Journal of Banking and Financial Technology (2019) 3:1–17
https://doi.org/10.1007/s42786-018-00002-6

ORIGINAL ARTICLE

A survey of blockchain from security perspective

Dipankar Dasgupta[1] · **John M. Shrein**[1] · **Kishor Datta Gupta**[1]

Published online: 3 January 2019

Abstract
The report starts with an overview of the blockchain security system and then highlights the specific security threats and summarizes them. We review with some comments and possible research direction. This survey, we examines the security issues of blockchain model related technologies and their applications. The blockchain is considered a still growing like the internet in 1990. It has the potential to disrupt so many technology areas in the future. But as a new underdeveloped field, it is suffering many setbacks mostly resulting from the security area. Its security concerns coming not only from distributed/decentralized computing issue or Cryptography algorithm issue, from some unexpected field too. Here, in this paper, we tried to classify the security concerns for the blockchain based on our survey from recent research papers. We also tried to show which way blockchain development trends are going.

Keywords Blockchain · Security · Applications · Vulnerability · Threats

1 Introduction

There is growing interest in all industrial sectors to use blockchain technology for their purposes (such as secure contracts, financial transactions, sharing health information, etc.) while it was originally developed to support cryptocurrencies such as Bitcoin. It is worth noting that Bitcoin is now treated as a stock in Wall Street and financial market while its purpose and real value is yet to materialize, and its future is not clear. It is agreeable that Blockchain is a computer algorithm to provide distributed communication in a peer-to-peer network of subscribers where the transactions are transparent among the parties involved. The fundamental questions need to be addressed in terms of Blockchain's security, privacy and limitations concerns also need to discussed. This paper offers a viewpoint of blockchain security concerns and present recent developments.

✉ Dipankar Dasgupta
dasgupta@memphis.edu

John M. Shrein
jmshrein@memphis.edu

Kishor Datta Gupta
kgupta1@memphis.edu

[1] The University of Memphis, Memphis, USA

1.1 Algorithm based security

Typically blockchains run on a decentralized, peer-to-peer network in which all entities adhere to the same protocols, preventing any single entity from controlling the underlying infrastructure. Ideally, this open, decentralized, permissionless architecture prevents any entity from exerting regulatory pressures or otherwise interfering with blockchain operations.

DSA is an asymmetric key cryptography system in which a private key is used to digitally sign messages and the corresponding public key may be used to verify those messages. The elliptic curve variant of DSA, ECDSA, is commonly used in blockchain implementations because it offers several advantages, such as reduced key size and faster computation than other discrete logarithm-based algorithms and factoring modulus algorithms. Elliptic curves are suitable for cryptographic operations are defined by specific domain parameters. A number of such curves, some standardized by NIST, IEEE, ANSI, and other groups, are available.

1.2 Hashing operations based security

Cryptographic hashes have several properties that turn out to be very useful to blockchain operations. Blockchains make extensive use of cryptographic hash functions to provide integrity, consistency, and enhanced security. A

well-designed hash function should support the hiding property, be resistant to collisions, and support puzzle friendliness. Given a hash output, the hiding property demands that it should be difficult to find the plaintext input. The property of collision resistance requires that is should be difficult to find any two plaintext inputs that produce the same hash output. Given a target hash set, the property of puzzle-friendliness demands that for any hash output, it should be difficult to find some hash input and nonce such that the output is in the target set. This property forms the basis of proof of work (PoW) type consensus mechanisms. Cryptographic hashing is vital to blockchain implementations because it provides the integrity required to ensure that the entire blockchain is immutable. Figure 1 illustrates the extensive use of hashing in the Bitcoin blockchain. In addition to the hashes uses in the Hashcash PoW algorithm and the hashing of the public key to represent addresses, blockchains use hashes in a variety of other ways. Every block stores a hash of the previous block. All transactions are hashed and represented in a Merkle tree, which is a binary tree in which each parent node is a hash of the concatenated hashes of its child nodes. The Merkle root hash value is stored in each block header, thus representing all transactions stored in a given block. Each transaction input references a previous transaction hash. If a weak or broken hash algorithm is used for any of these operations, the result could be disastrous.

