ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 8, August 2019

Blockchain Technologies for the Internet of Everything: Research Concerns and Problems

Shubham Kumar

Assistant Professor, Galgotias University, Greater Noida, U.P, India

ABSTRACT: This paper introduces an extensive review of the current blockchain conventions for the Internet of Things (IoT) systems. We start by portraying the blockchains and condensing the current studies that manage blockchain innovations. At that point, we give a diagram of the application areas of blockchain innovations in IoT, e.g, Internet of Vehicles, Internet of Energy, Internet of Cloud, Fog registering, and so on. Besides, we give a grouping of danger models, which are considered by blockchain conventions in IoT systems, into five principle classifications, to be specific, personality based assaults, control based assaults, cryptanalytic assaults, notoriety based assaults, and administration based assaults. What's more, we give a scientific categorization and a one next to the other correlation of the best in class techniques towards secure and protection saving blockchain advancements concerning the blockchain model, explicit security objectives, execution, restrictions, calculation multifaceted nature, and commu-nication overhead. In view of the ebb and flow overview, we feature open research difficulties and talk about conceivable future research bearings in the blockchain advances for IoT.

KEYWORDS: Blockchain, Consensus, Security, Threats, IoT

I. INTRODUCTION

Over the most recent couple of years, we have seen the capability of Internet of Things to convey energizing administrations over a few parts, from online networking, business, shrewd transportation and savvy urban areas to the enterprises [1], [2], [3]. IoT consistently interconnects heterogeneous gadgets with assorted utilitarian ities in the human-driven and machine-driven systems to meet the advancing prerequisites of the prior referenced sec-tors. By and by, the huge number of associated gadgets and gigantic information traffic become the bottleneck in gathering the required Quality-of-Services (QoS) due to the computa-tional, stockpiling, and data transfer capacity obliged IoT gadgets. Most as of late, the blockchain [4], [5], [6], [7], a change in outlook, is changing all the significant application territories of IoT by empowering a decentralized domain with mysterious and trustful exchanges. Joined with the blockchain innovation, IoT frameworks profit by the lower operational cost, decentralized asset the board, power against dangers and assaults, etc. Along these lines, the intermingling of IoT and blockchain innovation expects to beat the critical difficulties of understanding the IoT stage sooner rather than later.

DOI: 10.15680/IJIRCCE.2019. 0708013

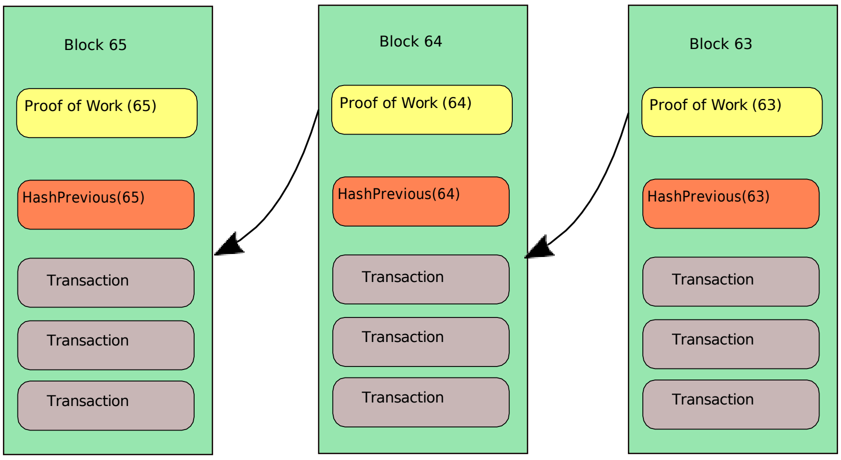


Fig. 1. Blockchain structure.

Blockchain, a circulated affix just open record tech-nology, was at first expected for the digital currencies, e.g., Bitcoin1. In 2008, Satoshi Nakamato [8] presented the con-cept of blockchain that has pulled in much consideration over the previous years as a rising shared (P2P) innovation for appropriated figuring and decentralized information sharing. Because of the selection of cryptography innovation and without a brought together control on-screen character or an incorporated information stockpiling, the blockchain can keep away from the assaults that need to assume responsibility for the framework. Afterward, in 2013, Ethereum, an exchange based state-machine, was displayed to program the blockchain tech-nologies. Curiously, because of its remarkable and appealing highlights, for example, value-based protection, security, the unchanging nature of information, auditability, trustworthiness, approval, framework straightforwardness, and adaptation to non-critical failure, blockchain is being connected in a few segments past the cryptographic forms of money. A portion of the territories are character the executives [9], insightful transportation [10], [11], [12], [13], [14], [15], production network the executives, portable group detecting [16], horticulture [17], Industry 4.0 [18], [19], Internet of Everything [20], [21], [18], [22], and security in mission basic frameworks [23].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 8, August 2019

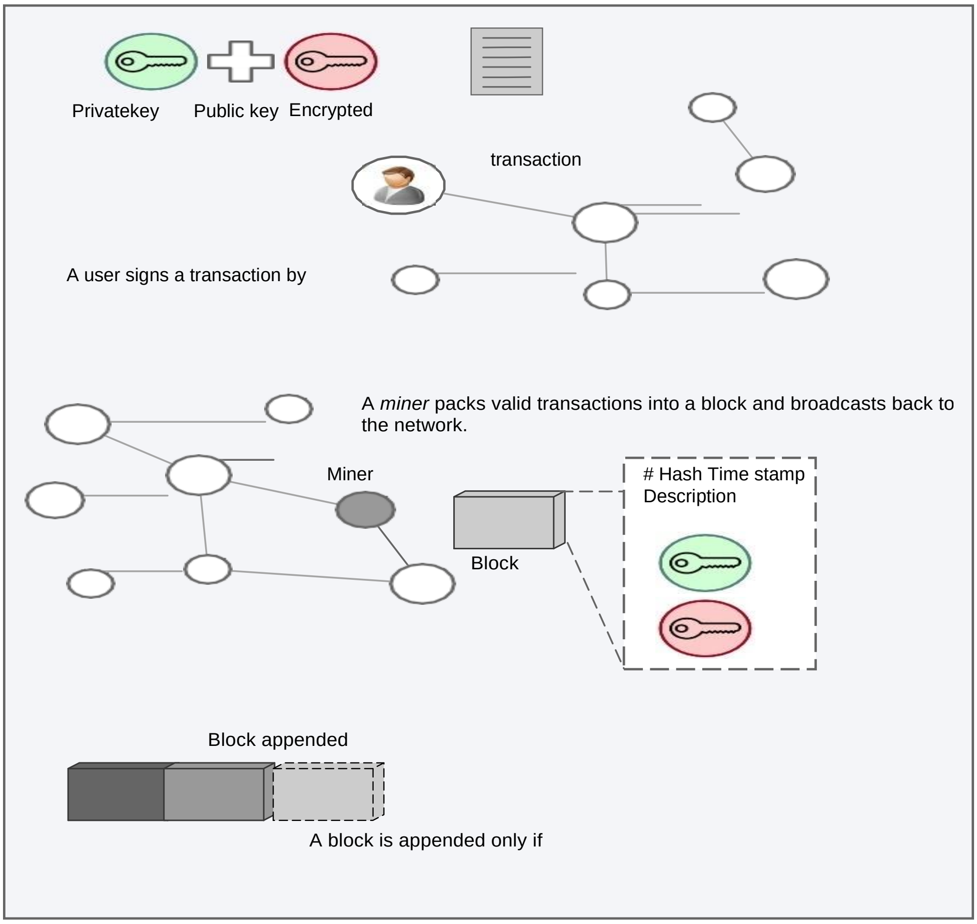

Privatekey
Public key
Encrypted
transaction
A user signs a transaction by
A *miner* packs valid transactions into a block and broadcasts back to the network.
Miner
Block
# Hash Time stamp
Description
Block appended
A block is appended only if

Fig. 2. An illustration of blockchain working methodology.

As appeared in Fig. 1, the blockchain structure is made out of a succession of squares, which are connected together by their hash esteems. In the blockchain arrange, an open record keeps up the carefully marked exchanges of the clients in a P2P organize. When all is said in done, a client has two keys: an open key for different clients for the encryption and a private key to peruse an encoded message, as appeared in Fig. 2. From the blockchain point of view, the private key is utilized for marking the blockchain exchange and the open key speaks to the remarkable location. Topsy-turvy cryptography is utilized to decode the message encoded by the comparing open key. At the underlying stage, a client signs an exchange utilizing its private key and communicates it to its friends. When the companions get the marked exchange, they approve the exchange and scatter it over the system. Every one of the gatherings who are engaged with the exchanges commonly approve the exchange to meet an accord understanding. When a dispersed agreement is come to, the uncommon hub, called as excavators, incorporates the legitimate exchange into a timestamped square. The square, which is incorporated by the excavator, is communicated again into the system. Subsequent to approving the communicate square, which contains the exchange, just as hash-coordinating it with the past square in the blockchain, the communicate square is affixed to the blockchain.

In view of the information the board and the kind of uses, blockchain can grouped either as private (authorization) or bar lic (permissionless). The two classes are decentralized and give a specific degree of insusceptibility against flawed or noxious clients for the record. The fundamental contrasts among private and open blockchains lie in the execution of the accord convention, the support of the record, and the approval to join to the P2P organize. Nitty gritty instances of these classes are outlined in [24]. With regards to IoT, blockchains can be arranged dependent on approval and validation. As appeared in Fig. 3, in a private blockchain, the unified confided in power that deals with the confirmation and approval procedure chooses the diggers. Then again, in an open blockchain (by and large, permissionless), there is no intercession of any outsider for the excavator determination and joining for another client to the blockchain organize.

As of late, there is an enormous measure of speculation from the ventures [25], [26] just as a noteworthy enthusiasm from the scholarly community to illuminate real research difficulties in blockchain advances. For instance, the agreement conventions are the real building squares of the blockchain innovations, in this manner, the dangers focusing on the accord conventions become a huge research issue in the blockchain. Moreover, blockchain forks carry dangers to the blockchain agreement conventions. Additionally, it is seen that the helplessness is about 51% for another blockchain [27]. Simultaneously, support of a few blockchains requires a lot of intensity utilization [28].

II. RELATED SURVEYS AND OUR CONTRIBUTIONS

There are connected overview papers [7], [29], [30], [31], [24], [32]that secured various parts of the blockchain technology. For instance, a short outline of blockchain for bitcoin was talked about in [29], [30]. Be that as it may, these overviews are restricted with respect to point by point dialog on research difficulties in blockchain. In addition, Sankar et al. [29] quickly exhibited the attainability of different agreement conventions in the blockchain. The point by point experiences of bitcon were exhibited in [7]. As of late, the reviews [24] exhibited the diagram of Blockchain-based IoT (BIoT) applications. The security and protection angles are exhibited in [32], [31] for bitcoin, one of the blockchain applications. Table I outlines the fundamental concentrations and significant commitments of the past com-prehensive reviews on blockchain advances. Despite the fact that the previously mentioned studies [7], [31], [24], [32] have established a strong framework for blockchain advances, our review contrasts in a few perspectives. The fundamental commitments of this paper are:

- We give reviews of the distinctive application do-mains of blockchain advances in IoT, e.g, Internet of Vehicles, Internet of Energy, Internet of Cloud, Fog figuring, and so forth.
- We order the risk models, which are considered by the blockchain conventions in IoT systems, into five fundamental classifications, in particular, personality based assaults, control based assaults, cryptanalytic assaults, notoriety based attacks, and administration based assaults.
- We survey existing examination on obscurity and protection in Bitcoin frameworks.

