ISSN 2278-3091

Volume 10, No.3, May - June 2021

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse1181032021.pdf

https://doi.org/10.30534/ijatcse/2021/1191032021

Survey on Transaction Verification Model based on Blockchain Architecture

Waqas Saeed [1], Dr Majid Husain [2], Hafiz M Mudassar Khan [3], Akbar Ali [4], Sajid Rehman Babar [5]

[1] Department of Computer Science, Sub Campus Gomal University Tank, Pakistan, waqas.researchers@gmail.com
[2] Department of Computer Science, Comsats University Sahiwal, Pakistan, majidhussain@ciitsahiwal.edu.pk
[3] Department of Computer Science, Superior University, Lahore, Pakistan, hafizmudassarkhan@gmail.com
[4] Department of Computer Science, Federal University of Technology, Islamabad, Pakistan, aakbarali18@gmail.com
[5] Department of Computer Science, Sub Campus Gomal University Tank, Pakistan, srehmanbabar@gmail.com

ABSTRACT

Similar to decentralized communication systems, a new technology called Blockchain (BC) has the potential to store and manage data in a decentralized manner. By removing the role of third party, all member in the chain has equal access to data. The concept BCT (Blockchain Technology) is not just limited to the cryptocurrencies, but it has been implemented in other areas like e-health, voting, finance, education, smart contract and even in Databases. This paper discusses various Blockchain applications and platforms and then compares these platforms on basis of different parameters. Despite of the advantages, Blockchain faces a significant issue of privacy. This paper examines various security related issues and challenges and presents an account of known possible attacks.

Key Words: Blockchain, Cryptocurrency, Cryptography, Authentication, Integrity, Privacy.

1. INTRODUCTION

A Blockchain (BC) is a distributed data structure that is replicated and shared among the users of a network. It was introduced with Bitcoin to solve the double-spending problem (a copy of the digital token is send to another merchant)[1]. To solve this problem a cryptographic technique is applied by CAFÉ Consortium and used electronic money (CAFÉ infrared Wallet and a card) by producing a secure open system for consumer payments. These wallets make use of public ledger called BC. By using BC the transactions is communicated to all parties are verified publicly in all network parties.[2] This a technology deals with the software platform for digital assets. Satoshi Nakamoto was the first who used BCT for bitcoin (crypto currency) in 2008 [3]. In BCT is a distributed data structure which replaces the centralized systems to over the problem of single point of failure [4]. In BC there is a concept of ledgers (can be a book, database, directory, file or other transactional record), [5]which are replicated to more than one user. This technology is based on the community validation to keep the ledgers' contents matched. It is the touchstone technology which made the standard change from trusting humans to trusting machines and shifted to decentralize from centralized control. It usually consists of consensus method for validation of sequential order of requests, transactions and information execution, modification, or creation. However, the correct transaction order is risky while establishing ownership because the correct order may cause privileges and responsibilities validation errors. BC uses one-way cryptographic hash function which makes this technology forge proof where records are maintained as irreversible and non-reputable replicated ledgers. BC provides security, anonymity and data integrity.

There are three main types of pf BC: 1. Public BC (everyone can participate in consensus process and can also check and verify the transaction such as Bitcoin and Ether um), 2. Private BC (only known and trusted node, that has restricted authority on data access can participate. All nodes are restricted, this type of BC is useful between the companies that have same legal mother entity), and 3. Consortium BC (in this type of BC, the data can be open or private and can be seen as partly decentralized. Usually has partnership like business to business, every node has an authority to choose in advance such as Hyperledger).[6-9] Some BC types are permissioned (contain semi-trusted members, all participating nodes are verified and registered in the BC network) while others are permission-less (it is publicly available, participating nodes are anonymous and un-trusted. Consensus is achieved by solving hard cryptographic puzzles (Pow), which is computationally intensive and cause a Sybil attack (a node in a network claim multiple identities [1] [10].

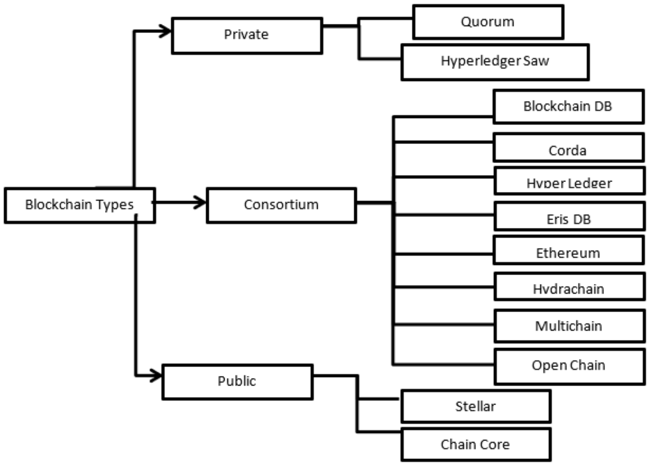


Figure 1: Blockchain platform types

BC is decentralized (no need of trusted-third party), transparent (data is recorded by every node in BC), open-source (people can create their own applications), autonomy (anyone can transfer and update data safely), immutable (once the data is written it cannot be changed, unless someone gets 51% control on the node), anonymity (only person's BC address is needed, its real identity is kept anonymous) [11].Table 1 presents different Blockchain platforms and compares these on the basis of different parameters.