2 Potential vulnerabilities in blockchain

Our literature review focuses several security concerns and other issues in Blockchain Implementation, we classify these in eight categories as described in flowchart at Fig. 2.

2.1 Vulnerability of cryptographic operations

Blockchain security depends on the strength and robustness of the cryptographic primitives used to conduct transactions and maintain a detailed history of past activity [1]. Cryptographic hashes are used in virtually all blockchain operations to maintain the integrity of the chain and all transactions. Digital signature algorithm (DSA), which is based on asymmetric key cryptography, and cryptographic hashing are the primary algorithms used in blockchain implementations. The specific algorithms is chosen by the application developers of blockchain technology.

2.1.1 Cryptographic key vulnerability

Many of these standardized elliptic curves either have theoretical weaknesses or were generated using questionable parameters. For example, the NIST P-256 curve is viewed skeptically by some cryptographers because derivation of the curve parameters are not well explained and allow for some possibility of manipulation such that the curve may contain intentional weaknesses or "backdoors". There is some precedence for this type of intentional weakness as NIST previously published a standard for a cryptographically secure random number generator based on elliptic curve operations called Dual_EC_DRBG. The backdoor was suspected even before the standard was published and it was later revealed in a Reuters article that RSA Security was paid $10 million to incorporate this algorithm as the default random number generator in the RSA BSAFE library, though RSA denies this allegation [43]. The backdoor allows someone that knows a secret set of numbers to break the encryption of any message given only 32 bits of ciphertext [53].

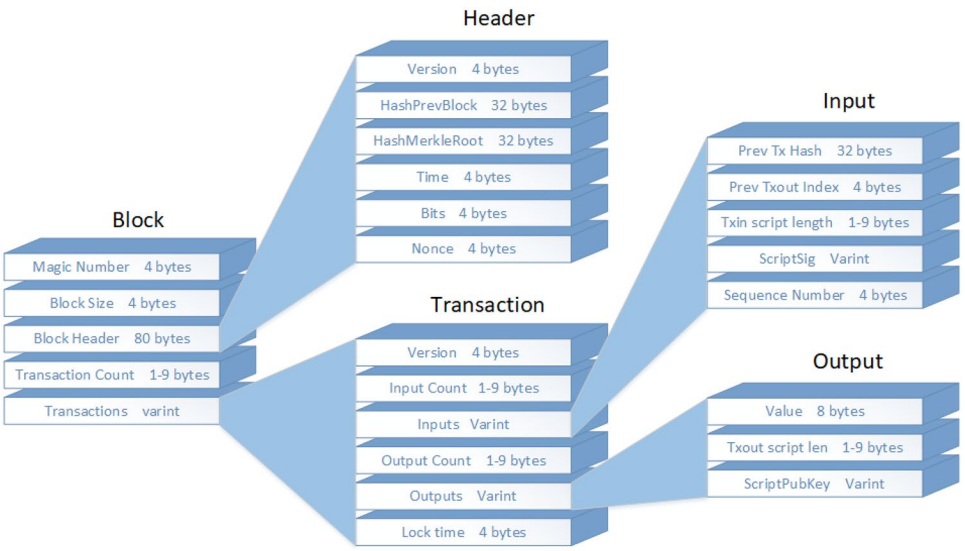

Fig. 1 Bitcoin block structure, showing several values that are represented by hash values

