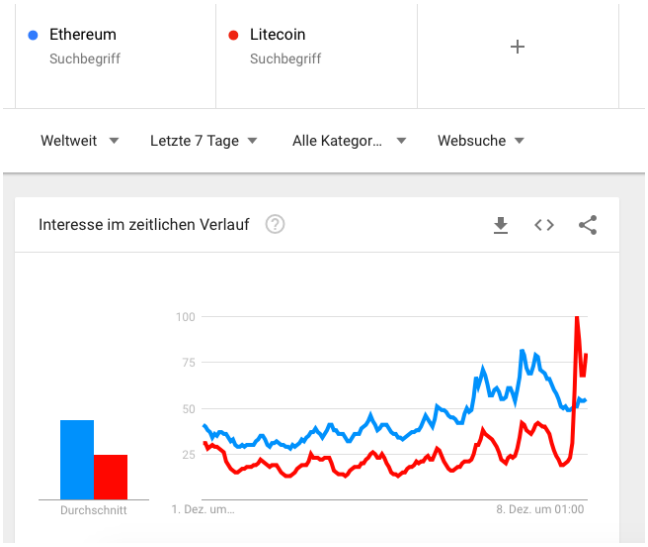

Fig 6 Litecoin

Fig.5 shows the comparison between Litecoin surpasses ethereum on google trends

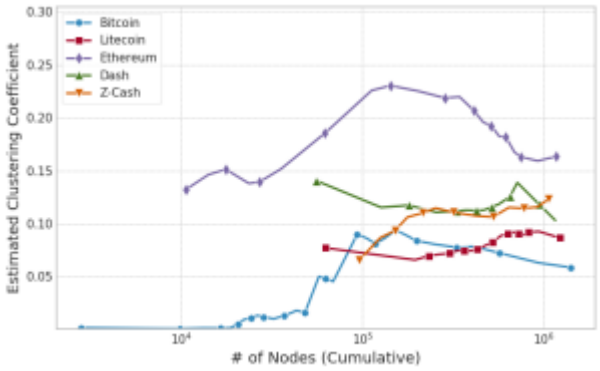

Fig 6 clustering the number of nodes

Fig. 6 shows the Clustering coefficient of CMTG vs the number of its nodes.

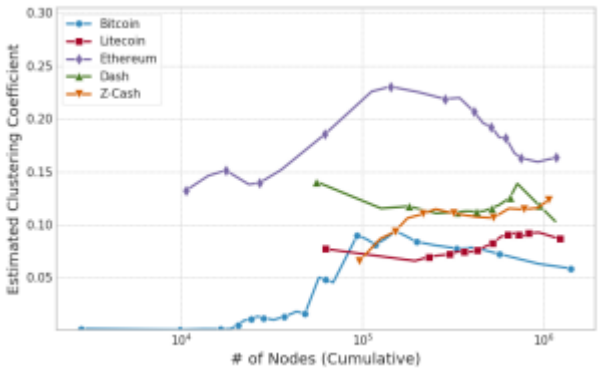

Fig 7 Maximum clique size

Fig 7 shows the maximum clique size of CMTG vs the number of its nodes.