Table 1: Comparison of Different BC Types w.r.t Different BC Platforms

Blockchain Platforms (Distributed Ledger System)	Consensus Process				Platforms		
	Public	Private	Permissioned	Permission-Less	Open-Source	Paid	Free
Big Chain DB[12-15]	✓	✓	✓	✓	✓	✓	✓
Chain Core [12, 16-18]	✓	×	Works on only those roles which are permitted to it for operating, accessing and participating in a network	×	✓	Developer	Customer
Corda R3 [12, 19-21]		✓	✓	×	✓	✓	✓
Credits[12, 22, 23]		✓			✓		?
Domus Tower Blockchain [12, 24]	?	?	✓	✓	?		?
Element Blockchain Platform[12, 18, 25]		?	?	?	×	×	✓
Eris: DB[12, 26, 27]		✓	✓	×	✓	✓	✓
Ethereum[12, 18, 28, 29]		✓	✓	✓	✓	×	✓
Hydra Chain[12, 30-35]		✓	✓	✓	✓	✓	✓
Hyer Ledger Fabric[12, 18, 20, 36-38]		✓	✓	✓	✓		✓
Hyperledger Iroha[12]		?	?	?	?	?	?
Hyperledger Sawtooth Lake [12, 37]	×	✓	×	✓	✓	×	✓
Multichain[12, 18, 34, 35]	✓	✓	✓	×	✓	✓	✓
Open chain[12, 18, 34, 35]	✓	✓	✓	×	✓		
Quorum[12, 39-41]	×	✓	✓	×	✓	×	✓
Stellar[12, 39, 42]	✓	×	?	?	✓	×	✓
Symbiont Assembly [12, 43]	✓	✓	✓	✓	✓	✓	✓

2. WORKING METHODOLOGY OF BC

A typical structure of BC consists of n blocks, each block in the chain carries a list of a transactions (the data in the BC depends on the type of the BC), hash of the block (once the block is created its hash is been calculated, which in helpful in detecting the change in the block), and a hash to the previous block (effectively makes the chain of blocks, this makes the BC so secure).The exception to this is the first block of the chain , called genesis, which is common to all clients in a BC network and has no parent [7]. The first block has no hash of the previous block, somehow if the attacker gets the first block it will calculates the hashes of the subsequent blocks. To mitigate this, there is a mechanism called PoW (Proof-of-Work) in the BC, which slows down the creation of new blocks (e.g; in case of bitcoin, it takes 10mins to calculate the required PoW and add a new block to the chain). This mechanism makes it very hard to tamper with the blocks, because if you temper with one block, you need to calculate the PoW of all the following blocks[44]. It combined multi-field infrastructure construction that contains multiple concepts such as: Cryptography (the use of asymmetric cryptography brings authentication, integrity, and nonrepudiation into the network), Mathematics, Algorithms and Economic Model. It uses distributed consensus algorithm solve the problem of traditional distributed databases by combining peer-to-peer networks [45]. Once the data is written in the BC it cannot be changed without being the change detected or rejected by the other nodes in the network[10]. BC in public, everyone is allowed to join the network. When someone joins this network, he gets the full copy of the BC. The nodes can use this to verify everything is still in order. Users interact with the BC via a pair of private/public keys [46].They use their private key to sign their own transactions, and they are addressable on the network via their public key. Every signed transaction is broadcasted by a user's node to its one-hop peers [8]. The intermediate peers assure the received transaction is valid before broadcasting it over whole the network, the invalid transactions are rejected by the peers.[46, 47]. In order to successfully tamper with the BC, the attacker needs to tamper with all blocks of the chain, redo the PoW for each block and take control of 50% of the peer-to-peer network. Only than the attacker will accept by all other nodes in the network, so this is practically impossible to do. BC are also constantly evolving, one of the recent development is the creation of smart contracts (simple programs that are stored on the BC)[46]. It is based on automatically exchange of coins under certain conditions.

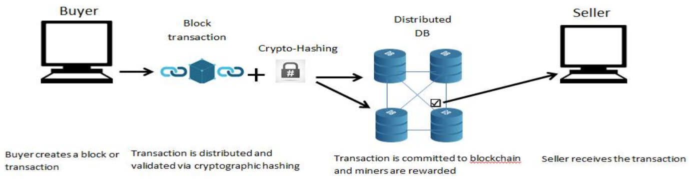

Buyer
Block transaction
Crypto-Hashing
Distributed DB
Seller
Buyer creates a block or transaction
Transaction is distributed and validated via cryptographic hashing
Transaction is committed to blockchain and miners are rewarded
Seller receives the transaction

Figure 2: Basic Working of BC

Application Areas General Discussion

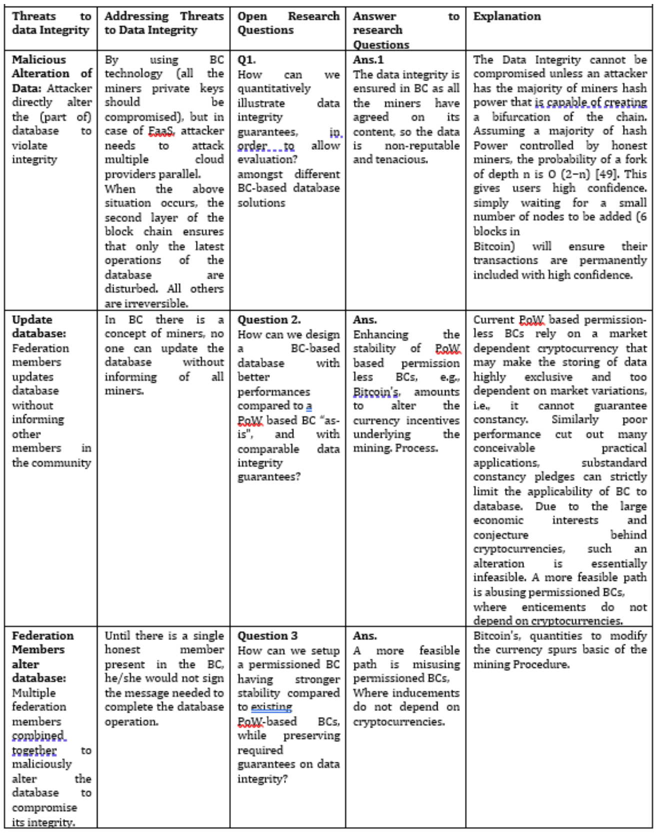
As BC has evolving nature, it is used in almost all fields to provide data security. There is no doubt that BC is a hot cake in recent years. The government should make analogous regulations for this technology, organizations should be ready to grasp BCTs, averting it brings too much influence to recent systems. The BCT has the possibility to renovate banking structure, speed reimbursements, and modernize stock exchanges while providing the transparency needed in this modern era of high-tech if we can secure this technology more [8]. Recent research endeavors have applied BC in Cryptocurrencies, Cloud distributed environments, e-health, Finance Smart Contracts and even in Databases. Most business units prefer cloud to deal, manage, store, control and secure their data. Once the data is in the cloud the owner does not have control over it. And this may lead to compromise the confidentiality, Integrity and Availability of data (CIA). The BCT is more suitable to provide CIA in Cloud Environment, big data authentication, IoTs, Digital identities, Finance, Business Industries, Health.