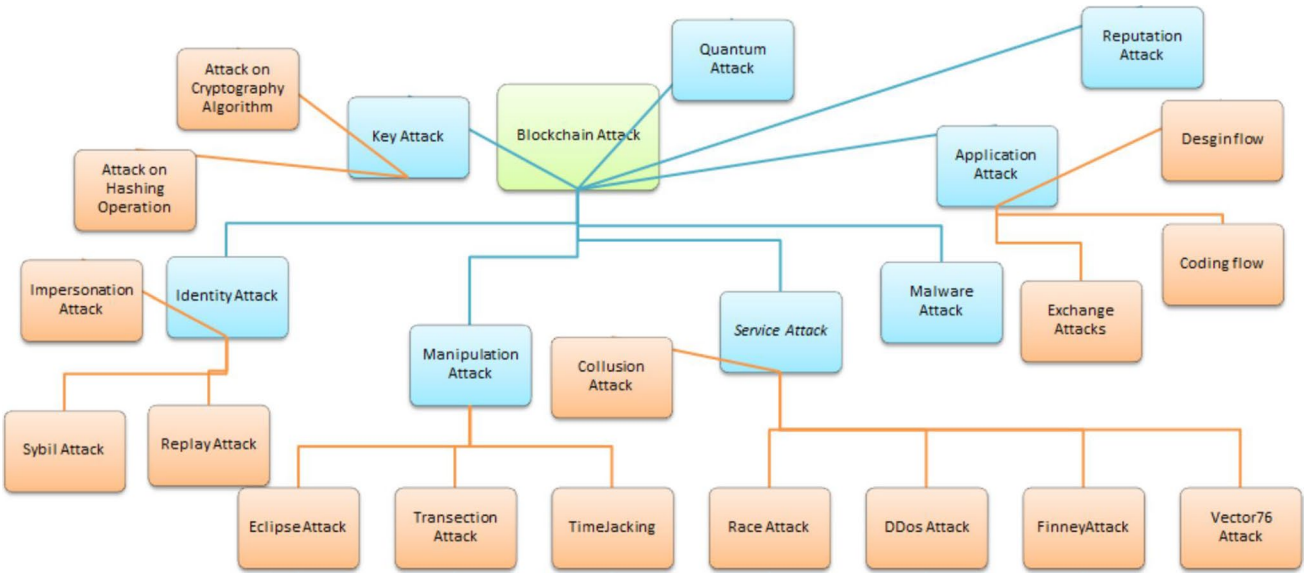

Fig. 2 Classification of Blockchain vulnerability

Some blockchains, such as Bitcoin and Ethereum for example, use the secp256k1 curve, which is a type of elliptic curve that allows efficient computation due to its non-random construction. Due to the parameters chosen for secp256k1, it is accepted as not having a backdoor due to exhaustive search for parameters that allow for intentional weaknesses. However, as detailed by Bernstein and Lange in [5], there are several deficiencies in secp256k1 that may lead to weaknesses. Other blockchain implementations have opted for Curve25519, which the chosen parameters are well explained and do not suffer from the limitations of other curves. in ECC ECC may also be susceptible to other types of attacks. It turns out that the operations used for addition and doubling under ECC differ enough in timing and power consumption such that it may be possible to carry out side-channel attacks examines in operation and associated with fault analysis, timing attacks, and power attacks [60]. Bernstein and Lange detail several additional factors that may lead to weaknesses in a variety of curves [5]. ECDSA, as well as other cryptographic algorithms, rely on a cryptographically secure random number generator because it may be possible to recover a private key given a public key that was generated with a poor random number generator. In 2013,it was recorded that Android Bitcoin wallets were vulnerable due to a flaw in a Java-based pseudo-random number generator [20].

2.1.2 Hashing operation vulnerability

SHA-256 is widely used in blockchain Hashing function operation and implementations, though other hashing algorithms such as Ripemd160 and sCrypt are also used. SHA-256 is currently assumed as unbreakable. however, it is susceptible to the length extension attack. Using this attack, a hash of a signed message can be modified by appending some attacker-controlled data to the original message without knowing the shared secret. Ferguson and Schneier suggest double SHA-256 as a way to prevent the length extension attack [54]. These hash functions are also susceptible to birthday attacks, which are probabilistic attack that breaks collision resistance by repeated evaluations. The real-world effectiveness of this type of attack was recently demonstrated for the SHA-1 algorithm [57]. Thus, algorithms like MD5 and SHA-1 are effectively broken and should never be used for any cryptographic operation.

2.2 Identity vulnerability

When adversary attack the blockchain network by trying to compromise blockchain users identity, it is referred as Identity attack. Some of these attack are described below

2.2.1 Replay attack

It is a form of attack where the attacker spoof the communication between two valid parties and gain the access. Stealing hashkey and reusing it to makes the attacker a valid user, which is common threat to blockchain community. However using key pair based exchange protocol is effective to protect user from these types of attack. Some blockchains using one-time private public key pair [11] to detect such replay attack while some [30] uses elliptic curve based encryption to have protection against it.