DOI: 10.15680/IJIRCCE.2019. 0708013

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

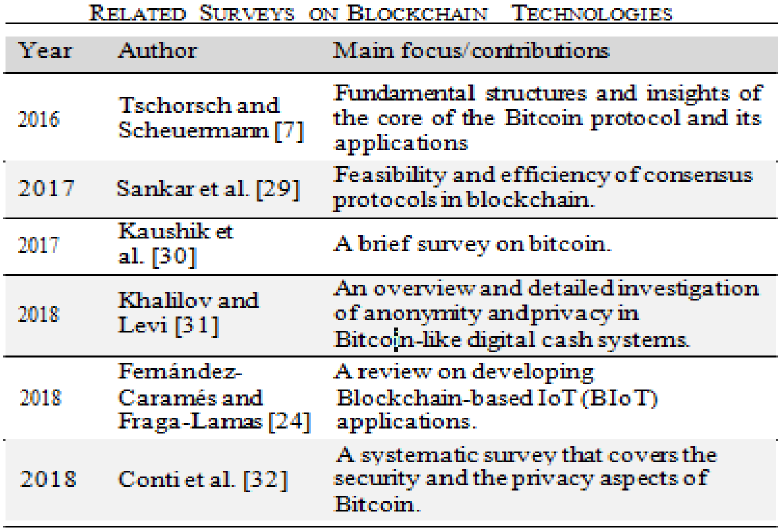
International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 8, August 2019

TABLE I
RELATED SURVEYS ON BLOCKCHAIN TECHNOLOGIES



Year	Author	Main focus/contributions
2016	Tschorsch and Scheuermann [7]	Fundamental structures and insights of the core of the Bitcoin protocol and its applications
2017	Sankar et al. [29]	Feasibility and efficiency of consensus protocols in blockchain.
2017	Kaushik et al. [30]	A brief survey on bitcoin.
2018	Khalilov and Levi [31]	An overview and detailed investigation of anonymity and privacy in Bitcoin-like digital cash systems.
2018	Fernández-Caramés and Fraga-Lamas [24]	A review on developing Blockchain-based IoT (BIoT) applications.
2018	Conti et al. [32]	A systematic survey that covers the security and the privacy aspects of Bitcoin.

- We give a scientific categorization and a one next to the other correlation, in an unthinkable structure, of the cutting edge on the re-penny progressions towards secure and protection safeguarding blockchain advances as for blockchain model, explicit security objectives, execution and limita-tions, calculation unpredictability and correspondence over-head.
- We feature the open research difficulties and talk about the conceivable future research bearings in the field of blockchain innovations for IoT.

The rest of this paper is composed as pursues. Area II shows the application areas of blockchain technolo-gies in IoT. In Section III, we present the grouping of danger models that are considered by the blockchain conventions in IoT systems. In Section IV, we present a next to each other correlation, in a forbidden structure, of the best in class on the ongoing headways towards secure and protection safeguarding blockchain advancements. At that point, we talk about open issues and suggestions for further look into in Section V. At last, we reach our determinations in Section VI.

III. BLOCKCHAIN APPLICATIONS FOR THEIOT

As presented in Fig. 4, the blockchain technology can be effectively applied in almost all domains of IoT.

Internet of healthcarethings

The use of IoT in human services has permitted to sustain the ehealthcare frameworks with clinical information identified with the patients, their family, their companions, just as the social insurance suppliers. The information, called electronic therapeutic records (ETRs), is put away by the mindful medicinal services supplier. To encourage understanding information transportability, there are the electronic health records (EHRs), which have a more extravagant information structure than ETRs. In light of conveyed online database, Esposito et al. [33] proposed the plan of a blockchain-based plan for the IoT in human services. In a model of consortium blockchain, another *square* is instantiated and circulated when new human services information is made. To safeguard the security of patients and keep up the unchanging nature of EHRs, Guo et al. [34] presented a property based mark plot, named MA-ABS, which uses various specialists. The MA-ABS plan utilizes the blockchain tech-nology and can oppose to N-1 ruined specialists intrigue assaults. What's more, the MA-ABS is unforgeable in enduring a specific predicate assault. In this manner, Liang et al. [35] utilized the blockchain organize in portable human services applications for trustworthiness security, further examining or examination.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 8, August 2019

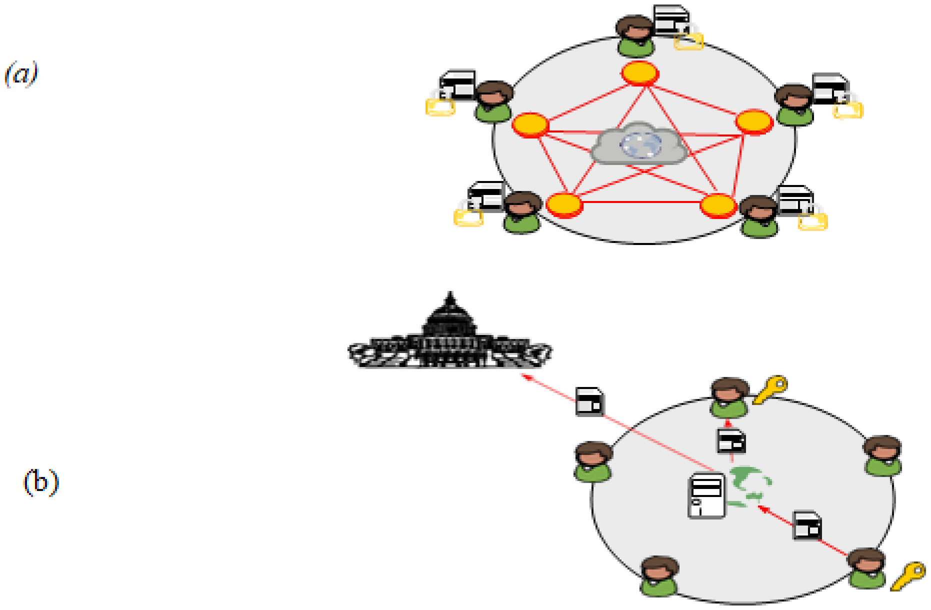


Fig. 3. (a) Public blockchain system; (b) Private blockchain system.

Internet of things in the 5Gera

In the IoT period, 5G will empower a completely portable and associated society for billions of associated objects [44]. To fathom the protection issues in the 5G heterogeneous correspondence envi-ronment, Fan et al. [45] proposed a blockchain-based security saving and information sharing plan. In light of adding squares to the blockchain, each new square is associated with the blockchain by its hash esteem. Note that the past hash worth can be known from the square header.

Internet of vehicles

The Internet of Vehicles (IoV) is a rising idea, which permits the combination of vehicles into the new period of the IoT so as to build up the keen correspondence be-tween vehicles and heterogeneous systems, for example, vehicle-to-vehicle, vehicle-to-street, vehicle-to-human, vehicle-to-sensor, and vehicle-to-everything. Notwithstanding, some ongoing works attempt to apply the blockchain innovation to IoV. In view of the decentralized security model, Huang et al. [10] proposed a blockchain environment model, named LNSC, for electric vehicle and charging heap the board. The LNSC model uses elliptic bend cryptography (ECC) to figure hash capacities electric vehicles and charging heaps. To maintain a strategic distance from the area following in the IoV, Dorri et al. [11] proposed a decentralized security safeguarding engineering, where overlay hubs deal with the blockchain. Likewise, the hash of the reinforcement stockpiling is put away in the blockchain.

Without the organization from the focal administrator, Lei et al. [12] proposed a blockchain-based powerful key man-agement for vehicular correspondence frameworks. In view of a decentralized blockchain structure, the outsider specialists are evacuated and the key exchange procedures are confirmed and verified by the security administrator arrange. In addition, Kang et al. [13] presented a P2P power exchanging framework, named PETCON, to outline point by point activities of restricted P2P power exchanging. Utilizing consortium blockchain technique, the PETCON framework can freely review and share exchange records without depending on a confided in outsider. To understand the issues of sending dependable declarations without re-vealing clients' personalities, Li et al. [14] proposed a protection safeguarding plan, named CreditCoin, for sending report ments secretly in the IoV. The CreditCoin plan utilizes the blockchain by means of a mysterious vehicular declaration collection convention to construct trust in the IoV interchanges. For information believability appraisal in the IoV, Yang et al. [15] proposed a blockchain-based notoriety framework, which can pass judgment on the got messages as either obvious or false dependent on the senders' notoriety esteems.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 8, August 2019