I. Cloud Environment

The authors have proposed the BC implementation of Big Data in Cloud Environments. They focus on the privacy (data integrity) and security in cloud environment rather than confidentiality. Because once the data is lost, there is no other way to get the original data back. Commonly there are two ways to protect data integrity in cloud environment:

1. Cryptographic Tools (digests, asymmetric keys), and **2. Data Replication Strategies**. Cryptographic Tools are meant to sign single pieces of data, so the attacker can easily be detected by signature validation. If the attacker somehow gets the secret keys, he/she may be able to launch an attack, which is practically undetectable. In order to ensure data integrity there is a need to implement some data replication strategies. The data replication strategies are already in the cloud environment but what if the cloud provider behaves maliciously, so never trust the cloud blindly. The authors implement BCT in order to remove trusted third party in the cloud, which will be empowered user control, durability and reliability of an authentication protocol. The main focus of the paper is on scenarios related to SUNFISH project about secure-by-design cloud federation, what are the threats to data integrity and how to address those threats using BCT.[48].

Table 2: Threats to Data Integrity in Cloud Computing and mitigate those Threats by implementing BCT.



Threats to data Integrity	**Addressing Threats to Data Integrity**	**Open Research Questions**	**Answer to research Questions**	**Explanation**
Malicious Alteration of Data: Attacker directly alter the (part of) database to violate integrity	By using BC technology (all the miners private keys should be compromised), but in case of FaaS, attacker needs to attack multiple cloud providers parallel. When the above situation occurs, the second layer of the block chain ensures that only the latest operations of the database are disturbed. All others are irreversible.	**Q1.** How can we quantitatively illustrate data integrity guarantees, in order to allow evaluation? amongst different BC-based database solutions	**Ans.1** The data integrity is ensured in BC as all the miners have agreed on its content, so the data is non-reputable and tenacious.	The Data Integrity cannot be compromised unless an attacker has the majority of miners hash power that is capable of creating a bifurcation of the chain. Assuming a majority of hash Power controlled by honest miners, the probability of a fork of depth n is O (2−n) [49]. This gives users high confidence. simply waiting for a small number of nodes to be added (6 blocks in Bitcoin) will ensure their transactions are permanently included with high confidence.
Update database: Federation members updates database without informing other members in the community	In BC there is a concept of miners, no one can update the database without informing of all miners.	**Question 2.** How can we design a BC-based database with better performances compared to a PoW based BC "as-is", and with comparable data integrity guarantees?	**Ans.** Enhancing the stability of PoW based permission less BCs, e.g., Bitcoin's, amounts to alter the currency incentives underlying the mining. Process.	Current PoW based permission-less BCs rely on a market dependent cryptocurrency that may make the storing of data highly exclusive and too dependent on market variations, i.e., it cannot guarantee constancy. Similarly poor performance cut out many conceivable practical applications, substandard constancy pledges can strictly limit the applicability of BC to database. Due to the large economic interests and conjecture behind cryptocurrencies, such an alteration is essentially infeasible. A more feasible path is abusing permissioned BCs, where enticements do not depend on cryptocurrencies.
Federation Members alter database: Multiple federation members combined together to maliciously alter the database to compromise its integrity.	Until there is a single honest member present in the BC, he/she would not sign the message needed to complete the database operation.	**Question 3** How can we setup a permissioned BC having stronger stability compared to existing PoW-based BCs, while preserving required guarantees on data integrity?	**Ans.** A more feasible path is misusing permissioned BCs, Where inducements do not depend on cryptocurrencies.	Bitcoin's, quantities to modify the currency spurs basic of the mining Procedure.

II. Big Data Authentication

Security Issues of Big Data Authentication	Requirements of Big Data Authentication
Password-Based Authentication: In the initial communication phase, the session key is derived from user's password in order to encrypt data to the KDC (Key Distribution Center). e.g; some breach occurs due to mishandle clients and all other passwords in the affected database are encrypted with the same key.	**Decentralized Authentication:** Replaces the username/password generated keys and the client-side SSL certificate with ECC (Elliptic Curve cryptography) generated keys, the same method is used in BC protocol. In this mechanism the user's private key is not exposed over the network and the user password is only used in the user's machine to access private key. This identification protocol is based on certain identification process using digital signature based on public keys. The user is authenticated when the transaction is only verified by appropriate private key.
Replay Attacks: In Kerberos there is a mechanism to detect replay attack, the authenticator embedded in Kerberos sends some extra data (encrypted IP, timestamp and ticket lifetime). IF the timestamp is same as the earlier packets timestamp than packet is rejected but here is no protocol that handles the case when same authenticator is used in parallel sessions.	**Password less and Anonymous Authentication:** Although there are some ways (biometric, PKI, QR-Codes etc) other than password are used for authentication. The BC proposed an authentication mechanism which is similar to the authentication mechanism used in Bitcoin (SIN).
Brute-Force Attacks: This attack targets the encrypted (using key based on user's password) timestamp (embedded in Kerberos pre-authentication data). There is no way to protect against this attack (using Windows smartcard logon with Kerberos extension or encrypt the network traffic between the client and KDC using IP security (IPsec)).	**No Session Keys:** Instead on session key, the BC uses SIN (advantage of using SIN is portability) is openly shared to everyone in the network and the private key is kept secret on the client-side. During the authentication process, the users are authenticated to the server by validating their digital signature against the user-shared public key and SIN. To prevent from attack replay signed nonce is greater than SIN's previous nonce. Same SIN is used is multiple devices without exposing users' credentials.
Keys Exposure: In Kerberos system if one key is compromised than anything i.e encrypted with that key cannot be trusted anymore. But in Kerberos version 5 there is a concept of perfect forward secrecy enables use of Cryptography key exchange using Diffie-Hellman. But there is no security against Logjam (attack against Diffie-Hellman key exchange protocol) used in	**Zero Single Point of the Failure System:** Every BC server which is used for mining purposes has a copy of BC data which is cryptographically trusted. Instead of securing form single point of failure the BC also reduce the chances of phishing (by the use of tampered-proof digital identity) and DoS attacks**.**