2.2.2 Impersonation attack

Impersonating a legitimate users are also used to gain access. Using an ECDSA algorithm can create defend against it also some other method [63] proposed to use distributed incentive based approach. BSeiN [11]on the Other hand used attribute based signature to validate users.

2.2.3 Sybil attack

These are general type of attack on peer-to-peer networks in which multiple fraudulent identities are created and controlled by a single rogue entity. In blockchain networks, this type of attack are used to isolate a target node from the rest of the honest network, which in turn are used to launch different types of attacks. For example, the attacker may refuse to relay transactions and blocks from the target node, conduct various forms of double spending attacks on the target by relaying only blocks that they create, filter specific transactions to conduct double spending in the case where the target accepts 0 confirmation transactions, or defeat anonymization protocols like Tor and JAP, in Fig. 3.

A blockchain framework called TrustChain [48] tackles this issue by creating using a immutable chain. This chain is product of interactions between each user which is temporally and ordered. Its computes a trustworthiness of an agents in an online community based on prior history. They used a system called "netflow" which makes sure that every user who is consuming resources are also sharing some resources back to the other nodes in the network.

2.3 Manipulation based attacks

Various types of routing attacks are possible where one or more nodes in a blockchain network may be partially or fully partitioned from the rest of the network for malicious purposes. Using such attacks, it may be possible to delay block propagation time for a significant amount of time, perform DoS attacks, isolate a large portion of the network mining power, and other attacks.Three types of attacks are most concerning includes Eclipse attack , Time jacking and Attack based on Transaction Malleability.

2.3.1 Eclipse attacks

Eclipse attacks are a type of attack in which an attacker attempts to isolate a target from the rest of the network by monopolizing all of the target's incoming and outgoing connections. This allows the attacker to corrupt the targets view of the blockchain, force it to waste compute power, or subvert the target's compute power for nefarious purposes [29]. In Fig. 4 Eclipse attack, where a Bitcoin node with 117 incoming TCP connections having maximum of eight outgoing TCP connections. These connections create gossip network which need for bitcoin block and transaction. The attack targets only the nodes that accept incoming connections [62].

2.3.2 Transaction malleability

Transaction malleability is a design flaw in Bitcoin for which transactions may be altered after being created but before being added to a block. The source and destination addresses and the transaction amount cannot be manipulated, but other portions of the transaction may be altered, which results in a transaction ID (TXID) that differs from the original. Mt. Gox, the once dominant but now defunct Bitcoin exchange managed transactions by TXID, but attackers were able to take advantage of this by submitting withdrawal requests, modifying the TXID, then claiming the withdrawal failed. Because Mt. Gox was unable to verify the status of the transaction due to the altered TXID, attackers were able to withdraw funds fraudulently. This was cited by Mt. Gox as one of the primary reasons for their bankruptcy, although research has surfaced to refute this claim [20].

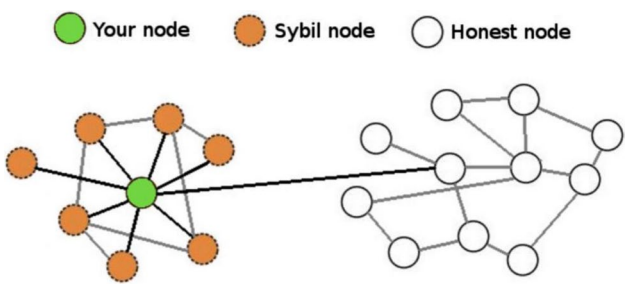

Fig. 3 Illustration of Sybil attack

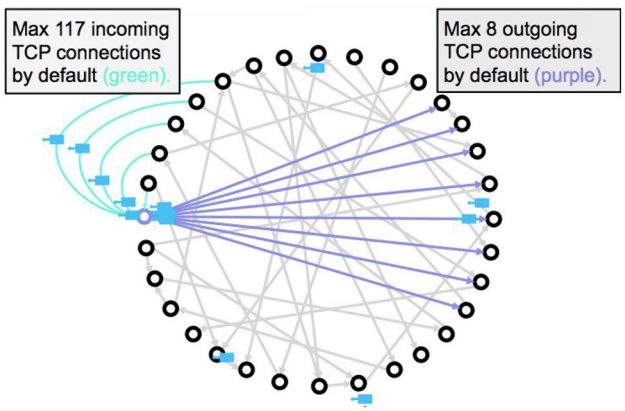

Fig. 4 Eclipse attack [62]

