

Technology Fundamentals of Blockchain and Consideration for Blockchain Security

U. Sai Ram, B. Surya Samantha

ABSTRACT---Blockchain has actually attracted interest as the next-generation economic technology because of its security that fits the informatization age. Extensive study is presently being performed in both the academic community and also sector using the Blockchain technology in many applications. Proof-of-Work, a cryptographic challenge, plays an important rôle in making certain BC security by keeping an electronic journal of purchases, which is taken into consideration to be incorruptible. In addition, BC makes use of an adjustable Public Key (PK) to tape the individuals' identification, which gives an added layer of privacy.

Index Terms : Blockchain (BC), Crypto-currency, Distributed Digital Ledger

I. INTRODUCTION

Blockchain (BC), the technology behind Bitcoin crypto-currency system, is thought about to be crucial for creating the foundation for making certain boosted security as well as privacy for numerous applications in numerous various other domain names consisting of the Web of Points (IoT) ecosystem. International study is presently being performed in both academic communities as well as market using Blockchain in diverse domain names. The Proof-of-Work (PoW) mathematical obstacle makes certain BC security by keeping an electronic journal of deals that is thought about to be unalterable. In addition, BC makes use of an adjustable Public Key (PK) to tape the customers' identification that offers an added layer of privacy. The effective fostering of BC has actually been executed in varied non-monetary systems such as in online ballot, decentralized messaging, dispersed cloud storage space systems, proof-of-location, health care, etc. Current research study short articles, as well as projects/applications, were evaluated to determine the application of BC for improved security and also to recognize its linked difficulties and also thence to recommend services for BC allowed improved security systems.

Cyber-attacks versus CIA homes create various disabilities on information depend on according to the weakened home. Particularly, undermining schedule stops information to be fetched just for the short-lived time period, yet procedures can be returned to as quickly as information come once again. Endangering privacy reveals rather exclusive information and also can not be changed, however, initial information is still

readily available and also useful, a minimum of to the level permitted by the caused damages (i.e., an organization sufferer of information leak might need to deal with financial effects). Rather, damaging information stability is an extremely destructive attack that constantly leads crucial concerns to information count on. Certainly, damaging information can go unseen and also drive procedures maliciously, by erasing certain entrances (i.e., to eliminate troublesome traces) or by changing specific areas of information (i.e., to transform information customers' behavior). In 2015, Kaspersky Laboratory figured out a large cyber-attack targeting over than 100 monetary institutes worldwide that siphoned off cash from account equilibriums for an approximated worth of around \$1 billion¹. In a different way from privacy as well as accessibility, as soon as stability is endangered there is no other way to recover the initial information, it is shed for life. For that reason, as honesty attacks are refined to be found as well as actually efficient, in this paper we concentrate on information stability as opposed to privacy or accessibility.

Information stability problems are worsened in cloud computer settings, as information proprietors barely manage where their information is saved, that can really access them, and also in which means. However, an increasing number of exclusive and also public organizations are outsourcing their information, be- create "it alleviates the worry of upkeep price in addition to the expenses of keeping information locally". For that reason, making certain information stability homes in cloud computer settings have actually come to be an immediate requirement to address.

As the groundwork of blockchain contain some combo of information resource, acquisition, surveillance, deal as well as additionally different other distributed device modern-day innovations, it is actually natural to visit if it is actually possible to make use of existing capacities of entirely expanded details along with details bodies through heavy duty combo right in to blockchain units. There exist available analysis study complications including multi-storage as well as additionally mark support, distinct acquisition concurrency variation, scalable investment throughput, professional as well as additionally reference details surveillance, sensible arrangement

Revised Manuscript Received on May15, 2019.

U. Sai Ram Assistant Professor Department of Information Technology, CBIT, Hyderabad, India

B. Surya Samantha Assistant Professor Department of Information Technology, CBIT, Hyderabad, India

tracking, relevant information protection and also personal privacy guarantees, aside from details water leak evasion.