TLS protocol. This attack allows the attacker to read or modify the data passed over the connection.	
Single Point of Failure: When the KDC is compromised, the attacker gets the root access to the database of encrypted password.	**Prevent Data Theft:** In order to secure highly sensitive data like financial data (bank accounts, credit cards, bank balance and etc) Petland (Professor in MIT) has used BC to build Enigma (peer-to-peer network). Enigma enables different/ multiple parties to mutually store and run computation on data, while keeping the data private. The mean idea is to implement the Enigma infrastructure is to provide privacy, security and freedom for conveying data.
Time Synchronization: It is critical to have synchronous clock with Kerberos server to prevent replay attack. NTP (Network Time Protocol) exposed to attacker to launch DoS attack. Other attacks like DNS hijacking and MITM also deployed on NTP due to lack of encryption such as SSL and no authentication.	**Unbreakable Record:** It is impossible to alter or modify the data once it is written into the blockchain by using the principle of "hash and block". The consensus is accomplished by POW protocol (is a piece of data that is difficult to produce but easy to verify by others) in the mining process.
Denial-of-Service (DoS) Attacks: If the intruder somehow gets the user's master key. He/She may be able to launch a dictionary attack by repeatedly attempting to decrypt message which is encrypted by a key derived from user's password.	
Unsalable Protection: The security of the system depends on Identity Management System, to act as a server. So, there is no need for to manage, secure and coordinate individual databases on both client and generic server side. The solution in Kerberos initial TGT and cross-realm authentication based on Public-key Cryptography. But there is no security guarantee in some cases where attacker compromises, he hosts or non-expired ticket which remains the host's cache memory.	
Certificate Authorities: If the CA is compromised, the services are unavailable to clients and second the CA has users signing keys, those would allow the CA to impersonate key owner.	

In [48] the table shows some security issues of big data and the requirements of big data authentication by implementing BCT.

III. IoTs

[50] Presents the IoT ecosystem bank on centralized server-client model. A cloud server is used to identify and authenticate all the devices which are connected together through internet. However, this paradigm will fail for larger IoT ecosystem in future. The decentralized paradigm development was thought to be survived the challenges, but still there left some issues to be addressed like privacy and security in massive IoT peer to peer network. To track billions of connected devices, processing transactions and coordinating devices the BC might become the integral part and standard element.

The Current IoT is not fully automated as all the actions rules and commands are set by the user. The actual achievement might happen if BC control all the devices instead of direct user control. This can be achieved by using smart contracts. Smart contracts are actually sets of terms and conditions that must be agreed upon by both parties before the transaction takes place using BC. Implementing smart contracts is made possible by Ethereum which is a podium for creating BC systems. Ethereum has its own network, nodes and miners, just like Bitcoin. But the Ethereum nodes are proficient to achieve every type of contract that comes to them. The first ever application of IoT BC using Ethereum podium is Slock.it. These Slocks are tangible objects that can be controlled by BC. Now anyone can sell, share or rent anything using Slock.it without any middleman.

IV. Digital Identity

Digital identity is somehow similar to personal identity but adopted in cyberspace by an organization, person or a device. Unlike in real world a user may have more than one identity over the internet as per application requirements [1]. Generation of huge amount of data makes two problems for Cloud Service Provider (CSP): **1. Privacy of user owned data**, and **2. Multiple- identity Management**. BC has been implemented to solve such problems[51]. Although there is a centralized way to proof identities, CSP verify each identity by its passwords, user credentials. The blockchain can offer this approach by decentralizing the ownership of credential and offering a universally available protocol for verifying one's record in an immutable chain of data. This data rather than being store on per app basis is stored in a shared ledger. This shared ledger is downloaded by each individual user of BC and is a record of every transaction ever made. The main element of BC is its BC id, which is used to authenticate each user that he/she claim to be. This is publically available has no sensitive data stores in a plain format. A generic authentication flow that has been tested and utilized by companies such as Block Stack relies on a BC handshake. Security is achieved by Proof-of-Work (PoW)[1].

The transparent and decentralized nature of the BC network enables the development of a non-refutable and unbreakable record of data, which is the fundamental feature to many applications, such as identity management. I/O Digital provide the technology for businesses to have their own interoperable private BC / sidechain and the possibilities to store data in the BC for smart contracts, identity management, messaging and more After testing, I/O Digital decided to move forward with a more advanced system, the Decentralized I/O Name Server. Key features of the DIONS will include transferring aliases from user to user, storing identities on the BC and an encrypted messaging system. DIONS will utilize the I/O Digital blockchain to attach sensitive identity credentials to a specific Bitcoin or I/O Coin address. They are currently developing an open API for every developer to use and it will be available soon. [52]. There is another a novel approach of building a decentralized transparent immutable secure personal archive management and service system based on the concept of Proof-of-X (proof of identity, proof of property ownership, proof of specific transaction, proof of college degree, proof of medical records, proof of academic achievements, etc). Personal Archive Service System (PASS) is to use BCT to exploit its desirable features such as immutable, transparency, anonymous and public consensus. The subjects control its own PDAs and makes decision to whom to release. Figure 1 illustrates the general infrastructure and architecture view of a PASS under BC. The subject, represented by icon has its own repository or wallet that aggregates all its relevant PDAs. The certifiers issue certificates to its owners as well as to a trusted network. It does such certificates once for everyone involved and should not be bothered anymore. There is no need to have a third party or an inquisitor. They also pass the certificates to a consortium-oriented block chain network that the trust is developed in a delegated proof of stake. A client makes a request to the subject and gain access to those granted PDAs[53].