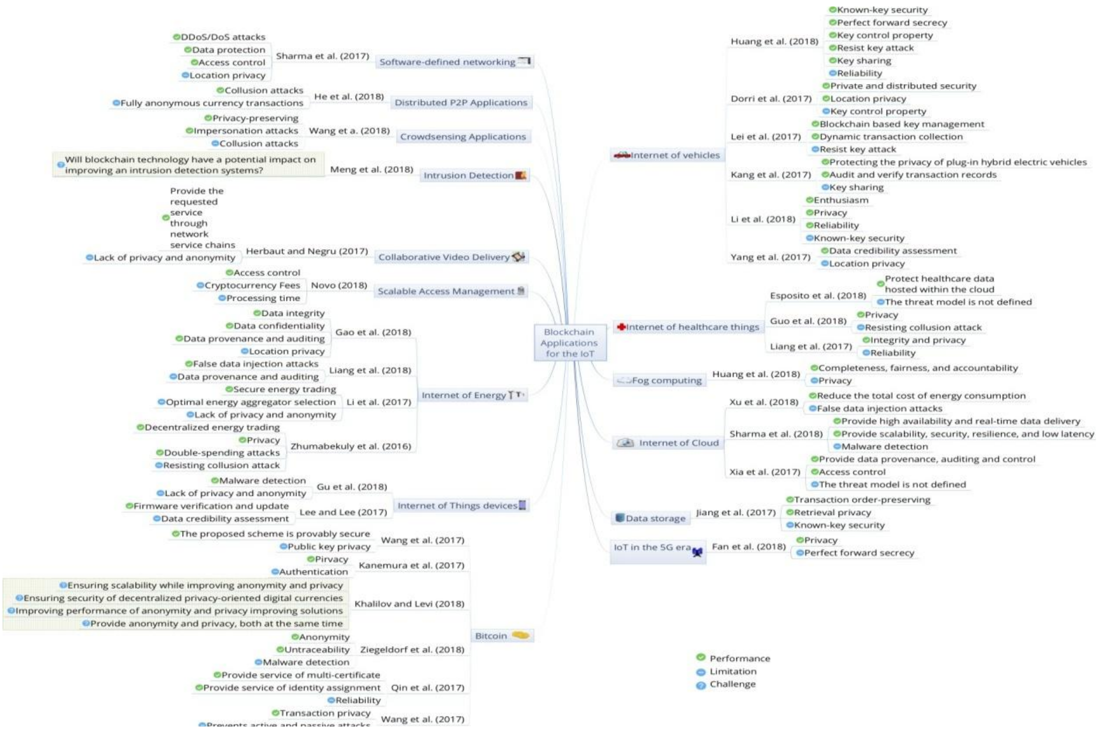

Blockchain Applications for the IoT
Software-defined networking
Sharma et al. (2017)
DDoS/DoS attacks
Data protection
Access control
Location privacy
Distributed P2P Applications
He et al. (2018)
Collusion attacks
Fully anonymous currency transactions
Crowdsensing Applications
Wang et a. (2018)
Privacy-preserving
Impersonation attacks
Collusion attacks
Intrusion Detection
Meng et al. (2018)
Will blockchain technology have a potential impact on improving an intrusion detection systems?
Collaborative Video Delivery
Herbaut and Negru (2017)
Provide the requested service through network service chains
Lack of privacy and anonymity
Scalable Access Management
Novo (2018)
Access control
Cryptocurrency Fees
Processing time
Internet of Energy
Gao et al. (2018)
Data integrity
Data confidentiality
Data provenance and auditing
Location privacy
Liang et al. (2018)
False data injection attacks
Data provenance and auditing
Li et al. (2017)
Secure energy trading
Optimal energy aggregator selection
Lack of privacy and anonymity
Zhumabekuly et al. (2016)
Decentralized energy trading
Privacy
Double-spending attacks
Resisting collusion attack
Internet of Things devices
Gu et al. (2018)
Malware detection
Lack of privacy and anonymity
Lee and Lee (2017)
Firmware verification and update
Data credibility assessment
Bitcoin
Wang et al. (2017)
The proposed scheme is provably secure
Public key privacy
Kanemura et al. (2017)
Pirvacy
Authentication
Khalilov and Levi (2018)
Ensuring scalability while improving anonymity and privacy
Ensuring security of decentralized privacy-oriented digital currencies
Improving performance of anonymity and privacy improving solutions
Provide anonymity and privacy, both at the same time
Ziegeldorf et al. (2018)
Anonymity
Untraceability
Malware detection
Qin et al. (2017)
Provide service of multi-certificate
Provide service of identity assignment
Reliability
Wang et al. (2017)
Transaction privacy
Prevents active and passive attacks
Internet of vehicles
Huang et al. (2018)
Known-key security
Perfect forward secrecy
Key control property
Resist key attack
Key sharing
Reliability
Dorri et al. (2017)
Private and distributed security
Location privacy
Key control property
Lei et al. (2017)
Blockchain based key management
Dynamic transaction collection
Resist key attack
Kang et al. (2017)
Protecting the privacy of plug-in hybrid electric vehicles
Audit and verify transaction records
Key sharing
Li et al. (2018)
Enthusiasm
Privacy
Reliability
Known-key security
Yang et al. (2017)
Data credibility assessment
Location privacy
Internet of healthcare things
Esposito et al. (2018)
Protect healthcare data hosted within the cloud
The threat model is not defined
Guo et al. (2018)
Privacy
Resisting collusion attack
Liang et al. (2017)
Integrity and privacy
Reliability
Fog computing
Huang et al. (2018)
Completeness, fairness, and accountability
Privacy
Internet of Cloud
Xu et al. (2018)
Reduce the total cost of energy consumption
False data injection attacks
Sharma et al. (2018)
Provide high availability and real-time data delivery
Provide scalability, security, resilience, and low latency
Malware detection
Xia et al. (2017)
Provide data provenance, auditing and control
Access control
The threat model is not defined
Data storage
Jiang et al. (2017)
Transaction order-preserving
Retrieval privacy
Known-key security
IoT in the 5G era
Fan et al. (2018)
Privacy
Perfect forward secrecy
Performance
Limitation
Challenge

Fig. 4. Blockchain applications for the IoT.

Internet of Energy

The Internet of Everything (IoE) gives an imaginative idea to expand the perceivability of Everything utilization in the Smart Grid. In light of the sovereign blockchain innovation, Gao et al. [20] presented a checking framework on Smart Grid, named GridMonitoring, for guaranteeing straightforwardness, provenance, and unchanging nature. The GridMonitoring framework depends on four layers, in particular, 1) Registration and confirmation layer, 2) Smart meter, 3) Processing and accord hubs, and 4) Data preparing on the brilliant matrix organize. In present day control frameworks, Liang et al. [21] proposed an information security structure dependent on disseminated blockchain, which can oppose against information control that are propelled by digital assailants (e.g., false information infusion assaults). To ensure information exactness, Liang's system utilizes the agreement component, which is naturally executed by each hub and has the rep-resentative qualities, in particular, 1) Setting of open/private key update recurrence, 2) Block age, 3) Miner determination, and 4) Release of meter's memory occasionally. For secure Everything exchanging Industrial Internet of Things (IIoT), Li et al. [18] presented the Everything blockchain, which depends on the consortium blockchain innovation and the Stackelberg game. Aitzhan and Svetinovic [22] executed a token-based pri-vate decentralized Everything exchanging framework for in decentralized savvy lattice Everything, which can be connected to the IoE.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

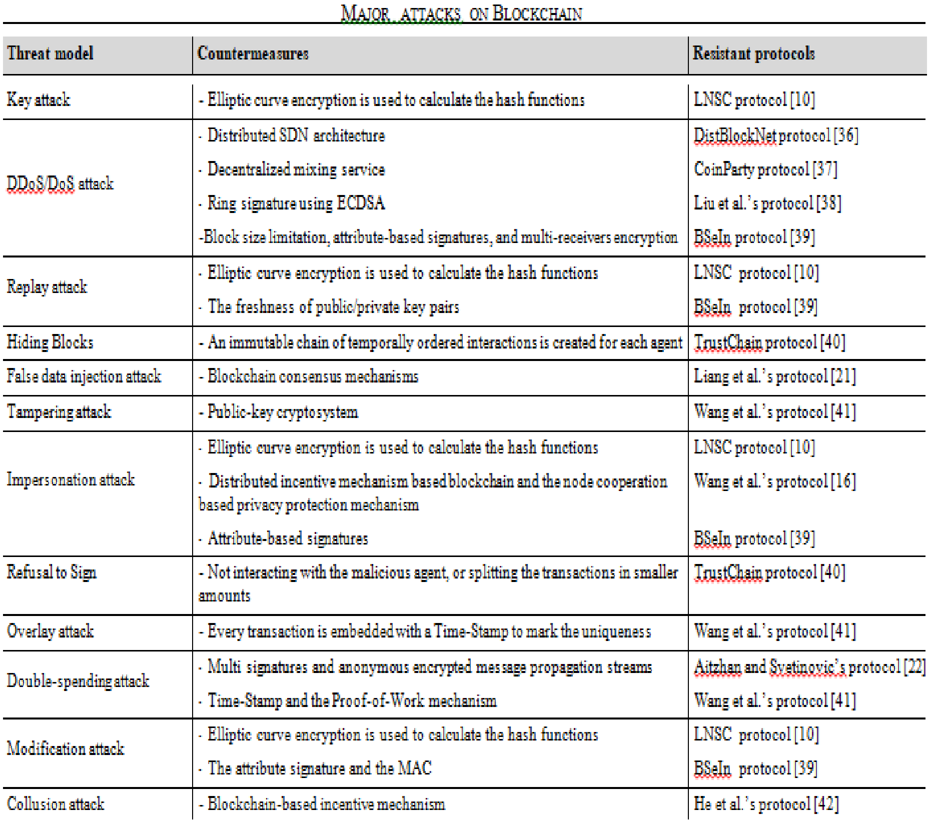
International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 8, August 2019

TABLE II
MAJOR ATTACKS ON BLOCKCHAIN



Threat model	Countermeasures	Resistant protocols
Key attack	- Elliptic curve encryption is used to calculate the hash functions	LNSC protocol [10]
DDoS/DoS attack	- Distributed SDN architecture - Decentralized mixing service - Ring signature using ECDSA -Block size limitation, attribute-based signatures, and multi-receivers encryption	DistBlockNet protocol [36] CoinParty protocol [37] Liu et al.'s protocol [38] BSeIn protocol [39]
Replay attack	- Elliptic curve encryption is used to calculate the hash functions - The freshness of public/private key pairs	LNSC protocol [10] BSeIn protocol [39]
Hiding Blocks	- An immutable chain of temporally ordered interactions is created for each agent	TrustChain protocol [40]
False data injection attack	- Blockchain consensus mechanisms	Liang et al.'s protocol [21]
Tampering attack	- Public-key cryptosystem	Wang et al.'s protocol [41]
Impersonation attack	- Elliptic curve encryption is used to calculate the hash functions - Distributed incentive mechanism based blockchain and the node cooperation based privacy protection mechanism - Attribute-based signatures	LNSC protocol [10] Wang et al.'s protocol [16] BSeIn protocol [39]
Refusal to Sign	- Not interacting with the malicious agent, or splitting the transactions in smaller amounts	TrustChain protocol [40]
Overlay attack	- Every transaction is embedded with a Time-Stamp to mark the uniqueness	Wang et al.'s protocol [41]
Double-spending attack	- Multi signatures and anonymous encrypted message propagation streams - Time-Stamp and the Proof-of-Work mechanism	Aitzhan and Svetinovic's protocol [22] Wang et al.'s protocol [41]
Modification attack	- Elliptic curve encryption is used to calculate the hash functions - The attribute signature and the MAC	LNSC protocol [10] BSeIn protocol [39]
Collusion attack	- Blockchain-based incentive mechanism	He et al.'s protocol [42]

Internet of Things devices

In the Internet of Things gadgets, aggressors try to exfiltrate the information of IoT gadgets by utilizing the pernicious codes in malware, particularly on the open source Android stage. By using measurable investigation technique, Gu et al. [46] introduction duced a malware recognition framework dependent on the consortium Blockchain, named CB-MDEE, which is made out of de-tecting consortium chain by test individuals and open chain by clients. The CB-MDEE framework embraces a fluffy correlation strategy and different checking capacities In request to lessen the false-positive rate and improve the discovery capacity of malware variations. To secure the installed gadgets in the IoT, Lee et al. [47] a firmware update plan dependent on the blockchain innovation, which the inserted gadgets have the two diverse activity cases, specifically, 1) reaction from a check hub to a solicitation hub, and 2) reaction from a reaction hub to a solicitation hub.

Access Management inIoT

For overseeing IoT gadgets, Novo [48] proposed a dispersed access control framework utilizing the blockchain innovation. The design of this framework is made out of six parts, specifically, 1) Wireless sensor systems, 2) Managers, 3) Agent hub, 4) Smart contract, 5) Blockchain system, and 6) Management center points. This framework brings a few points of interest for the entrance control in IoT, for example, 1) portability, which can be utilized in disengaged managerial frameworks; 2) openness, which guarantees that the entrance control principles are accessible whenever; 3) simultaneousness, which permits that the entrance control arrangements can be altered at the same time;

DOI: 10.15680/IJIRCCE.2019. 0708013

4) lightweight, which implies that the IoT gadgets needn't bother with any change to embrace this framework; 5) versatility, as the IoT gadgets can be associated through various compelled systems; 6) straightforwardness, where the framework can safeguard the area security.