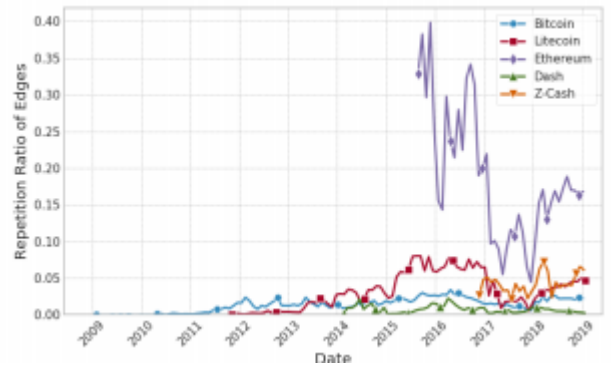

Fig 8 Repetition ratio of edges

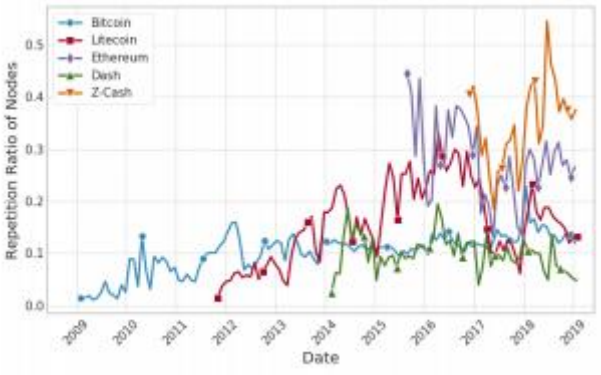

Fig 8 Repetition ratio of nodes

6. DISCUSSION AND CONCLUSION

It is noteworthy to comprehend blockchains as for bitcoin, yet you ought not recognize that all blockchain common structures need bitcoin fragments, for example, confirmation of work, longest chain rule, and so forth. Bitcoin is the head undertaking at keeping up a decentralized, open record with no suitable control or association. There are fundamental difficulties included private passed on records and blockchains can be sent to deal with different game-plans of issues. As ever, there are tradeoffs and upsides and disadvantages to each game-plan, and you have to consider these freely for every individual use case utilizing pushed trust signature mean affirmed exchange and better execution result.

7. REFERENCES

[1] Yining Hu, Ahsan Manzoor, Parinya Ekparinya, Madhusanka Liyanage, Kanchana Thilakarathna, Guillaume Jourjon, Aruna Seneviratne, "A Delay-Tolerant Payment Scheme Based on the Ethereum Blockchain" IEEE Access, 2019, pp. 33159 – 33172

[2] Tien Tuan Anh Dinh, Rui Liu, Meihui Zhang, Gang Chen, Beng Chin Ooi, Ji Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems" IEEE Transactions on Knowledge and Data Engineering, 2018, pp. 1366 – 1385

[3] Shangping Wang, Xu Wang, Yaling Zhang "A Secure Cloud Storage Framework With Access Control Based on Blockchain" IEEE Access, 2019, pp. 112713 – 112725
[4] Haya R. Hasan ; Khaled Salah "Proof of Delivery of Digital Assets Using Blockchain and Smart Contracts", IEEE,2018, pp. 2169-3536
[5] Ming Li, Jian Weng , Anjia Yang , Wei Lu , Yue Zhang , Lin Hou, Jia-Nan Liu, Yang Xiang, "CrowdBC: A Blockchain-Based Decentralized Framework for Crowdsourcing" IEEE Transactions on Parallel and Distributed Systems, 2018, pp. 1251 – 1266
[6] G. Wood, ''Ethereum: A secure decentralised generalised transaction ledger,'' Ethereum Project Yellow Paper, vol. 151, pp. 1–32, Apr. 2014.
[7] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, ''Eclipse attacks on bitcoin's peer-to-peer network,'' in Proc. USENIX Secur. Symp., 2015, pp. 129–144.
[8] P. R. Rizun, ''A transaction fee market exists without a block size limit,'' in Proc. Block Size Limit Debate Working Paper, 2015, pp. 1–16.
[9] J. Poon and V. Buterin, ''Plasma: Scalable autonomous smart contracts,'' White Paper, 2017, pp. 1–47.

[10] P. Rimba, A. B. Tran, I. Weber, M. Staples, A. Ponomarev, and X. Xu,''Comparing blockchain and cloud services for business process execution,'' in Proc. IEEE Int. Conf. Softw. Archit. (ICSA), Apr. 2017,pp. 257–260.

[11] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, ''Bitcoin-NG: A scalable blockchain protocol,'' in Proc. NSDI, 2016, pp. 45–59.

[12] G. Karame, E. Androulaki, and S. Capkun, ''Two bitcoins at the price of one? Double-spending attacks on fast payments in bitcoin,'' IACR Cryptol. ePrint Arch., Tech. Rep. 2012/248, 2012.

[13] Y. Sompolinsky and A. Zohar, ''Accelerating bitcoin's transaction processing. Fast money grows on trees, not chains,'' IACR Cryptol. ePrint Arch., Tech. Rep. 881, 2013.

[14] M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan, ''On the instability of bitcoin without the block reward,'' in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2016, pp. 154–167.

[15] J. Poon and V. Buterin, ''Plasma: Scalable autonomous smart contracts,'' White Paper, 2017,