A new technology which is similar to machine learning is Ascribe. SPOOL (Secure Public Online Ownership Ledger) is a proprietary protocol of Ascribe for the application of BC. All the transactions relating to ownership are documented by this protocol as this protocol was specially designed for this task. By using this technique, the whole internet being searched by performing the resemblance match contrary to the author's content. After performing this check, the system creates bi-directional links if copies are matched. So BC idea of selling and storing proprietorship of digital data will be best presented by an analogy of sending an e-mail with a sign that authenticate the selling of content. The intricacy of legal licensing and ownership processes is coped up with just accepting the terms of service. To resolve a dispute of proprietorship the Time-Stamping is useful to present in the court[50].

V. Financial System

Public and private Keys are used in this technology for the rights on the data and authorization of data transactions without the need of human intervention or reliance providers, verification or negotiation [54]. A group of sovereign organizations have the privilege to work with common data sources, automatically reconciling among all contributors. The author proposes a precise model to develop Mixed-Integer Nonlinear Programming (MINLP) optimization problems for computing best Proof of Work configuration constraints that trade off hypothetically differing features such as availability, resiliency, security, and cost in this governed setting. A wide range of applications improve the welfare of goods and inheritance of financial services [55]. Their custom instance was one of the monetary progressions that generate economic substances. In the aforesaid methodology, owners of a BC system can stipulate permissible ranges for the size of the shared nonce space, the anticipated level of difficulty, and the number of miners used; and they can add mathematical constraints that specify requirements on availability, security, resiliency, and cost suppression.

The Authors did not use Hash technology and BFT Technology because they both are manipulated easily, therefore they use BC based on cryptographic puzzle which are much more resilient. A transaction is considered to be unreliable or inacceptable if its location value is Null or its hash does not identical to the one stored outwardly. Here they defined two very important things out of which one is K which is a suitable constant and its value is equal to or greater than 0. And Block Height signifies the number of blocks added to the BC. Therefore, a transaction is considered to be a reliable or valid if 0 is less than or equal to location and location + K is less than current Block Height. To ensure the resiliency of trustworthiness, the value of K can also be considered as a function of how fast blocks are added to the chain. The auditor's job is to do inspection of any transaction by having a critical examination of its triple stored. So if he finds the location value equal to Null or location + K is greater than Current Block Height then he affirms the transaction neither legal nor reliable. [56] The block chain model has many advantages, but privacy is not one of them. Amount transactions flow of money is all exposed and visible. To solve this issue of privacy, Hawk is represented which avoids storage of financial transactions in block chain.

A HAWK compiler avoids the need of applying cryptography but itself is responsible for a cryptographic protocol between the block chain and the users. The HAWK framework is composed of two portions: 1. O/PRIVATE is concerned with private information and distribution of payments. 2. O/PUBLIC has nothing to do with private data and money exchange.

VI. Health

The BCT has been implemented in other vast database areas such as e-health [57].Patient's health care data is highly sensitive and often distributed across multiple healthcare institutes/hospitals. Sometime patient needs to share its data, during treatment or for research purposes. Block chain technology based on permission-based approach (sharing ledger), enables the patient to distribute his/her data in the peer network. Everyone (doctors, hospitals, insurance companies, pharmacies) in the network can access the patient's data that he/she gives permission to access. By using shared distributed ledger will provide traceability, data security, patient data privacy and as well as the transparency of the data aggregation process.

In [57] Using block chain technology the authors proposed a secure and transparent framework for health care data management for EMR for managing and sharing Oncology Patient record using permissioned based approach, which provide better privacy protection, ensure availability of the data and do not involves transaction fees and mining.. They get the data from ARIA which provide oncology specific information system and image management. ARIA combines radiation, medical and surgical oncology information and can assist clinicians to manage different kinds of medical data, develop oncology-specific care plans, and monitor radiation dose received by patients.

To develop the prototype of the proposed framework the author used Hyper ledger Fabric (open-source implementation of the block chain). The architecture consists of user interface and backend (consists of three components): 1. Membership Service, 2. Certification authority, 3. Network of nodes (deployed in hospital and connected to database), 4. Load Balancer (to redirect the patient to any other trusted node in the network if one node is not present) and, 5. Separate Cloud-Based storage (for patient data and certificates).

1. A membership service is used to register a patient in the system, creates a public/private key pair using AES.
2. After receiving the certificate from the certification authority, the patient is able to login and create his record.
3. To the extent of access control policies, the patient submits a transaction that mention which doctor is able to access which kind of patient's data in the specified time period.
4. After encrypting the data with patient's secret key, he is able to upload the encrypted data into cloud repository.
5. Calculate the hash of the encrypted data to ensure data integrity.
6. The metadata like Hash of the file, file URL, and patient's ID contained in the transaction that will be stored on a block chain that uploaded the file.
7. Using certificate of the doctor the patient key is shared in order to access patient's data.