Collaborative video delivery

The dissemination of astounding substance in the IoT these days challenges for the web access suppliers. Be that as it may, Herbaut and Negru [49] proposed a decentralized handling instrument for shared blockchain-based video conveyance, which is depending on cutting edge system administrations chains. In particular, this administration instrument is made out of three blockchains, specifically, 1) the substance expediting blockchain, 2) the conveyance observing blockchain, and 3) the provisioning blockchain. What's more, this administration component is conveyed with the open source venture Hyperledger-Fabric 2 where the outcomes demonstrate that the quantity of hubs marginally expands the conver-gence time .

Internet of Cloud

In the Internet of Cloud (IoC), billions of IoT gadgets transfer their information to the cloud through the web association using virtualization innovation. Xu et al. [50] presented a savvy asset the executives for cloud datacenters dependent on the blockchain innovation, so as to spare and lessen the absolute expense of Everything utilization. In particular, the clients utilize their individual private keys to sign an exchange, while the neighboring clients check the communicate exchange. The square is disposed of when it doesn't pass check. In this way, Sharma et al. [51] proposed an appropriated cloud architec-ture that utilizations three developing advancements, to be specific, programming characterized organizing (SDN), mist figuring, and a blockchain strategy. The SDN controllers of the mist hub are utilized to give programming interfaces to arrange the board operation erators. The blockchain procedure is utilized to give versatile, dependable, and high-accessibility administrations. Likewise, Xia et al. [52] proposed a blockchain-based information sharing framework, named MeDShare, for cloud specialist co-ops. This framework utilizes four layers specifically, 1) User layer, 2) Data inquiry layer, 3) Data organizing and provenance layer, and 4) Existing database foundation layer.

Intrusion Detection

Numerous methods for executing interruption recognition sys-tems (IDSs) in the IoT condition have been proposed, which are situated in AI. To improve the collective interruption location frameworks (CIDSs), Alexopoulos et al. [53] presented using blockchain innovation so as to verify the trading of cautions between the collab-speaking hubs. Meng et al. [54] talked about the relevance of blockchain innovation in an interruption discovery frameworks. Present day interruption discovery frameworks must be founded on collabo-rative correspondence among conveyed IDSs [55], requesting broad information sharing among substances and trust calculation. So as to manage the security worries that are raised by the information trade and to stifle insider assaults, the blockchain innovation is connected. Along these lines, the utilization of confided in outsider, which is additionally a solitary purpose of disappointment, that is required in conventional community oriented IDSs can be maintained a strategic distance from.

Software-defined networking

To build IoT's transfer speed, specialists have been propos-ing the Software Defined Networking (SDN) innovation, which gives insightful steering and improves basic leadership forms by the SDN controller [56]. As of late, Sharma et al. [36] proposed a circulated IoT organize archi-tecture, named DistBlockNet. In light of the blockchain tech-nology, DistBlockNet design can give adaptability and adaptability, without the requirement for a focal controller. The dis-tributed blockchain system utilizes two kind of hubs, specifically, 1) the controller/confirmation hub, which keeps up the refreshed stream principles table data and 2) the solicitation/reaction hub, which updates its stream guidelines table in a blockchain arrange.

Fog computing

Haze figuring, additionally called edge processing, is a profoundly virtualized stage that empowers registering and capacity be-tween end-clients and the server farm of the customary distributed computing [5]. Without the outsiders, Fog gadgets can com-municate with one another. Be that as it may, the blockchain strategy can be utilized to encourage interchanges between haze hubs and IoT gadgets. Huang et al. [57] proposed a reasonable installment conspire for re-appropriating calculations of Fog gadgets. In light of the bitcoin, this plan thinks about the accompanying security properties, specifically, fulfillment, decency, and responsibility

Distributed P2PApplications

In conveyed shared (P2P) applications for the IoT, the IoT gadgets self-sort out and participate for another type of utilizations, for example, community films, sending records, conveying messages, electronic trade, and transferring information utilizing sensor systems. To boost clients for collaboration, He et al. [42] proposed an honest motivator system dependent on the blockchain method for dynamic and conveyed P2P conditions. To avert narrow minded clients and guard against the agreement assaults, this plan proposed a valuing methodology, which enables moderate hubs to acquire rewards from blockchain exchanges because of their commitment to a triumph ful conveyance.

Crowdsensing Applications

The rising versatile crowdsensing worldview is a novel class of portable IoT applications (e.g., geological detecting applications). Wang et al. [16] is a fascinating motivating force mech-anism for protection safeguarding in crowdsensing applications dependent on the blockchain digital forms of money. In particular, this system can dispense with the security and protection issues utilizing the diggers' obvious information quality assessment to manage the pantomime assaults in the open and straightforward blockchain.

What's more, to accomplish k-namelessness security assurance, the instrument utilizes a hub collaboration technique for taking part clients.

Datastorage

The information stockpiling can manage heterogeneous information assets for IoT-based information stockpiling frameworks. The most effective method to share and secure these touchy information are the fundamental difficulties in IoT information stockpiling. In view of the blockchain innovation, Jiang et al. [58] proposed a private catchphrase search, named Searchain, for decentralized capacity. The Searchain design incorporates two segment, in particular, 1) exchange hubs in a shared structure and 2) a blockchain of all the arranged squares. Moreover, the Searchain design can give client protection, vagary, and responsibility.

Bitcoin

Propelled in 2009, Bitcoin is the distributed (P2P) pay-ment organize that needn't bother with any focal experts. In light of the center procedure of blockchain, Bitcoin clients don't utilize genuine names; rather, pen names utilized. Accordingly, Bitcoin depends on three fundamental specialized parts: exchanges, agreement Protocol, and correspondence arrange.

The current research on namelessness and security for Bitcoin framework are exhibited in Tab. III. Khalilov and Levi [72] have distributed an intriguing examination on secrecy and security in Bitcoin-like advanced money frameworks. In particular, the investigation ordered the techniques for examining secrecy and protection in Bitcoin into four classes, specifically, 1) Transacting, 2) Utilizing off-arrange data, 3) Utilizing system, and 4) Analyzing blockchain information.

As examined by Wang et al. [71], Bitcoin works practically speaking, yet not in theory,and the principle issue is the way to ensure the potential purchasers' security in Bitcoin utilizing the open key infras-tructure. Wang et al. [71] examined the assigned verifier evidence of advantages for bitcoin trade utilizing elliptic bend cryptogra-phy. In particular, the creators proposed a protection safeguarding plan, named DV-PoA, which can fulfill unforgeability. Note that the DV-PoA plan utilizes elliptic bend discrete log-arithm issue, elliptic bend computational Diffie-Hellman issue, and impact obstruction of cryptographic hash func-tion. Also, to secure the protection of disentangled installment check (SPV) customers, Kanemura et al. [70] proposed a security protecting Bloom channel structure for a SPV customer dependent on γ Deniability.

By evacuating the confided in outsider, Qin et al. [73] proposed a distributively blockchain-based PKI for Bitcoin framework, named Cecoin. To guarantee the consistency, Cecoin utilizes a motivating force component and an appropriated accord convention. To give multi-declaration administrations and personality task, Cecoin changes over a triple (address, area, cert) to a tuple (key, address, cert), and key speaks to way of cert in the tree. Along these lines, to secure the exchange protection in Bitcoin, Wang et al. [41] proposed a structure by including the homomorphic Paillier encryption framework to cover the plaintext sums in exchanges. To take care of the trust issue in Bitcoin, Huang et al. [57]proposed a dedication based testing plan of ringer, which can be utilized for conventional calculations in the redistributing registering.

IV. THREAT MODELS FORBLOCKCHAIN

In this segment, we present and portray the danger models that are considered by the blockchain conventions in IoT net-works. A synopsis of 16 assaults are given in Table II, and are characterized into the accompanying five fundamental classes: personality based assaults, control based assaults, cryptanalytic at-tacks, notoriety based assaults, and administration based assaults, as introduced in Figure 5

Identity-based attacks

The assaults under this classification fashion personalities to masquer-ade as approved clients, so as to gain admittance to the framework and control it. We characterize four assaults, to be specific: Key assault, Replay assault, Impersonation assault, and Sybil assault.

***Key attack*:**

This assault is characterized with regards to a framework consolidating electric vehicles and charging heaps, as pursues: "If the private key of an electric vehicle that has been utilized for long-term releases, the aggressor can imitate this electric vehicle to hoodwink others" [10]. To manage this assault, LNSC convention [10] gives a shared confirmation component between the electric vehicles and charging heaps. To this end, it utilizes the elliptic bend encryption to figure the hash capacities, and subsequently it guarantees flexibility against the key spillage assault.

***Replay attack*:**

The point of this assault is to parody the personalities of two gatherings, capture their information parcels, and hand-off them to their goals without modifica-tion. To oppose against this assault, LNSC [10] utilizes the possibility of elliptic bend encryption to compute the hash capacities. Then again, BSein [39] utilizes a new one-time open/private key pair, which is created for each solicitation, to scramble the message and process the Message Authentication Code (MAC). Along these lines, the replay assault can be identified.

DOI: 10.15680/IJIRCCE.2019. 0708013

***Impersonation attack*:**

A foe attempts to take on the appearance of an authentic client to perform unapproved tasks. As introduced in Table II, there are three techniques that are proposed to secure against this assault. The possibility of elliptic bend encryption to figure the hash capacities, is proposed by LNSC convention [10]. Wang et al. [16] propose a circulated impetus based collaboration mech-anism, which ensures the client's security just as an exchange check strategy for the hub participation. The system conceals the client's security data inside a gathering, and guarantees their insurance from the pantomime assault. BSeIn [39], then again, utilizes characteristic based marks, i.e., just real terminals can produce a substantial mark, and subsequently any pantomime endeavor will be identified when its relating verification activity falls flat.