Furthermore, although the blockchain information resource works with a very clear persistence of streaming business details, there is actually no one-size-fits-all information resource company for an use. While blockchain is actually in the beginning made to maintain offer info, there is actually an extending interest rate in offering analytics potentials in blockchain-based details units. Specifically, within this newspaper, our company will definitely make clear on information research problems like incorporated analytics for blockchain, along with details combo in addition to analytics throughout on-chain in addition to off-chain relevant information.

II. RELATEDWORKS

In this field, our company speak about the vital concept of blockchain along with the existing research. Our company also look into the information make use of blockchain in bitcoin.

Blockchain

A blockchain is actually a modern technology that enables all individuals to preserve a publication possessing all investment info as well as additionally to improve their diaries to keep security when there is actually a new offer. Since the advancement of the Web as well as additionally data security innovation has really created it possible for all attendees to verify the honesty of a bargain, the singular element of falling short to take place coming from the reliance on an accredited third celebration has really been actually addressed.

The blockchain has broker-free (P2P-based) qualities, consequently eliminating unneeded charges with p2p purchases without permission by a 3rd party. Given that possession of the purchase details by lots of people makes hacking tough, security cost is conserved, deals are immediately authorized and also taped by mass engagement,

and also punctuality is ensured. Taking into consideration that the hash truly worths spared in each peer in the block are actually influenced due to the really worths of the previous blocks, it is actually exceptionally challenging to misstate as well as additionally modify the subscribed info. Although relevant information adjustment is actually possible if 51% of peers are actually hacked at the precise very same opportunity, the assault scenario is actually truly remarkably difficult.

Community, key-based verification as well as additionally a hash component that may be decoded are actually each taken advantage of to provide protection in the blockchain. The ECDSA (Elliptic Shape Digital Hallmark Method) electronic hallmark formula, which affirms the digital hallmark created throughout a handle between individuals, is actually taken advantage of to confirm that the offer details has in fact certainly not been actually customized.

The blockchain is actually a managed guidelines that preserves details in a kind equivalent to a spread information resource as well as additionally is actually made to create aimlessly managing it daunting thinking about that the system people save in addition to verify the blockchain. Each block is actually a structure consisting of a header and also a body system. The header is composed of the hash really worths of the previous and also existing blocks in addition to the nonce. The block relevant information is actually scanned in the records resource utilizing the mark technique. Although the block performs certainly not possess the hash truly worth of the adhering to block, it is actually featured as a strategy (Body 1).

In addition, the body could be easily used, connected, in addition to boosted taking advantage of an available information as well as additionally investment files could be truthfully accessed to help make the packages social as well as likewise lower controlling expenditures.

Although making use of a confidential public key as account details makes it possible for one to recognize that sent out just how much to one more peer, it still guarantees privacy given that there is no chance of discovering info referring to the proprietor.