The same mechanism is used to register doctor in a system. Likewise, the doctors are able to upload and the patient's data. The doctor only accesses those data which is based on patients permissions specified in the transaction. In [50] Tal Rapke visionary approaches deliberate that people own and access their health and life records. Block chain provides a way to implement this consumer centered approach to the health sector. By implementing the block chain technology, Government and other Healthcare centers will be free to protect patient's data. Only those can see the patient's data whom he/she wish to share with. Another scenario by Gupta et al. proposed is to store only metadata (patient's id, visit Id, provider ID, and payer id) about health and events on the BC and the actual data is stored in somewhere in a health cloud. Another research says that there is no need to store all the data on a BC. The transaction in the blockchain contains (user id, encrypted health link, timestamp when transaction was created, and the type of stored data). The actual data is stored in a cloud pool and does not have any privacy issue because data is encrypted and digitally signed to ensure authenticity and privacy of the information. To store data in cloud it will be the base for querying, mining analysis and machine learning.

There is another way to store medical record in to the BC is by utilizing Ethereum's smart contract. The proposed solution is MedRec builds the big data in three types of contracts: 1. Registrar Contract (it stores all the essential detail and public keys of participants), only for certified institutions, 2. Patient-Provider Relationship Contract (issued when one node manage or store other node), and 3. Summary Contract (help patient to locate his/her medical history).

All of the above solutions enable user to discover and manage their own record but there is need for global standard to store, share, and access encrypted data on cloud.

VII. Business Industry (Product Centric)

[58] Product centric approach was invented to achieve standardization and flow of information regarding the subject being taken under consideration which is to avoid fragmentation of data to different organizations over the product life cycle but to share complete form, between organizations. But it has its cons when considering lack of digital trust and multi version con-currency control. Also, when data is shared among organizations it might get edited or corrupted. To avoid this from happening, the authors used BCT. Before a shared platform for product data management, it was difficult to perform access, update and distribution among supply chain parties. For this purpose, there is a need for the creation of product centric information management and its respective architectures.

Control Mechanism in Consumer Centric Industrial Supply Chain Platform has led to restructuring of current demand and supply network structure which transferred control of data from consumers/companies to platform companies. A new control mechanism /coordination was introduced in consumer centric industrial.

Supply chain called two sided platforms and multi-sided platforms. Two-sided market is indirect approach having mediator role in interaction between end users through mediator's pipeline by charging by both parties. On the other hand, multi-sided markets provide direct flow of information avoiding the need to go through the choke point pipeline of the mediator.

There is a lack of symmetry and flexibility between the parties who exchange particular bit of data. Each party wants company specific information system which requires tailoring if not reprogramming before they can be put in good use.

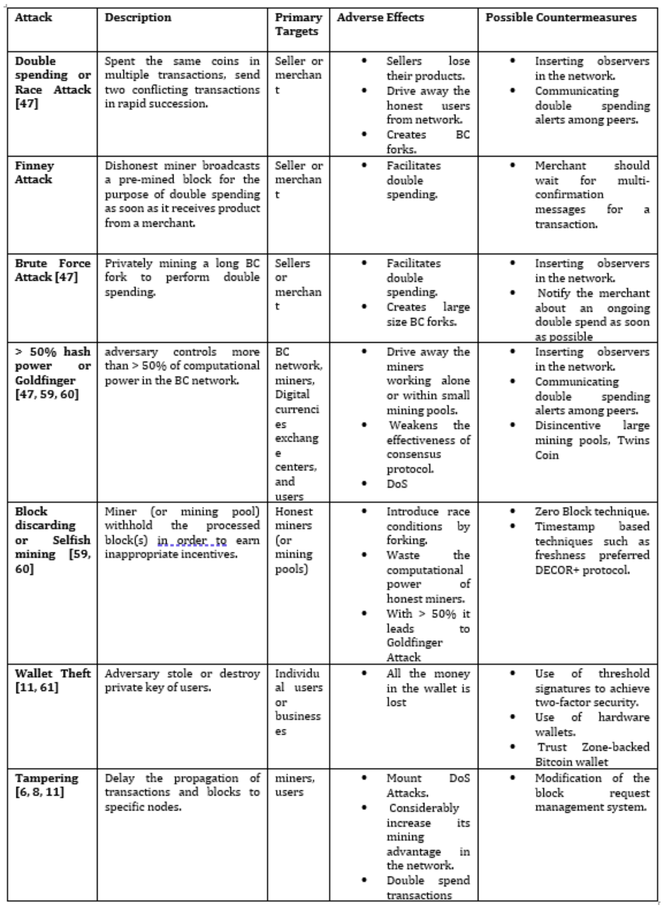
Due to lack of synchronization in product data it becomes obsolete or some time inaccurate. To solve these issues product centric approach was introduced which led to product individual called agent distributed between organizations and available in multisystem. Weather to choose individual platform and shared platform architecture depends on its users but in a wider context shared platform at the following pros over individual platform:

Interoperability and Updating of such platforms become time consuming and requires the software which is difficult to find in the first place. Secondly any kind of manipulative strategy by a company can affect overall security of the platform. Another thing is whether it should be centralized or decentralized platforms.

Security Issues and Challenges However, the BC provides security, anonymity, integrity and etc. Instead of these benefits the BCT faces some challenges such as; due to its decentralized nature it is difficult to find out the faulty node BCT also leads to some attack cases like Double Spending Attack, 51% Attack, Brute Force Attack, Finny Attack and etc

[11]. In the below table, we discuss some of the possible attack cases, what these attack means, their primary target, adverse effect and some possible counter measures to mitigate against these attacks.

TABLE 3: POSSIBLE ATTACK CASES, THEIR EFFECT AND COUNTERMEASURES.