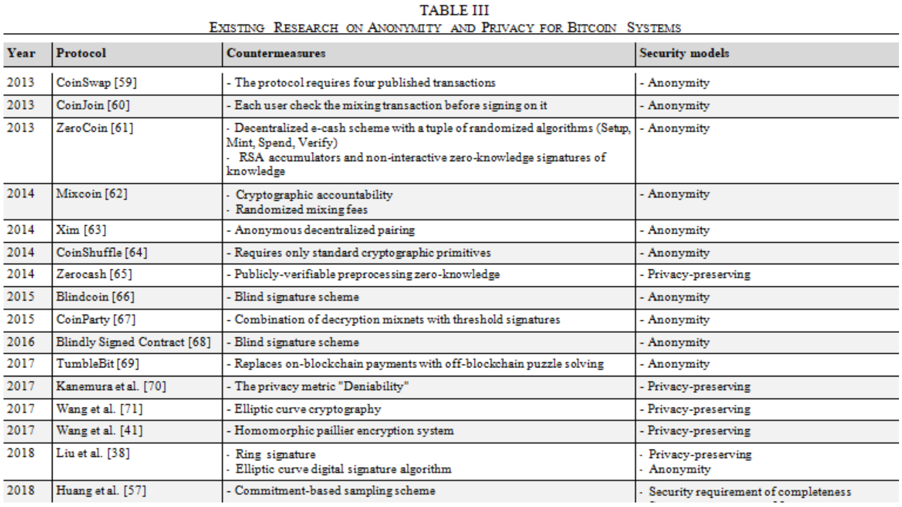


TABLE III
Existing Research on Anonymity and Privacy for Bitcoin Systems

Year	Protocol	Countermeasures	Security models
2013	CoinSwap [59]	- The protocol requires four published transactions	- Anonymity
2013	CoinJoin [60]	- Each user check the mixing transaction before signing on it	- Anonymity
2013	ZeroCoin [61]	- Decentralized e-cash scheme with a tuple of randomized algorithms (Setup, Mint, Spend, Verify) - RSA accumulators and non-interactive zero-knowledge signatures of knowledge	- Anonymity
2014	Mixcoin [62]	- Cryptographic accountability - Randomized mixing fees	- Anonymity
2014	Xim [63]	- Anonymous decentralized pairing	- Anonymity
2014	CoinShuffle [64]	- Requires only standard cryptographic primitives	- Anonymity
2014	Zerocash [65]	- Publicly-verifiable preprocessing zero-knowledge	- Privacy-preserving
2015	Blindcoin [66]	- Blind signature scheme	- Anonymity
2015	CoinParty [67]	- Combination of decryption mixnets with threshold signatures	- Anonymity
2016	Blindly Signed Contract [68]	- Blind signature scheme	- Anonymity
2017	TumbleBit [69]	- Replaces on-blockchain payments with off-blockchain puzzle solving	- Anonymity
2017	Kanemura et al. [70]	- The privacy metric "Deniability"	- Privacy-preserving
2017	Wang et al. [71]	- Elliptic curve cryptography	- Privacy-preserving
2017	Wang et al. [41]	- Homomorphic paillier encryption system	- Privacy-preserving
2018	Liu et al. [38]	- Ring signature - Elliptic curve digital signature algorithm	- Privacy-preserving - Anonymity
2018	Huang et al. [57]	- Commitment-based sampling scheme	- Security requirement of completeness

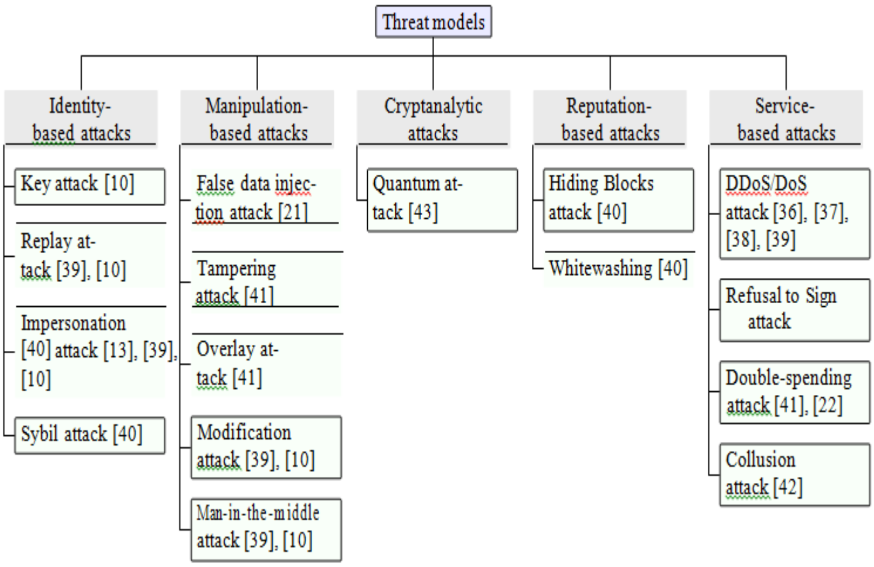


Fig. 5. Classification of threat models for Blockchain.

***Sybil attack*:**

Under this assault, a foe makes many phony characters. By performing numerous collaborations in the system, the foe can increase an enormous impact inside the network, i.e, expanding/diminishing the notoriety of certain specialists. TrustChain [40] addresses this issue by making an unchanging chain of transiently requested between activities for every specialist. It registers the reliability of specialists in an online network with Sybil-opposition by utilizing earlier exchanges as info. It guarantees that operators who use assets from the network likewise contribute back.

Manipulation-basedattacks:

***False data injection attack*:**The point of this assault is to bargain the information trustworthiness of the control framework to settle on it take wrong control choices. Liang et al. [21] considers the meter hub as a private blockchain organize.

***Tampering attack*:** The foe may alter the bitcoin exchanges of the bitcoin addresses, sums and other data in the wake of marking. To avert this assault, Wang et al. [41] utilize an open key cryptosystem that is good with the current Bitcoin framework. They propose including the homomorphic Paillier encryption framework to cover the plaintext sums in exchanges, and the scrambled sums will be checked by the Commitment Proof.

***Overlay attack*:** It implies that the assailant adds a fabrication scrambled add up to the first encoded sum under the beneficiary's open key. In [41], this assault is distinguished as each exchange is inserted with a timestamp to check its uniqueness. Various contributions under a similar dealer can be recognized and connected to the various exchanges, and subsequently opposition against the overlay assault is guaranteed

Modification attack: It comprises in changing the communicate exchange or the reaction message. To manage this at-tack, LNSC [10] utilizes the possibility of elliptic bend encryption to figure the hash capacities. BSeIN [39], then again, utilizes the quality mark and the MAC.

***Man-in-the-middle attack*:** An assailant by ridiculing the characters of two gatherings can furtively transfer and even adjust the correspondence between these gatherings, which accept they are conveying legitimately, yet in truth the entire discussion is under the influence of the aggressor. To oppose against this assault, BSeIn [39] gives secure shared validation. In [10], LNSC gives shared au-thentication by utilizing elliptic bend encryption to compute the hash capacities.

Cryptanalytic attacks:

They intend to break the cryptographic calculation and ex-represent its keys. In [43] the quantum assault is examined in blockchain. This assault is intended to settle the elliptic bend computerized logarithm, i.e., get the private key from the elliptic bend open key. Along these lines, an enemy can sign unapproved exchanges and produce the legitimate mark of clients. To manage this issue, Yin et al. [43] utilizes the possibility of grid based mark conspire., which permits inferring many sub-private keys from the seed in the deterministic wallet of blockchain.

Reputation-based attacks

An operator controls his notoriety by transforming it to a positive one. In this classification, we can locate the accompanying assaults, to be specific: Hiding Blocks assault, and Whitewashing assault.

DOI: 10.15680/IJIRCCE.2019. 0708013

***Hiding Blocks attack*:**

Under this assault, an operator just uncovered exchanges that positively affect his notoriety and conceals the ones with negative notoriety. In [40], an unchanging chain of transiently requested interac-tions for every operator. Since each record has an arrangement number, any operator in the system can demand explicit records of others. The mentioned operators can't decline to give their records. Something else, different operators will quit interfacing with them**.**

***Whitewashing*:**

At the point when an operator has negative notoriety, it can dispose of its character and make another one. There is no real way to avoid this conduct. Nonetheless, it is proposed in [40] to give lower needs to the specialists of new characters when applying the assignment approach.

Service-basedattacks:

They point either to make the administration inaccessible or cause it to carry on uniquely in contrast to its determinations. Under this classification, we can locate the accompanying assaults:

***DDoS/DoS attack*:**

It includes sending a lot of solicitations to cause the disappointment of the blockchain framework. As appeared in Table II, there are four techniques that are proposed to manage this assault. Distributed SDN engineering is proposed by DistBlockNet convention in [36]. CoinParty [37] proposes decentralized blending administration. Liu et al. [38] utilize a ring-based mark with Elliptic Curve Digital Signature Algorithm (ECDSA). The versatility against DOS in BSeIn [39] is accomplished by constraining the square size, checking the maxi-mum number of quality marks for the exchange info, and utilizing multi-recipients encryption to give secrecy to approved members.

***Refusal to Sign attack*:**

It includes sending a lot of solicitations to cause the disappointment of the blockchain framework. As appeared in Table II, there are four strategies that are proposed to manage this assault. Distributed SDN engineering is proposed by DistBlockNet convention in [36]. CoinParty [37] proposes decentralized blending administration. Liu et al. [38] utilize a ring-based mark with Elliptic Curve Digital Signature Algorithm (ECDSA). The strength against DOS in BSeIn [39] is accomplished by restricting the square size, checking the maxi-mum number of characteristic marks for the exchange info, and utilizing multi-recipients encryption to give classification to approved members.

***Double-spending attack*:**

It implies that the aggressors spend the equivalent bitcoin twice to secure additional sums. In [41], the Time-Stamp and the Proof-of-Work system is utilized. In [22], a multi-signature exchange is utilized, where a base number of keys must sign an exchange before spending tokens.

***Collusion Attack*:**

Hubs can conspire with one another and act childishly to boost their benefit. In [42], a motivator system and evaluating methodology is proposed to ruin the narrow minded practices.

IV. EXISTING RESEARCH ON SECURITY AND PRIVACY IN BLOCKCHAIN-BASEDIOT

Table IV condenses examine for blockchain-based IoT security and protection**.**

Authentication

In [78], Lin et al. proposed a novel transitively shut undirected diagram verification plot that can bolster blockchain-based character the executives frameworks. In compar-ison to other contending validation plots, their professional posal gives an extra capacity of progressively including or erasing hubs and edges. Additionally, this novel plan that was based on Ethereum comprehends the confirmation prob-lem of non-existent edges, which is a realized test in transitive mark plans. Lin et al.in [39] proposed a novel blockchain-based structure that can guarantee a safe remote client confirmation. The proposed system joins characteristic based marks, multi-recipients encryption and Mes-sage Authentication Code. In [14], Li et al. proposed a novel protection saving Blockchain-based declaration arrange for Vanets that depends on a limit verification convention called Echo-Announcement.