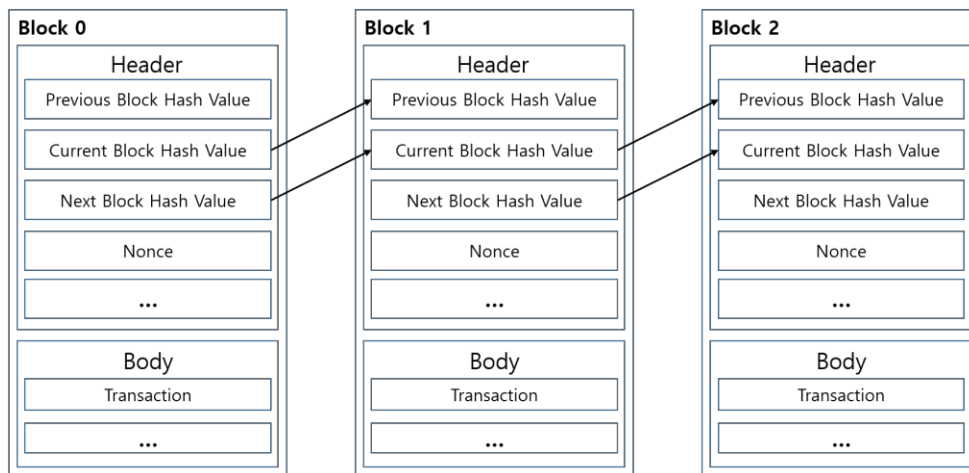


Figure 1. Blockchain connection structure

The hash feature is made use of to confirm that the block information including the purchase information is not modified and also to locate the nonce worth to obtain a brand-new block, along with to ensure the honesty of deal information throughout a bitcoin purchase. The integrity of the acquisition info could be verified using the public key-based data shield of encryption of the hash well worth of the bargain relevant information. Additionally, taking advantage of the beginning hash really worth, which compiles the hash really worth of each of the package info, produces it achievable for extremely effortless settlement of whether the bitcoin relevant information was actually tweaked since the source hash well worth is actually enhanced when the well worth is actually completely transformed concurrently.

There are actually tons of constant investigates to enrich safety and security using these attributes of the blockchain. Among the absolute most vital component of the blockchain is actually safety and security referring to the specific technique made use of in report shield of encryption along with there are actually investigation studies on precisely just how to shelter the personal technique. An assailant makes an effort a "reuse assault" along with different other assaults to receive the personal vital inhibited a peer's gizmo so as to hack the bitcoin. The enemy can hack the bitcoin because the information might be dropped if the assailant can acquire the individual trick. To resolve this trouble, research studies on using both software and hardware protections for accepting purchases are continuous.

Bitcoin is really at risk of infection by malware because it is usually sold extensively utilized gadgets such as peers' Computers or mobile phones. The malware permeating with numerous courses such as email, USB, or applications with inadequate security have to be found as well as deal with considering that it can contaminate a peer's tool. The demand for security is expanding, especially in professions of products made use of in video games because much of them utilize bitcoins. Because of this, there have actually been researching studies on spotting as well as dealing with malware in the video game atmosphere [9].

Permissioned/private blockchain. In Bitcoin, a social implementation of blockchain, bodies that join the transfer of homes are actually classified and also any type of type of body may acquire entailed. Meanwhile, considerable amounts of company systems may possess a need for a distributed publication that is actually simply on call to a closed community of prominent bodies. Approval blockchain advancements including Hyperledger Component [8] as well as additionally R3 Corda [5] have in fact been actually created to preserve these necessities, i.e., facilities obtaining included the world wide web- project is actually realized to see to it that their permissions may be pinpointed in addition to the jobs of a company are actually only visible to those people of organisation system that possess a criteria to realize

One of the durability of bitcoin is actually that it is actually testing to misstate in addition to change the publication given that many peers discuss the offer diary. Due to the fact that it takes the details videotaped the majority of the diaries, hacking is actually basically tough unless the rival tweaks and also misstates 51% of all peers' diaries, additionally if the info of some diaries are actually transformed. Still, there are actually concerns that 51% of the diaries may be misstated as well as likewise altered together thinking about increasing determining electrical power as well as additionally there are actually investigation studies highly recommending the intermediary verification operation or even type of the verification method so as to attend to the issue.

Smart agreement. Some dispersed journal innovations support an added capacity called a clever agreement, which resembles the idea of saved treatment in classic relational data sources somewhat. Smart agreements enable the common company procedures within a company network to be standardized, automated as well as imposed through computer system programs to boost the honesty of the journal.

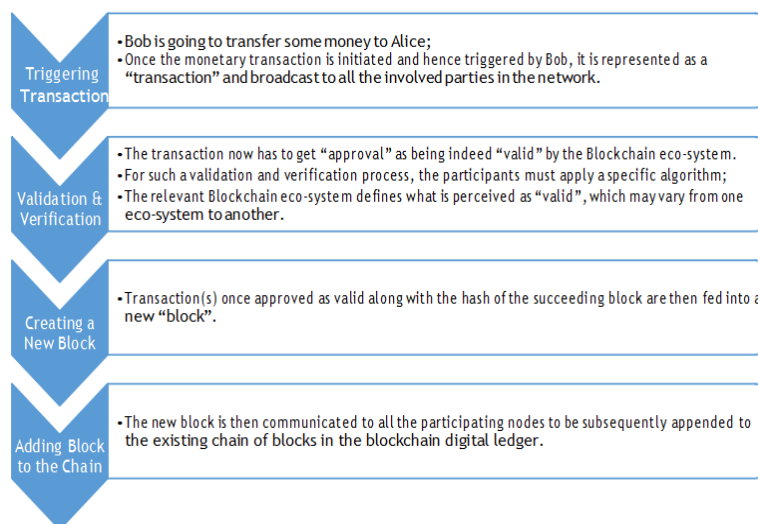


Figure 2. Operation of the Blockchain.