Attack	Description	Primary Targets	Adverse Effects	Possible Countermeasures
Double spending or Race Attack [47]	Spent the same coins in multiple transactions, send two conflicting transactions in rapid succession.	Seller or merchant	• Sellers lose their products. • Drive away the honest users from network. • Creates BC forks.	• Inserting observers in the network. • Communicating double spending alerts among peers.
Finney Attack	Dishonest miner broadcasts a pre-mined block for the purpose of double spending as soon as it receives product from a merchant.	Seller or merchant	• Facilitates double spending.	• Merchant should wait for multi-confirmation messages for a transaction.
Brute Force Attack [47]	Privately mining a long BC fork to perform double spending.	Sellers or merchant	• Facilitates double spending. • Creates large size BC forks.	• Inserting observers in the network. • Notify the merchant about an ongoing double spend as soon as possible
> 50% hash power or Goldfinger [47, 59, 60]	adversary controls more than > 50% of computational power in the BC network.	BC network, miners, Digital currencies exchange centers, and users	• Drive away the miners working alone or within small mining pools. • Weakens the effectiveness of consensus protocol. • DoS	• Inserting observers in the network. • Communicating double spending alerts among peers. • Disincentive large mining pools, Twins Coin
Block discarding or Selfish mining [59, 60]	Miner (or mining pool) withhold the processed block(s) in order to earn inappropriate incentives.	Honest miners (or mining pools)	• Introduce race conditions by forking. • Waste the computational power of honest miners. • With > 50% it leads to Goldfinger Attack	• Zero Block technique. • Timestamp based techniques such as freshness preferred DECOR+ protocol.
Wallet Theft [11, 61]	Adversary stole or destroy private key of users.	Individual users or businesses	• All the money in the wallet is lost	• Use of threshold signatures to achieve two-factor security. • Use of hardware wallets. • Trust Zone-backed Bitcoin wallet
Tampering [6, 8, 11]	Delay the propagation of transactions and blocks to specific nodes.	miners, users	• Mount DoS Attacks. • Considerably increase its mining advantage in the network. • Double spend transactions	• Modification of the block request management system.

3. CONCLUSION

BCT works like a user opinion database in which every participant can add up according to their experience and nature of operations. The lack of leadership in data-controlled terms minimizes dictation and modification by a single entity, replacing by algorithmically incentivized procedures regarding one shared consensus view.

For sustaining both BCT and product centric data management following conditions and circumstances should be taken under consideration. That the data must be shared, data should be allowed to modify by parties, having agreement on the content to be shared within the database.

How much professional trust and interdependence exists in parties, a trustworthy and selected intermediator as well which is important as if even other conditions are already present.

The block chain model has many advantages, but the privacy is not one of them. Amount transactions flow of money is all exposed and visible. To solve this issue of privacy, Hawk is represented which avoids storage of financial transactions in block chain.

A HAWK compiler avoids the need of applying cryptography but itself is responsible for a cryptographic protocol between the block chain and the users. The HAWK framework is composed of two portions: 1. O/PRIVATE is concerned with private information and distribution of payments. 2. O/PUBLIC has nothing to do with private data and money exchange.

REFRENCES

1. Available: https://www.investopedia.com/terms/d/doublespending.asp
2. I. D. Rubasinghe and T. De, "Transaction Verification Model over Double Spending for Peer-to-Peer Digital Currency Transactions based on Blockchain Architecture," International Journal of Computer Applications, vol. 163, 2017.
3. J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review," PLoS ONE, vol. 11, p. e0163477, 10/0305/10/received09/09/accepted 2016.
4. J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review," PLoS ONE, vol. 11, p. e0163477, 10/0305/10/received09/09/accepted 2016.
5. G. R. Nair and S. Sebastian, "BlockChain Technology Centralised Ledger to Distributed Ledger," 2017.
6. M. Mainelli and M. Smith, "Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)," The Journal of Financial Perspectives, vol. 3, pp. 38-69, 2015.
7. J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in Security and Privacy (SP), 2015 IEEE Symposium on, 2015, pp. 104-121.
8. M. B. Taylor, "The Evolution of Bitcoin Hardware," Computer, vol. 50, pp. 58-66, 2017.
9. F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications Surveys & Tutorials, vol. 18, pp. 2084-2123, 2016.
10. L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on, 2017, pp. 1-5.
11. I.-C. Lin and T.-C. Liao, "A Survey of Blockchain Security Issues and Challenges," IJ Network Security, vol. 19, pp. 653-659, 2017.
12. R. Nagpal. (20 Dec). 17 blockchain platforms—a brief introduction. Available: https://www.bigchaindb.com/whitepaper/