2.3.3 Timejacking

Timejacking is an attack that attempts to skew a target node's timestamp by connecting to a target with multiple peers and reporting an incorrect time to the target. A node uses the network time to validate new blocks. By skewing a node's view of the network time, it would reject new blocks with a timestamp greater than a predetermined duration. Like the Sybil and Eclipse attacks, this would allow the malicious nodes to virtually isolate the target node from the rest of the network. By isolating a target node, fraudulent transactions could be created and sent to the target. By continuing the attack, fraudulent confirmations could be sent to the target until the target accepts the transaction as confirmed. Even more advanced attacks could be conducted on multiple targets to speed up the clocks of the mining pool, thus increasing the difference in time between the mining pool and a target node.

Several countermeasures are already available to help mitigate many of these attacks. Network encryption randomized port negation when making new connections, UDP heartbeats to determine if messages are being intercepted, retrieval of block data from multiple nodes instead of a single node, increased diversity of node connections, round-trip time monitoring, and other methods could largely mitigate many of these attacks [42].

2.4 Quantum vulnerability

The most popular cryptographic algorithms have long been threatened by the looming era of quantum computing. ECC and ECDSA, being based the elliptic curve discrete logarithm problem (ECDLP), are among those algorithms threatened by the expectation of quantum computers in the near future. Quantum computers with a sufficient number of qubits and Toffoli gates using a modified version of Shor's algorithm will be able to break ECC. Figure 5 shows that it takes significantly fewer qubits and Toffoli gates to break ECC than RSA [12, 21]. New so-called post-quantum cryptographic algorithms based on supersingular elliptic curves, lattice-based constructions, multivariate polynomials, hash functions, and other methods are already being developed to address this issue, as are blockchain implementations, such as Quantum Resistant Ledger, that seek to avoid this weakness. Interestingly, wallet addresses in Bitcoin and other cryptocurrencies are not actually public keys, rather they are hashes of the public keys, meaning that public keys are not known simply because addresses are public. While hashes are not entirely quantum resistant, they do fare much better than ECC and RSA.Using Grover's algorithm, preimage resistance for hash algorithms like SHA-256 are breakable in $O(\sqrt{N})$ evaluations, where N is the size of the function domain. For SHA-256, this would result in 2^{128} evaluations instead of 2^{256}, which is still considered computationally difficult [26, 27]. Even by leveraging the birthday attack, SHA-256 collision resistance can still only be broken in 2^{85} operations.

2.5 Reputation based attack

A user in block chain can change his reputation from negative to a positive one and can fool the framework. Tempering the user reputation is another big concern for the block chain community.It can be done mainly two way one is hiding the negative transaction and another is creating a new account. There is no mentionable approach against this concern yet to seem, only Trustcoin [48] made some proposals which is also more detection based than prevention based.

ECDLP in $E(\mathbb{F}_p)$ simulation results					Factoring of RSA modulus N interpolation from [21]		
$\lceil \log_2(p) \rceil$ bits	#Qubits	#Toffoli gates	Toffoli depth	Sim time sec	$\lceil \log_2(N) \rceil$ bits	#Qubits	#Toffoli gates
110	1014	$9.44 \cdot 10^9$	$8.66 \cdot 10^9$	273	512	1026	$6.41 \cdot 10^{10}$
160	1466	$2.97 \cdot 10^{10}$	$2.73 \cdot 10^{10}$	711	1024	2050	$5.81 \cdot 10^{11}$
192	1754	$5.30 \cdot 10^{10}$	$4.86 \cdot 10^{10}$	1 149	–	–	–
224	2042	$8.43 \cdot 10^{10}$	$7.73 \cdot 10^{10}$	1 881	2048	4098	$5.20 \cdot 10^{12}$
256	2330	$1.26 \cdot 10^{11}$	$1.16 \cdot 10^{11}$	3 848	3072	6146	$1.86 \cdot 10^{13}$
384	3484	$4.52 \cdot 10^{11}$	$4.15 \cdot 10^{11}$	17 003	7680	15362	$3.30 \cdot 10^{14}$
521	4719	$1.14 \cdot 10^{12}$	$1.05 \cdot 10^{12}$	42 888	15360	30722	$2.87 \cdot 10^{15}$