III. TECHNOLOGY FUNDAMENTALS OF BLOCKCHAIN

This site briefly defines the essentials of the technology in charge of the Blockchain. A Blockchain includes 2 numerous elements, as follow:

1. Bargain: A package, in a Blockchain, indicates the activity-activated because of the individual.
2. Block: A block, in a Blockchain, is really a collection of particulars tape-recording the acquisition and also various other connected applicable details consisting of the right collection, the timestamp of production, and so on
3. The Blockchain may simply either be really social or perhaps exclusive, trusting the set of its personal usage. A social Blockchain produces it practical for all individuals alongside review together with make up accreditations consisting of in Bitcoin, supply to it. Irrespective, there are in fact some social Blockchains that restrict the simplicity of accessibility to merely either to analyze or perhaps to make up..

IV. CONSIDERATION FOR BLOCKCHAIN SECURITY: CHALLENGES

Blockchain innovation has really been actually administered or even acknowledged as cybercash as well as likewise is actually definitely taken advantage of. Consider, nevertheless, that countless surveillance concerns happening in blockchain setup, purchase, wallet, along with program use have really been actually disclosed. This newspaper inspections the trends of surveillance issues raised today along with the safety level of the existing blockchain. Our company believe this initiative is actually remarkably crucial as the end results may work as bottom details for producing potential blockchain innovation as well as additionally enhancing surveillance.

Settlement of Blockchain

Although there have to simply be actually one blockchain taking into consideration that it is actually the successive web link of created blocks, a blockchain could be divided straight in to 2 considering that both very most existing blocks could be generated for a short while if 2 numerous peers prosper in removing the remedy for making the block at the identical opportunity. In such a circumstance, the block that is actually gone by as the present block due to the majority of peers in the bitcoin system to arise to mine is going to definitely wind up being actually worthless. Essentially, the bitcoin is going to surely follow many of the peers that possess fifty% and even extra exploration capability (operating ability). Therefore, if an opponent possesses 51% exploration capability, a "51% Strike", where the assailant possesses command of the blockchain in addition to he/she may include falsified bargains, could be a concern. Depending on to an analysis study, an assailant may know wrongful increase along with simply 25% operating ability through a hazardous exploration method rather than 51%. Due to the fact that today operating potential of the whole entire bitcoin system is actually presently higher getting notable operating capacity is

actually taken into account to become challenging. Regardless, exploration pool-- the companies of exploration peers-- have in fact been actually proactively removing to boost the possibility of exploration. Consequently, this hazard has in fact found yourself being actually a worry. Recently, GHash, a leading exploration pool, briefly exceeded the fifty% restriction, needing the bitcoin community to experience interior as well as likewise outdoors adjustments to manage the risk. Primarily, the chance of handling the blockchain is actually related to the common protection of the bitcoin along with such safety threats possess really briefly affected the economic components due to the attributes of the bitcoin, which is actually frequently properly concerning the market place fee.

Security of Transaction

Thinking about that the composition utilized in inputs in addition to outcomes is actually a systems foreign language along with versatility, a variety of purchase kinds may be established using such. A bitcoin arrangement [11] is actually a method of utilization bitcoin for the existing proof as well as additionally a financial option. A frequently used method includes cultivating the contract using the document that contains a multiple-signature method named multisig. Although the compositions are actually utilized to take care of a huge assortment of bitcoin concerns, the possibility of an improperly established purchase has in fact additionally increased as the complexity of the document increases. A bitcoin using a badly established safeguarding composition is actually dealt with considered that nobody can easily use it as the position document may certainly not be actually created. To this end, there are actually investigation studies that advise models of bitcoin contract-type offers to confirm the preciseness of a composition made use of in a purchase.