13. (2016, 12 sDec). Usecase. Available: https://www.bigchaindb.com/usecases/
14. R. M. Trent McConaghy, Andreas M¨uller,, T. T. M. Dimitri De Jonghe, Greg McMullen,, S. B. Ryan Henderson, and a. A. Granzotto. (June 8, 2016, 20 Dec). BigchainDB: A Scalable Blockchain Database.
15. J. Omaar. (20 Dec). Forever Isn't Free: The Cost of Storage on a Blockchain Database. Available: https://medium.com/ipdb-blog/forever-isnt-free-the-cost-of-storage-on-a-blockchain-database-59003f63e01
16. (20 Dec). Chain Protocol Whitepaper. Available: https://chain.com/docs/1.2/protocol/papers/whitepaper#3-data-model
17. P. Sandner. (20 Dec). Comparison of Ethereum, Hyperledger Fabric and Corda. Available: https://medium.com/@philippsandner/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6
18. (2016, 20 Dec). The road ahead. Available: https://www.corda.net/2016/11/the-road-ahead/
19. (2016, 20 Dec). Data model. Available: https://docs.corda.net/releases/release-M7.0/data-model.html
20. (2016, Credits. Revision e917b4e8., 20 Dec). FAQ. Available: https://credits.readthedocs.io/en/latest/faq.html#is-credits-a-distributed-ledger-or-blockchain
21. (Version 1.6/25.10.2017, 20 Dec). Decentralized financial system CREDITS. Available: https://credits.com/Content/Docs/TechnicalPaperENG.pdf
22. R. Creighton. (20 Dec). Domus Tower Blockchain (DRAFT). Available: http://domustower.com/
23. A. Fowler. (Jul 13, 2017). Confidentiality Unlocks Blockchains for Businesses. Available: https://blockstream.com/2017/07/13/confidentiality-unlocks-blockchains-for-businesses.html
24. R. Dixit. Private Blockchain Platforms - Eris vs. Corda. Available: https://www.linkedin.com/pulse/private-blockchain-platforms-eris-vs-corda-rajeev-dixit/
25. (20 Dec). erisdb-js (Alpha). Available: https://www.npmjs.com/package/eris-db
26. A. Tomasicchio. (2017). The Best Blockchain Developer Tools. Available: https://blockgeeks.com/blockchain-developer-tools/
27. T. Swanson. (April 6, 2015). Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledgersystems. Available: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf
28. S. Purkayastha. (20 Dec). Eight Blockchain platforms for rapid prototyping. Available: http://radiostud.io/eight-blockchain-platforms-comparison/
29. A. Mohan. (Sep 22, 2016). Open source Blockchain platforms. Available: https://lightrains.com/blogs/opensource-blockchain-platforms
30. E. M. Jialin Li, Dan R. K. Ports. (28, 2017). Eris: Coordination-Free Consistent Transactions Using In-Network Concurrency Control. Available: https://syslab.cs.washington.edu/papers/eris-sosp17.pdf
31. HeikoHeiko. Permissioned Distributed Ledger based on Ethereum. Available: https://pypi.python.org/pypi/hydrachain/0.3.2
32. T. Sharma, "List Of Best Open Source Blockchain Platforms," 29 August, 2017
33. (2016, 20 Dec). plateforms to develop private blockchain [duplicate]. Available: https://ethereum.stackexchange.com/questions/8911/plateforms-to-develop-private-blockchain
34. P. Jayachandran. (May 31, 2017). The difference between public and private blockchain. Available: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/
35. (20 Dec). Docs » Types of Blockchain. Available: https://mastanbtc.github.io/blockchainnotes/blockchaintypes/
36. (20 Dec). Docs » Introduction. Available: https://hyperledger-fabric.readthedocs.io/en/release/blockchain.html#what-is-hyperledger-fabric
37. A. Albrecht, "An overview of the blockchain universe," December 27, 2016.
38. JPMorgan. (2017). Available: https://www.jpmorgan.com/country/US/EN/Quorum
39. M. d. Castillo. (Oct 16, 2017). IBM's Stellar Move: Tech Giant Uses Cryptocurrency in Cross-Border Payments. Available: https://www.coindesk.com/ibms-stellar-move-tech-giant-use-lumen-cryptocurrency-payments-rail/
40. E. Hofmann, U. M. Strewe, and N. Bosia, "Background III—What Is Blockchain Technology?," in Supply Chain Finance and Blockchain Technology, ed: Springer, 2018, pp. 35-49.
41. J. A. Garay, A. Kiayias, and N. Leonardos, "The Bitcoin Backbone Protocol: Analysis and Applications," in EUROCRYPT (2), 2015, pp. 281-310.
42. K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292-2303, 2016.
43. M. Conti, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," arXiv preprint arXiv:1706.00916, 2017.
44. N. Abdullah, A. Hakansson, and E. Moradian, "Blockchain based approach to enhance big data authentication in distributed environment," in Ubiquitous and Future Networks (ICUFN), 2017 Ninth International Conference on, 2017, pp. 887-892.
45. J. B. A. M. J. Clark, A. N. J. A. K. Edward, and W. Felten, "Research Perspectives and Challenges for Bitcoin and Cryptocurrencies."
46. E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in Smart Technologies, IEEE EUROCON 2017-17th International Conference on, 2017, pp. 763-768.

47. A. Bakre, N. Patil, and S. Gupta, "Implementing Decentralized Digital Identity using Blockchain," 2017.
48. O. Jacobovitz, "Blockchain for Identity Management," 2016.
49. Z. Chen and Y. Zhu, "Personal Archive Service System using Blockchain Technology: Case Study, Promising and Challenging," in AI & Mobile Services (AIMS), 2017 IEEE International Conference on, 2017, pp. 93-99.
50. T. Aste, P. Tasca, and T. Di Matteo, "Blockchain Technologies: The Foreseeable Impact on Society and Industry," Computer, vol. 50, pp. 18-28, 2017.
51. L.-N. Lundbæk, A. C. D'Iddio, and M. Huth, "Centrally Governed Blockchains: Optimizing Security, Cost, and Availability," in Models, Algorithms, Logics and Tools, ed: Springer, 2017, pp. 578-599.
52. A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in Security and Privacy (SP), 2016 IEEE Symposium on, 2016, pp. 839-858.
53. A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "How Blockchain Could Empower eHealth: An Application for Radiation Oncology," in VLDB Workshop on Data Management and Analytics for Medicine and Healthcare, 2017, pp. 3-6.
54. J. Mattila, T. Seppälä, and J. Holmström, "Product-centric information management: A case study of a shared platform with blockchain technology," in Industry Studies Association Conference, 2016.
55. R. Zhang and B. Preneel, "Publish or Perish: A Backward-Compatible Defense against Selfish Mining in Bitcoin," in Cryptographers' Track at the RSA Conference, 2017, pp. 277-292.
56. A. Chepurnoy, T. Duong, L. Fan, and H.-S. Zhou, "TwinsCoin: A Cryptocurrency via Proof-of-Work and Proof-of-Stake," IACR Cryptology ePrint Archive, vol. 2017, p. 232, 2017.
57. R. Gennaro, S. Goldfeder, and A. Narayanan, "Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security," in International Conference on Applied Cryptography and Network Security, 2016, pp. 156-174.
58. X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," Future Generation Computer Systems, 2017.
59. R. Kienzler. (Nov 24, 2016). Architecture of the Hyperledger Blockchain Fabric - Christian Cachin - IBM Research Zurich. Available: https://www.slideshare.net/ormium/architecture-of-the-hyperledger-blockchain-fabric-christian-cachin-ibm-researchzurich?qid=c9388f32-58e2-47f2-b4a8-f65bb786ab61&v=&b=&from_search=11
60. M. Conti, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," arXiv preprint arXiv:1706.00916, 2017.