Creators in [75] proposed an ID-based straightly homo-morphic mark plots that can be utilized for acknowledging verification in blockchains. The framework enables an endorser to create straightly homomorphic marks, and henceforth it maintains a strategic distance from the inadequacies of open key authentications. Moreover, it is demonstrated to be powerful against a few assaults. In [74] creators presented the idea of blockchain as an administration. Their proposed blockchain based-ID as a Service (BIDaaS) instrument, is another sort of IDaaS that can be utilized for personality and validation the board. Confirmation can be accomplished without the utilization of any preregistered data of the client. At long last in [43] creators adapt to the issue of keeping the wallet in a generally little size while guaranteeing the vigor of exchange validation by presenting a novel enemy of quantum exchange confirmation conspire.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

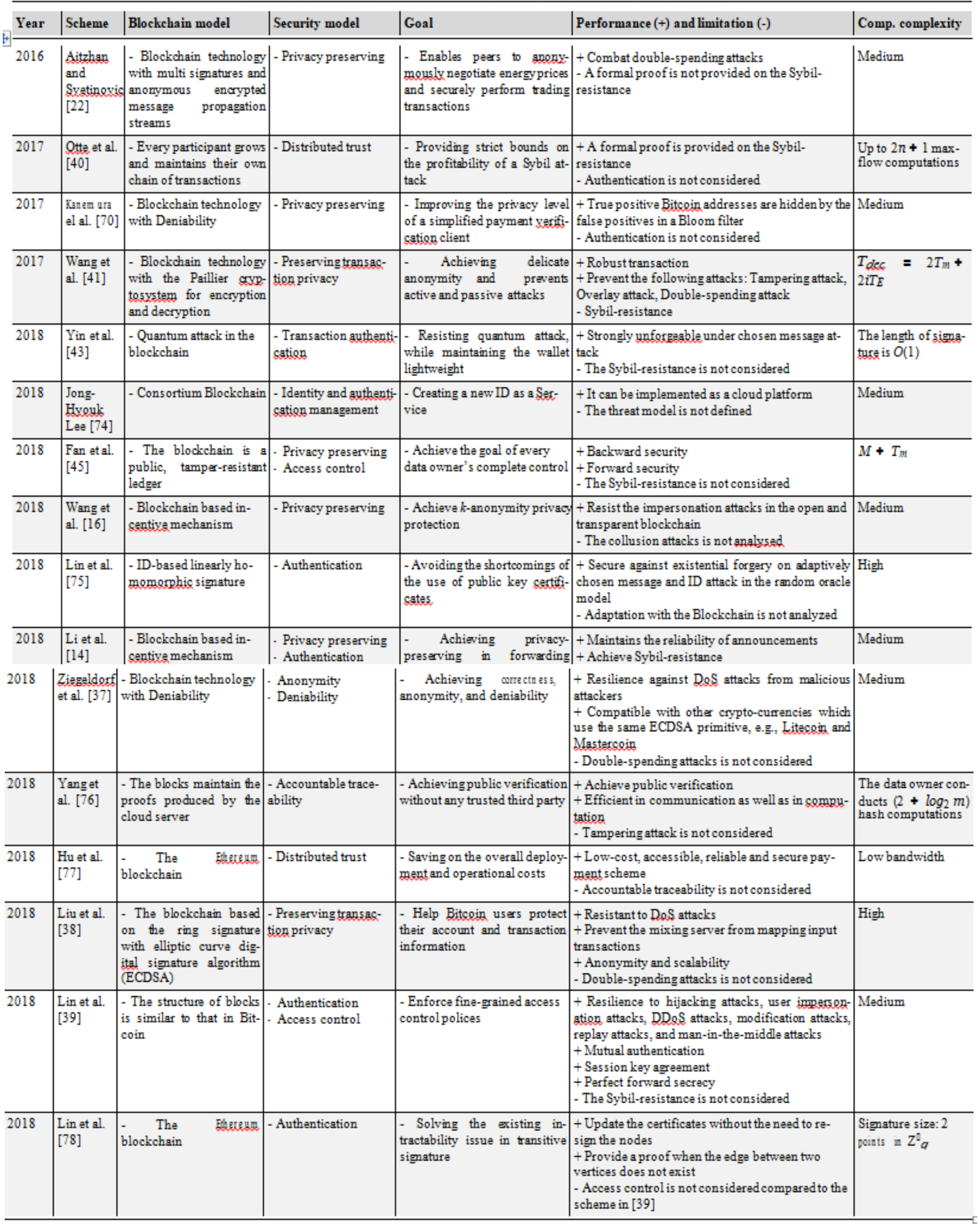
International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 8, August 2019

TABLE IV
EXISTING RESEARCH FOR BLOCKCHAIN-BASED IOT SECURITY AND PRIVACY



Year	Scheme	Blockchain model	Security model	Goal	Performance (+) and limitation (-)	Comp. complexity
2016	Aitzhan and Svetinovic [22]	- Blockchain technology with multi signatures and anonymous encrypted message propagation streams	- Privacy preserving	- Enables peers to anonymously negotiate energy prices and securely perform trading transactions	+ Combat double-spending attacks - A formal proof is not provided on the Sybil-resistance	Medium
2017	Otte et al. [40]	- Every participant grows and maintains their own chain of transactions	- Distributed trust	- Providing strict bounds on the profitability of a Sybil attack	+ A formal proof is provided on the Sybil-resistance - Authentication is not considered	Up to $2n + 1$ max-flow computations
2017	Kanemura el al. [70]	- Blockchain technology with Deniability	- Privacy preserving	- Improving the privacy level of a simplified payment verification client	+ True positive Bitcoin addresses are hidden by the false positives in a Bloom filter - Authentication is not considered	Medium
2017	Wang et al. [41]	- Blockchain technology with the Paillier cryptosystem for encryption and decryption	- Preserving transaction privacy	- Achieving delicate anonymity and prevents active and passive attacks	+ Robust transaction + Prevent the following attacks: Tampering attack, Overlay attack, Double-spending attack - Sybil-resistance	$T_{dec} = 2T_m + 2iT_E$
2018	Yin et al. [43]	- Quantum attack in the blockchain	- Transaction authentication	- Resisting quantum attack, while maintaining the wallet lightweight	+ Strongly unforgeable under chosen message attack - The Sybil-resistance is not considered	The length of signature is $O(1)$
2018	Jong-Hyouk Lee [74]	- Consortium Blockchain	- Identity and authentication management	- Creating a new ID as a Service	+ It can be implemented as a cloud platform - The threat model is not defined	Medium
2018	Fan et al. [45]	- The blockchain is a public, tamper-resistant ledger	- Privacy preserving - Access control	- Achieve the goal of every data owner's complete control	+ Backward security + Forward security - The Sybil-resistance is not considered	$M + T_m$
2018	Wang et al. [16]	- Blockchain based incentive mechanism	- Privacy preserving	- Achieve *k*-anonymity privacy protection	+ Resist the impersonation attacks in the open and transparent blockchain - The collusion attacks is not analysed	Medium
2018	Lin et al. [75]	- ID-based linearly homomorphic signature	- Authentication	- Avoiding the shortcomings of the use of public key certificates	+ Secure against existential forgery on adaptively chosen message and ID attack in the random oracle model - Adaptation with the Blockchain is not analyzed	High
2018	Li et al. [14]	- Blockchain based incentive mechanism	- Privacy preserving - Authentication	- Achieving privacy-preserving in forwarding	+ Maintains the reliability of announcements + Achieve Sybil-resistance	Medium
2018	Ziegeldorf et al. [37]	- Blockchain technology with Deniability	- Anonymity - Deniability	- Achieving correctness, anonymity, and deniability	+ Resilience against DoS attacks from malicious attackers + Compatible with other crypto-currencies which use the same ECDSA primitive, e.g., Litecoin and Mastercoin - Double-spending attacks is not considered	Medium
2018	Yang et al. [76]	- The blocks maintain the proofs produced by the cloud server	- Accountable traceability	- Achieving public verification without any trusted third party	+ Achieve public verification + Efficient in communication as well as in computation - Tampering attack is not considered	The data owner conducts $(2 + log_2\ m)$ hash computations
2018	Hu et al. [77]	- The Ethereum blockchain	- Distributed trust	- Saving on the overall deployment and operational costs	+ Low-cost, accessible, reliable and secure payment scheme - Accountable traceability is not considered	Low bandwidth
2018	Liu et al. [38]	- The blockchain based on the ring signature with elliptic curve digital signature algorithm (ECDSA)	- Preserving transaction privacy	- Help Bitcoin users protect their account and transaction information	+ Resistant to DoS attacks + Prevent the mixing server from mapping input transactions + Anonymity and scalability - Double-spending attacks is not considered	High
2018	Lin et al. [39]	- The structure of blocks is similar to that in Bitcoin	- Authentication - Access control	- Enforce fine-grained access control polices	+ Resilience to hijacking attacks, user impersonation attacks, DDoS attacks, modification attacks, replay attacks, and man-in-the-middle attacks + Mutual authentication + Session key agreement + Perfect forward secrecy - The Sybil-resistance is not considered	Medium
2018	Lin et al. [78]	- The Ethereum blockchain	- Authentication	- Solving the existing intractability issue in transitive signature	+ Update the certificates without the need to resign the nodes + Provide a proof when the edge between two vertices does not exist - Access control is not considered compared to the scheme in [39]	Signature size: 2 points in Z^2_q

Notations :

M : The time for one exponentiation;
Tm:The size of the ciphertext;
$Tdec$: The time for decryption;

DOI: 10.15680/IJIRCCE.2019. 0708013

Tm:The unit of modular multiplication time;
TE:The unit of modular exponentiation time

Privacy-preserving

In the center of blockchain theory lies the private key that can open the cryptographic assurance of the computerized resources. The private key turns into the most noteworthy helplessness of a blockchain framework whether it is put away on a bit of paper, screen, circle, in nearby memory or in the cloud. Clients will in general utilize advanced wallets that can be either programming or equipment, for example Trezor or Keepkey, which are defenseless against different assaults like shortcoming infusions [79].

Another arrangement that is making strides these days is the utilization of equipment security modules (HSMs), a crypto-processor that safely produces, ensures and stores keys. The whole cryptographic key lifecycle occurs inside the HSM. A HSM can be an independent gadget that works disconnected or can be installed in a server, can be solidified against altering or harm, and is generally situated in a physically secure territory to counteract unapproved get to. At last another age of ultra-secure PCs that have implanted a HSM and requires two-factor validation is as of late presented. This PC can be ensured against physical assaults with a sealed packaging and components like programmed erasion of the private key if there should be an occurrence of any rupture of the inserted physical or legitimate security controls [80]. Utilizing confided in PCs both as secure advanced wallets and blockchain hubs. Security affirmation of clients and associations need so as to believe this new innovation can be given sooner rather than later.

To accomplish k-obscurity security insurance, Wang et al. [16] utilize a hub collaboration confirmation approach, in which each gathering contains K hubs to meet the goal of K-namelessness assurance. Aitzhan et al. [22] proposed a thought that secures parties from inactive listening in by covering up non-content information. For upgrading the exchange protection in Bitcoin, Wang et al. [41]achieve exchange by utilizing cryptographic techniques, i.e., utilizes the open key framework. Through the standard ring mark and ECDSA unforgeability, Liu et al. [38] proposed a thought that can accomplish the obscurity.

One other part of protection in blockchain frameworks is about obscurity. In spite of the fact that it is conceivable to plan a nearly im-changeable, alter safe exchange, this exchange can be seen all through the majority of the hubs on the blockchain organize. One promising examination on supporting private exchanges inside a blockchain is zk-STARKs, which joins zCash and Ethereum. The mix of the two innovations makes it conceivable to keep secrecy when directing installments, dazzle barters, and notwithstanding casting a ballot [73].

Trust

A blockchain-based installment conspire that is stet up in a remote locale setting was presented in [77]. The proposed plan is expected to have a discontinuous network to a bank's focal framework. Conveyed trust is practiced with the utilization of a two-layer design, where the bank approves a lot of chosen townspeople to go about as excavators who on their turn approve exchanges among residents with tokens and the bank. In [40] creators present an instrument where each member develops and keeps up his own chain of exchanges. The proposed methodology gives conveyed trust, without the need of any guard, while being vigorous against Sybil assaults.