Security of Wallet

As the essential treatment to hacking assaults of a bitcoin handbag, offline, awesome storage-type budgets like a bodily bitcoin piece or even a newspaper bitcoin spending plan that is actually certainly not connected to the Internet, are actually provided. Similar methods contain the hardware-type bitcoin wallets to minimize the risk pertaining to on the net investments. The tools budget, like Trezor, outlets the key in a tamper-proof storing area unit connected to the pc unit using USB, that is actually, merely when taken advantage of in addition to the accredited deal is actually transferred to use the within always kept method and also merely when the consumer is actually confirmed. To place it merely, the storing area unit is actually connected simply when there is actually a need to build a bitcoin purchase, remaining in amazing storage-like standing up the rest of the amount of time. Although it is actually so much more risk-free as well as protected than

fridge given that there is actually an additional proof operation, problems including reduction of fridge in addition to the vacancy of user-friendliness in addition both the tools prize

The bitcoin deal with is actually the hash truly worth of a social crucial etched along with a collection of social along with specific techniques. Because of this, the safeguarding document of a bitcoin purchase along with a handle as the result may be opened up along with an unlocking composition that possesses in fact the worth licensed along with the public secret of the deal with as well as additionally the personal technique. The bitcoin prize stores information like the personal method of the deal with to become taken advantage of for the production of the position document. It suggests that reduction of details in the wallet creates a reduction of bitcoin looking at that the particulars are actually critical for using the bitcoin. Because of that, the bitcoin prize has really happened the significant subject of bitcoin spell through hacking. To assure the protection of the bitcoin prize, remedies have in fact provided multisig for numerous hallmarks. Looking at that multisig simply allows a purchase when there is actually higher than one hallmark, relying on the configuration, it could be taken advantage of as the repeated safety and security quality of the spending plan. As an instance, if multisig is actually installed in an on-line bitcoin finances in addition to is actually established to require the operator's hallmark in addition to the hallmark of the on the net handbag internet site whenever a purchase is actually performed coming from the handbag, harmful bitcoin drawback may be defended versus taking into consideration that the operator's private trick is actually certainly not always kept, likewise when the online budget site is actually taken command of through a hacking assault. On top of that, multisig is actually establishing straight in to options that allow drawback coming from the bitcoin spending plan only through biometric relevant information or even various gadgets using a two-factor confirmation as well as likewise a variety of other activities.

Security of Software

The insect of the software program treatment took advantage of in bitcoin could be critical. Although the principal Bitcoin Designer Documents web site simply makes clear all bitcoin treatments, the bitcoin primary software application is actually still efficient as the referral considering that the extensive treatments of the incredibly early bitcoin unit have in fact been actually determined by means of the software application performed through Satoshi Nakamoto.

Nonetheless, likewise the bitcoin primary software program request, which requires to become additional reliable than just about anything, is actually certainly not without the concern of software application failure like insect. Among one of the most popular software application pests is actually the CVE-2010-5139 sensitivity that took place in August 2010. As a result of the insect induced through integer spillover, prevent deal, where 0.5 bitcoin was actually offered as 184 mountain bitcoin, was actually included in a traditional block, as well as likewise the concern was actually certainly not resolved up till 8 h eventually. Moreover, there was actually a bug where a

block improved in variant 0.8 was actually certainly not honed in variant 0.7 as the information resource was actually improved coming from BerkeleyDB to LevelDB considered that the bitcoin variant of the bitcoin center was actually upgraded coming from 0.7 to 0.8. It produced the peers of variant 0.7 as well as additionally peers of variety 0.8 to possess a variety of blockchains for 6 h. Each of these concerns are actually occasions showing that the fundamental positive self-image in the surveillance of bitcoin offers of a block as possessing substantial depth after a quantity of your time along with could be imperiled through a software application insect [9].