V. OPEN QUESTIONS AND RESEARCHCHALLENGES

To finish our diagram, we layout both open inquiries and research difficulties that could improve the abilities and viability of blockchain for the IoT, abridged in the accompanying suggestions:

Resiliency against CombinedAttacks

As introduced in this review, numerous security answers for bloackchain-based IoT have been proposed in the writing, every one of which is intended to handle distinctive security issues and risk models. The fundamental inquiry that may emerge is the manner by which to structure a security arrangement that can be flexible against com-bined assaults while considering the execution attainability of the arrangement, particularly if there should arise an occurrence of low asset compelled IoT gadgets.

Dynamic and Adaptable Security Framework

Heterogeneous gadgets are sent in the IoT arrange, running from low-control gadgets to top of the line servers. Henceforth, a solitary security arrangement can't be conveyed for all the blockchain-based IoT structures because of the diverse measure of assets that are given. Consequently, the security arrangement ought to at first adjust to the current assets, and choose which security administrations to offer, to meet the base security necessities of the end-clients. In this manner, one of the difficulties that ought to get more consideration later on is the means by which to structure such a dynamic and versatile security system for blockchain-based IoT designs.

Compliance with GDPR

The new guideline that produced results from the 25th of May of 2018 awards end-clients new controls over close to home information, and places new commitments upon information controllers. In an absolutely decentralized blockchain framework there are no responsible information processors making the execution of GDPR troublesome. Additionally then again, the privilege to be overlooked that is one of the primary rules of GDPR is deeply opposing thought behind blockchain innovation. On open blockchains, all information is repeated and shared over all machines in the system and just the blend with believed equipment arrangements can understand this issue. Some underlying endeavors are as of now embraced [81], [82] however this is a promising zone of research for the not so distant future.

Energy-efficient Mining

Mining incorporates the execution of the blockchain con-sensus calculations, for example, Proof-of-Work (PoW). Furthermore, the blockchain develops as the clients store their exchanges. Along these lines, all the more dominant excavators are required to deal with the accord conventions in the blockchain. A few Everything productive agreement calculations, for example, Proof-of-Space [83], Deligated Proof-of-Space [84] and Proof-of-Stake [85] and small scale blockchain [86], [87] to store just late blockchain exchanges are proposed. Nonetheless, asset and power-obliged IoT gadgets are not constantly fit for gathering the considerable computational and control utilization in the master cessing of blockchain agreement and putting away of blockchains. Along these lines, the structure of Everything effective accord conventions is one of the noteworthy research difficulties in the blockchain innovations for IoT.

Social Networks and Trust Management

When we talk about security we need to take at the top of the priority list that phony news can be a piece of a digital assault. Huge scale gossip spreading could present serious social and financial harms to an association or a country [88] particularly with the utilization of online informal organizations. Blockchains could be a methods for constraining gossip spreading as exhibited in [89] where a blockchain-empowered informal community is displayed.

Blockchain-specific Infrastructure

The capacity restricted IoT gadgets probably won't have the option to store the enormous size blockchain that develops as the squares are added in the blockchain. In addition, it is generally observed that the IoT gadgets store the blockchain's information that are not utilize ful for their own exchanges. In this way, blockchain-explicit hardware that supports the decentralized stockpiling of enormous size blockchain become a difficult issue. Additionally, the location the executives and hidden correspondence conventions assume noteworthy jobs in blockchain foundation. Additionally, dependability among the computational asset improved gadgets must be built up in the blockchain framework. Plus, the Application Programming Interface (APIs) ought to be easy to use however much as could reasonably be expected.

Vehicular Cloud Advertisement Dissemination

As displayed in this review, in light of a decentralized blockchain structure, different obscurity plans are proposed to shroud the genuine personalities in IoV. In this way, since the ve-hicle's genuine character, vehicle's genuine area, and exchange could be revealed in vehicular cloud notice spread [90], basic security issues emerge as pursues:

- How to structure a solitary quality access control convention dependent on blockchain innovation for safeguarding transac-tion security in vehicular cloud promotion dissemina-tion?
- How to devise a protection safeguarding mystery sharing plan dependent on blockchain innovation to recognize partici-pation of chose vehicles in exchanges? e.g., by utilizing the homomorphic Paillier encryption framework.
- How to plan a low intricacy based validation utilizing the blockchain innovation among RSUs and standard ticipating vehicles during the commercial dispersal process?

Skyline Query Processing

Horizon question has turned into a significant issue in database investigate, e.g., concentrated database, dispersed database, and comparability search. The reviewed plans have not yet considered the plausibility of utilizing the horizon inquiry with blockchain. As of late, Hua et al. [91] proposed a security saving on-line restorative essential analysis system, named CINEMA, which uses the horizon question. In particular, CINEMA outline work can secure clients' medicinal information protection and guarantee the privacy of analysis model dependent on a horizon conclusion model. In this way, how to deal with the security and protection issues when a horizon determination model is built by a great deal of blockchains? Henceforth, the protection safeguarding plans dependent on the blockchain with horizon question are significant difficulties and ought to be examined later on.

VI. CONCLUSION

In this paper, we overviewed the best in class of existing blockchain conventions intended for Internet of Things (IoT) systems. We gave an outline of the application spaces of blockchain advances in IoT, e.g., Internet of Vehicles, Internet of Energy, Internet of Cloud, and Fog registering. Through broad research and investigation that was directed, we had the option to group the danger models that are considered by the blockchain conventions in IoT systems, into five fundamental classes, in particular, character based assaults, control based assaults, cryptanalytic assaults, notoriety based assaults, and administration based assaults. There still exist a few testing research zones, for example, versatility against joined assaults, dynamic and versatile security system, consistence with GDPR, Everything productive mining, interpersonal organizations and trust man-agement, blockchain-explicit foundation, vehicular cloud commercial dispersal, and Skyline question handling, which ought to be additionally examined sooner rather than later.

REFERENCES

[1]“IDC, Worldwide Internet of Things Forecast, 2015–2020,” IDC #256397.
[2]“IDC, Worldwide Internet of Things Forecast Update 2015–2019,” Feb.
2016, Doc #US40983216.
[3]D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” *Ad Hoc Netw.*, vol.10,no.7,pp.1497–1516,Sept.2012.
[4]D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, “Everything you wanted to know about the blockchain: Its promise, components, processes, and problems,” *IEEE Consumer Electronics Mag.*, vol. 7, no. 4, pp. 6–14, July 2018.
[5]M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choud- hury, and V. Kumar, “Security and privacy in fog computing: Challenges,” *IEEE Access*, vol. 5, pp. 19 293–19 304, 2017.

[6]M. Swan, *Blockchain: blueprint for a new economy*, 1st ed. ÓReilly Media, Jan. 2015.

[7]F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” *IEEE Commun. Surveys & Tut.*, vol. 18, no. 3, pp. 2084–2123, Mar. 2016.

[8]S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [9]D. Wilson and G. Ateniese, “From pretty good to great: Enhancing PGP using bitcoin and the blockchain,” in *Network and System Security*. Springer International Publishing, 2015, pp. 368–375.

[10]X. Huang, C. Xu, P. Wang, and H. Liu, “LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem,” *IEEE Access*, vol. 6, pp. 13 565–13 574,2018.

[11]A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, “BlockChain: A Distributed Solution to Automotive Security and Privacy,” *IEEE Commun.Mag.*,vol.55,no.12,pp.119–125,dec2017.

[12]A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, “Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems,” *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, dec 2017.

[13]J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, “Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains,” *IEEE Trans. Ind. Informatics*, vol. 13, no. 6, pp. 3154–3164, dec 2017.

[14]L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, “CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles,” *IEEE Trans. Intell. Transp. Syst.*, pp. 1–17, 2018.

[15]Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, “A blockchain-based reputation system for data credibility assessment in vehicular networks,” in *2017 IEEE 28th Annu. Int. Symp. Pers. Indoor, Mob. Radio Commun.* IEEE, oct 2017, pp. 1–5.

[16]J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, “A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications,”*IEEEAccess*,vol.6,pp.17545–17556,2018.

[17]F. Tian, “An agri-food supply chain traceability system for China based on RFID & blockchain technology,” in *Proc. IEEE 13th Int. Conf. on ServiceSystemsandServiceManagement(ICSSSM)*,June2016.

[18]Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, “Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things,” *IEEE Trans. Ind. Informatics*, pp. 1–1, 2017.

[19]T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, “Blockchain technology innovations,” in *Proc. IEEE Technology & Engineering Management Conference (TEMSCON)*, June 2017.

[20]J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, “GridMonitoring: Secured sovereign blockchain based monitoring on smart grid,” *IEEE Access*, vol. 6, pp. 9917–9925, 2018.

[21]G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, “Distributed Blockchain-Based Data Protection Framework for Modern Power Systems against Cyber Attacks,” *IEEE Trans. Smart Grid*, pp. 1–1, 2018.

[22]N. Zhumabekuly Aitzhan and D. Svetinovic, “Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams,” *IEEE Trans. Dependable Secur. Comput.*, pp. 1–1,2016.

[23]N. Kshetri, “Blockchain’s roles in strengthening cybersecurity and protecting privacy,” *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, Nov. 2017.

[24]T. M. Fernández-Caramés and P. Fraga-Lamas, “A review on the use of blockchain for the internet of things,” *IEEE Access*, pp. 1–23, May 2018.

[25]“Crypto-currency market capitalizations,” accessed on 15 June, 2018. [Online]. Available: https://coinmarketcap.comhttps://coinmarketcap.com

[26]“Blockchain technology report to the US federal advisory committeeon insurance,” accessed on 15 June, 2018.[Online]. Available:https://www.treasury.gov/initiatives/fio/Documents/McKinsey_FACI_Blockchain_in_Insurance.pdf

[27]L. Bahack, “Theoretical Bitcoin attacks with less than half of the computational power,” Dec. 2013, arXiv:1312.7013v1.[Online]. Available: https://arxiv.org/pdf/1312.7013.pdf

[28]M. Ali, J. Nelson, R. Shea, and M. J. Freedman, “Blockstack: A global naming and storage system secured by blockchains,” in *Proc. Annual Technical Conference (USENIX ATC)*, June 2016, pp. 181–194.

[29]L. S. Sankar, M. Sindhu, and M. Sethumadhavan, “Survey of consensus protocols on blockchain applications,” in *Proc. IEEE 4th Int. Conf. on Advanced Comput. and Commun. Syst. (ICACCS)*, Jan. 2017.

[30]A. Kaushik, A. Choudhary, C. Ektare, D. Thomas, and S. Akram, “Blockchain-literature survey,” in *Proc. IEEE 2nd Int. Conf. Recent Trends in Electronics, Information & Communication Technology (RTE- ICT)*, May 2017.

[31]M. C. K. Khalilov and A. Levi, “A survey on anonymity and privacy in Bitcoin-like digital cash systems,” *IEEE Commun. Surveys & Tut.*, pp. 1–1, Mar. 2018.

[32]M. Conti, S. K. E, C. Lal, and S. Ruj, “A survey on security and privacy issues of Bitcoin,” *IEEE Commun. Surveys & Tut.*, pp. 1–39, May 2018.

[33]C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, “Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?” *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan. 2018.

[34]R. Guo, H. Shi, Q. Zhao, and D. Zheng, “Secure Attribute-Based Sig- nature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems,” *IEEE Access*, vol. 6, pp. 11 676–11 686, 2018.

[35]X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, “Integrating blockchain for data sharing and collaboration in mobile healthcare applications,” in *2017 IEEE 28th Annu. Int. Symp. Pers. Indoor, Mob. Radio Commun.*IEEE, oct 2017, pp.1–5.

[36]P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, “DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks,”*IEEECommun.Mag.*,vol.55,no.9,pp.78–85,2017.

[37]J. H. Ziegeldorf, R. Matzutt, M. Henze, F. Grossmann, and K. Wehrle, “Secure and anonymous decentralized Bitcoin mixing,” *Futur. Gener. Comput. Syst.*, vol. 80, pp. 448–466, mar 2018.

[38]Y. Liu, X. Liu, C. Tang, J. Wang, and L. Zhang, “Unlinkable Coin Mixing Scheme for Transaction Privacy Enhancement of Bitcoin,”*IEEE Access*, vol. 6, pp. 23 261–23 270,2018.

[39]C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, "Bsein: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *J. Netw. Comput. Appl.*, vol. 116, pp. 42–52, 2018.
[40]P. Otte, M. de Vos, and J. Pouwelse, "TrustChain: A Sybil-resistant scalable blockchain," *Futur. Gener. Comput. Syst.*, sep 2017.
[41]Q. Wang, B. Qin, J. Hu, and F. Xiao, "Preserving transaction privacy in bitcoin," *Futur. Gener. Comput. Syst.*, sep 2017.
[42]Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, "A Blockchain based Truthful Incentive Mechanism for Distributed P2P Applications,"*IEEE Access*, pp. 1–1,2018.
[43]W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, "An Anti-Quantum Transaction Authentication Approach in Blockchain," *IEEE Access*, vol. 6, pp. 5393–5401,2018.
[44]M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *J. Netw. Comput. Appl.*, vol. 101, pp. 55–82, jan 2018.
[45]K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," *IET Commun.*, vol. 12, no. 5, pp. 527–532, Mar. 2018.
[46]J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, "Consortium Blockchain-Based Malware Detection in Mobile Devices," *IEEE Access*, vol. 6, pp. 12 118–12 128, 2018.
[47]B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for em- bedded devices in an Internet of Things environment," *J. Supercomput.*, vol. 73, no. 3, pp. 1152–1167, mar 2017.
[48]O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.
[49]N. Herbaut and N. Negru, "A Model for Collaborative Blockchain-Based Video Delivery Relying on Advanced Network Services Chains," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 70–76, 2017.
[50]C. Xu, K. Wang, and M. Guo, "Intelligent Resource Management in Blockchain-Based Cloud Datacenters," *IEEE Cloud Comput.*, vol. 4, no.6,pp.50–59,nov2017.
[51]P. K. Sharma, M.-Y. Chen, and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," *IEEE Access*,vol.6,pp.115–124,2018.
[52]Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," *IEEE Access*, vol. 5, pp. 14 757–14 767,
2017.
[53]N. Alexopoulos, E. Vasilomanolakis, N. R. Ivanko, and M. Muhlhauser, "Towards blockchain-based collaborative intrusion detection systems," in*Proc.Int.Conf.CriticalInf.Infrastruct.Secur*,2017,pp.1–12.
[54]W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When Intrusion Detection Meets Blockchain Technology: A Review," *IEEE Access*, vol. 6, pp. 10 179–10 188, 2018.
[55]T. Cruz, L. Rosa, J. Proença, L. Maglaras, M. Aubigny, L. Lev, J. Jiang, and P. Simões, "A cybersecurity detection framework for supervisory control and data acquisition systems," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 6, pp. 2236–2246, 2016.
[56]K. Kalkan and S. Zeadally, "Securing internet of things (iot) with software defined networking (sdn)," *IEEE Commun. Mag.*, 2017.
[57]H. Huang, X. Chen, Q. Wu, X. Huang, and J. Shen, "Bitcoin-based fair payments for outsourcing computations of fog devices," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 850–858, jan 2018.
[58]P. Jiang, F. Guo, K. Liang, J. Lai, and Q. Wen, "Searchain: Blockchain- based private keyword search in decentralized storage," *Futur. Gener. Comput. Syst.*, sep 2017.
[59]G. Maxwll, "Coinswap," 2013. [Online]. Available: https://bitcointalk.org/index.php?topic=321228
[60]G. Maxwell, "Coinjoin: Bitcoin privacy for the real world," in *Post on Bitcoin forum*, 2013.
[61]I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous Distributed E-Cash from Bitcoin," in *2013 IEEE Symp. Secur. Priv.* IEEE, may 2013, pp. 397–411.
[62]J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for Bitcoin with Accountable Mixes," in *Int. Conf. Financ. Cryptogr. Data Secur.* Springer Berlin Heidelberg, 2014, pp. 486–504.
[63]G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, "Sybil- Resistant Mixing for Bitcoin," in *Proc. 13th Work. Priv. Electron. Soc. -WPES'14*.New York, New York, USA: ACM Press, 2014, pp. 149–158.
[64]T. Ruffing, P. Moreno-Sanchez, and A. Kate, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin," in *Eur. Symp. Res. Comput. Secur.* Springer, 2014, pp. 345–364.
[65]E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized Anonymous Payments from Bitcoin," in *2014 IEEE Symp. Secur. Priv.* IEEE, may 2014, pp. 459– 474.
[66]L. Valenta and B. Rowan, "Blindcoin: Blinded, Accountable Mixes for Bitcoin," in *Int. Conf. Financ. Cryptogr. Data Secur.* Springer Berlin Heidelberg, 2015, pp. 112–126.
[67]J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, "Coinparty: Secure multi-party mixing of bitcoins," in *Proc. 5th ACM Conf. Data Appl. Secur. Priv. - CODASPY '15*. New York, New York, USA: ACM Press, 2015, pp. 75–86.
[68]E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions," in *Int. Conf. Financ. Cryptogr. Data Secur.* Springer Berlin Heidelberg, 2016, pp. 43–60.
[69]E. Heilman, L. AlShenibr, F. Baldimtsi, A. Scafuro, and S. Goldberg, "TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub,"in*Proc.2017Netw.Distrib.Syst.Secur.Symp.* Reston, VA: Internet Society,2017.
[70]K. Kanemura, K. Toyoda, and T. Ohtsuki, "Design of privacy-preserving mobile Bitcoin client based on γ-deniability enabled bloom filter," in *2017 IEEE 28th Annu. Int. Symp. Pers. Indoor, Mob. Radio Commun.* IEEE, oct 2017, pp. 1–6.
[71]H. Wang, D. He, and Y. Ji, "Designated-verifier proof of assets for bit- coin exchange using elliptic curve cryptography," *Futur. Gener.Comput. Syst.*, jul2017.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 8, August 2019

[72]M. C. K. Khalilov and A. Levi, "A Survey on Anonymity and Privacy in Bitcoin-like Digital Cash Systems," *IEEE Commun. Surv. Tutorials*, pp. 1–1,2018.
[73]B. Qin, J. Huang, Q. Wang, X. Luo, B. Liang, and W. Shi, "Cecoin: A decentralized PKI mitigating MitM attacks," *Futur. Gener. Comput. Syst.*, oct2017.
[74]J.-H. Lee, "BIDaaS: Blockchain Based ID As a Service," *IEEE Access*, vol. 6, pp. 2274–2278, 2018.
[75]Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An ID- based linearly homomorphic signature scheme and its applicationin blockchain,"*IEEEAccess*,pp.1–1,2018.
[76]C. Yang, X. Chen, and Y. Xiang, "Blockchain-based publicly verifiable data deletion scheme for cloud storage," *J. Netw. Comput. Appl.*, vol. 103, pp. 185–193, feb 2018.
[77]Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna,
G. Jourjon, A. Seneviratne, and M. E. Ylianttila, "A Delay-Tolerant Payment Scheme Based on the Ethereum Blockchain," jan 2018. [Online]. Available: http://arxiv.org/abs/1801.10295
[78]C. Lin, D. He, X. Huang, M. K. Khan, and K.-K. R. Choo, "A New Transitively Closed Undirected Graph Authentication Scheme for Blockchain-based Identity Management Systems," *IEEE Access*, pp. 1– 1,2018.
[79]O. Boireau, "Securing the blockchain against hackers," *Network Secu- rity*, vol. 2018, no. 1, pp. 8–11, 2018.
[80]"This ultra-secure pc self destructs if someone messes with it," https://www.wired.com/2017/06/orwl-secure-desktop-computer/, accessed:2018-06-01.
[81]J. Lind, I. Eyal, F. Kelbert, O. Naor, P. Pietzuch, and E. G. Sirer, "Teechain: Scalable blockchain payments using trusted execution environments," *arXiv preprint arXiv:1707.05454*, 2017.
[82]I. Bentov, Y. Ji, F. Zhang, Y. Li, X. Zhao, L. Breidenbach, P. Daian, and
A. Juels, "Tesseract: Real-time cryptocurrency exchange using trusted hardware," 2017.
[83]S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," in *Proc. 35th Annual Cryptology Conference on Advances in Cryptology*, Aug. 2015, pp. 585–605.
[84]"DPOSdescriptiononbitshares,"accessedon15June,2018.[Online].
Available: http://docs.bitshares.org/bitshares/dpos.html [85]"Telehash," accessed on 15 June, 2018. [Online]. Available: http:
//telehash.org
[86]B. F.França, "Homomorphic mini-blockchain scheme," pp. 1–17, Apr. 2015, accessed on 15 June, 2018. [Online]. Available:http://cryptonite.info/files/HMBC.pdf
[87]J. D. Bruce, "The mini-blockchain scheme," 2014, accessed on
15 June, 2018. [Online]. Available: http://www.cryptonite.info/files/ mbc-scheme-rev2.pdf
[88]N. Ayres and L. A. Maglaras, "Cyberterrorism targeting the general public through social media," *Security and Communication Networks*, vol.9,no.15,pp.2864–2875,2016.
[89]Y. Chen, Q. Li, and H. Wang, "Towards trusted social networks with blockchain technology," *arXiv preprint arXiv:1801.02796*, 2018.
[90]Q. Kong, R. Lu, H. Zhu, and M. Ma, "Achieving secure and privacy- preserving incentive in vehicular cloud advertisement dissemination,"*IEEE Access*, vol. 6, pp. 25 040–25 050, 2018.
[91]J. Hua, H. Zhu, F. Wang, X. Liu, R. Lu, H. Li, and Y. Zhang, "Cinema: Efficient and privacy-preserving online medical primary diagnosis with skyline query," *IEEE Internet of Things Journal*, pp. 1–1, 2018.