V. BLOCKCHAIN: DATA INTEGRITY, PERFORMANCE, STABILITY

The blockchain is actually a fairly unique technology that has actually seemed on the marketplace in the latest years, to start with utilized as the social journal for the Bitcoin cryptocurrency[8]. It mostly includes successive chained blocks including reports, that are actually imitated on the nodules of a p2p system. These reports witness purchases took place in between nicknames. Purchases might include a cryptocurrency like, e.g., the Bitcoin, or even various another type of resources. The assortment of purchases, as well as their confining in establishment blocks, is actually executed in a decentralized style through recognized nodules of the system, i.e. miners. Miners use appropriate block building procedures, i.e., the exploration procedure, to accomplish opinion one of all the miners on recently produced blocks. Bitcoin is actually an instance of the permissionless blockchain, i.e., there is actually no stipulation for a nodule to end up being a miner. If rather there is actually an authorization and also certification level for miners, at that point the blockchain is actually permission.

The authentic exploration method, still utilized for Bitcoin and also Ethereum blockchain, is actually based upon the verification of job (PoW). It is composed in a computational demanding hashing job that is actually controlled depending on to the supposed blockchain problem that moderates the normal opportunity devoted through miners to achieve such a duty and also generate a brand new block. When a miner obtains the development of a brand-new block, it relays that block to all the various other miners. They look at such a block as the most up to the date of the establishment and also begin extracting brand new blocks to become tacked on. Because simpleness, our company may mention that when a miner has actually developed a brand-new block, it enters into the establishment (if numerous miners simultaneously include a block, a short-term fork is actually developed which is actually commonly swiftly settled given that deliberately miners consistently take into consideration the lengthiest establishment).

PoW-based blockchains take pleasure in several interesting homes associated with information stability, which observe coming from the exploration method as well



as coming from the total duplication of the blockchain on a lot of nodules. Certainly, when a block becomes part of the establishment, all miners have actually settled on its own materials, therefore it is actually almost non-repudiable as well as relentless (unless an aggressor possesses most of miners' hash electrical power that has the capacity to produce a fork of the establishment). Presuming a bulk of hash electrical power managed through sincere miners, the chance of a fork of intensity n is actually $(2 - n)$. This offers consumers higher assurance that just awaiting a handful of nodules to become incorporated (6 blocks in Bitcoin) will definitely guarantee their deals are actually entirely featured along with higher peace of mind.

Nonetheless, PoW-based blockchains possess a major setback: efficiency. This lack of functionality is in fact primarily because of the tv transmitting latency of blocks on the body in addition to the time-intensive task of PoW. As a matter of fact, each deal hung on a blockchain has a much higher verification latency, which makes an extremely decreased deal throughput. Another suitable stress concerning utilizing the blockchain involves its personal stability. Although, e.g., the Bitcoin's blockchain has in fact worked really efficiently up previously, there is really no commonly enabled scholastic project uncovering either why this has in fact developed, or perhaps whether it is going to certainly move on later, or maybe the span of your time it is actually going as well. The safety and security homes of the PoW-based point of view procedure are in fact still being in fact covered, as well as likewise existing "compositions carries out absolutely not likewise supply sufficient tools to analyze under which cost-effective as well as additionally social opinions Bitcoin by itself is actually visiting keep professional". Usually, PoW- situated blockchains using incentive devices located upon cryptocurrencies are in fact extremely based upon market varieties, which guides a night on the blockchain efficiency on the lasting.

VI. CONCLUSION

The blockchain has in fact a spread structure as well as additionally makes use of the peer network along with the computer system resources of peers. Technical actions such as proof of task along with proof of stack have really been related to increase the safety and security of blockchain. Although the protection of blockchain is regularly enhanced, concerns have in fact continued to be to be reported as well as additionally there are energised looks into on protection. An assaulter makes many initiatives to access a client's specific essential conserved in the consumer's computer system or wise tool in order to hack the bitcoin. There are looks into on using a secure token or waiting securely to protect the specific technique. In this research study, we assessed the blockchain modern technology in addition to linked core modern-day innovations as well as additionally examined the trend of looks into today to discuss even more places to be investigated.

REFERENCES

1. Beikverdi, A.; JooSeok, S. Pattern of concentration in Bitcoin's circulated system. In Procedures of the 2015 16th IEEE/ACIS International Meeting on Software Program

- Design, Expert System, Media and also Parallel/Distributed Computer (SNPD), Takamatsu, Asia, 1-- 3 June 2015.
2. Bonneau, J.; Miller, A.; Clark, J.; Narayanan, A.; Kroll, J.A.; Felten, E.W. Sok: Research study standpoints as well as problems for bitcoin and also cryptocurrencies. In Procedures of the 2015 IEEE Seminar on Protection and also Personal Privacy (SP), San Jose, CA, U.S.A., 17-- 21 Might 2015.
3. Christidis, K.; Michael, D. Blockchains and also Smart Buy the Web of Points. IEEE Gain access to 2016, 4, 2292-- 2303.
4. Huang, H.; Chen, X.; Wu, Q.; Huang, X.; Shen, J. Bitcoin-based reasonable settlements for contracting out estimations of smog tools. Potential Gener. Comput. Syst. 2016.
5. S.; Sangrae, C.; Soohyung, K. Dealing with IoT units making use of blockchain system. In Process of the 2017 19th International Seminar on Advanced Interaction Modern Technology (ICACT), Bongpyeong, Korea, 19-- 22 February 2017.
6. Armknecht, F.; Karame, G.; Mandal, A.; Youssef, F.; Zenner, E. Surge: Outline as well as Expectation. In Depend On and also Trustworthy Processing; Conti, M., Schunter, M., Askoxylakis, I., Eds.; Springer International Printing: Cham, Switzerland, 2015; pp. 163-- 180.
7. Vasek, M.; Moore, T. There is actually No Freebie, Also Utilizing Bitcoin: Tracking the Recognition as well as Revenues of Online Unit Of Currency Shams. In Procedures of the International Meeting on Financial Cryptography as well as Information Safety And Security, San Juan, Puerto Rico, 26-- 30 January 2015; Springer: Berlin/Heidelberg, Gemany, 2015.
8. Bojan Suzic, Bernd Prunster, Dominik Ziegler, Alexander Marsalek, and also Andreas Reiter. Balancing Power and also Safety and security: Getting Cloud Federations of People Entities. In C&TC, edition 10033 of LNCS, web pages 943-- 961. Springer, 2016.
9. Mor Weiss, Boris Rozenberg, and also Muhammad Barham. Practical Solutions For Format-Preserving File Encryption. CoRR, abs/1506.04113, 2015.
10. Gavin Hardwood. Ethereum: A safe and secure decentralised generalised deal journal. Ethereum Task Yellowish Newspaper, 2014.
11. Xueping Liang et cetera, "ProvChain: A Blockchain-based Information Derivation Design in Cloud Setting along with Boosted Personal Privacy as well as Supply," in Procedures of the 17th IEEE/ACM International Seminar on Set, Cloud as well as Framework Computer (CCGrid '17), Madrid, Spain, Might 14 - 17, 2017, pp. 468-477, Available:
12. Mahdi H. Miraz, Maaruf Ali, Peter Excell, and also Choosing Rich, "An Assessment on Web of Points (IoT), World Wide Web of Whatever (IoE) and also Net of Nano Points (IoNT)," in the Process of the Fifth International IEEE Seminar on World Wide Web Technologies and also Apps (ITA 15), Wrexham, UK, 2015, pp. 219-- 224, Available: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7317398>
13. Mahdi H. Miraz, Maaruf Ali, Peter S. Excell, and also Richard Selecting, "Web of Nano-things, Factors and also Every Thing: Future Development Trends," (to become released) Future World wide web, 2018.
14. Mahdi H. Miraz as well as Maaruf Ali, "Blockchain Enabled Enriched IoT Environment Safety And Security," (allowed) in procedures of the First International Meeting on Arising Technologies in Processing 2018 (iCETiC '18), Greater London, UK, 23 August 2018.
15. Sarah Undergrowth, "Blockchain Beyond Bitcoin," Communications of the ACM, vol. 59, no. 11, pp. 15-17, Nov 2016, Available: <https://doi.org/10.1145/2994581>