Fig. 5 Estimation of resources required to compute elliptic curve discrete logarithms using Shor's algorithm versus factoring an RSA modulus using Shor's algorithm

2.6 vulnerability in service

2.6.1 Race attack

The race attack, illustrated in Fig. 6 , allows for a situation in which an attacker creates two transactions, one genuine and one fraudulent. The target is any node that accepts transactions with 0-unconfirmed status, meaning the transaction is visible, but has not yet been included in a block. The attacker connects directly to the target as a network peer. The attacker also tries to connect closely or directly to a mining pool. By sending the fraudulent transaction to the target and the legitimate transaction to the mining pool, the attack may succeed if the target accepts the fraudulent transaction and provides some goods or services before ever seeing the legitimate transaction. This is why it is advised to wait for some minimum number of confirmations before considering a transaction valid.

2.6.2 DDoS attack

DDoS attacks are not specific to blockchain networks, but they can be used with some specific variation to attack blockchain and asset exchange networks. In this type of attack, an attacker typically leverages a network of hijacked devices to flood a network with an excessive amount of requests that cripple the network's ability to service legitimate traffic. Blockchain and exchange networks may protect against DDoS attacks in some fashion, but this protection is admittedly vulnerable to more complex attacks [65]. Bitcoin Gold, one of the cryptocurrencies forked from Bitcoin, suffered a massive DDoS attack during its launch, receiving of 10 million fraudulent requests per minute. According to [15], 74% of all Bitcoin-related sites have suffered a DDoS attack.

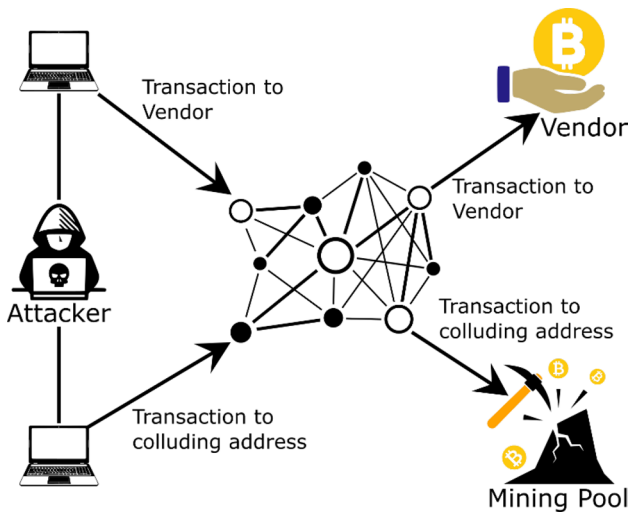

Fig. 6 An illustration of the race attack, which attempts to double-spend the same digital asset

2.6.3 Double spending attack

Bribery attacks are a type of attack in which an attacker creates a normal transaction to be included in a block. After waiting for some number of confirmations such that the transaction is irreversible, the attacker creates a fraudulent conflicting transaction and introduces it into a new fraudulent block. The attacker then bribes or rents a significant portion of the mining power in the network to extend the fraudulent branch until it becomes the longer branch, at which time the fraudulent transaction will become valid.

2.6.4 Finney attack

The Finney attack is a double-spending attack that requires a block to be pre-mined. This block will hold a fraudulent transaction but will not be broadcast yet. The same coins used in the fraudulent transaction will meanwhile be used as payment to a target node. After receiving some goods or services, the fraudulent block will then be broadcast to the rest of the network, thus invalidating the transaction sent to the target. Again, waiting for additional confirmations before accepting a transaction defeats this attack.

2.6.5 vector76 attack

The vector76 attack is a combination of the race and Finney attacks that targets victims that only require a single confirmation. In this case, the attacker establishes a direct connection to the target, such as an E-Wallet service, and to a mining pool. The attacker creates a large fraudulent transaction to deposit a large amount into the E-Wallet, and a small transaction with the same tokens to send to the miners. The attacker mines until a block is found. The fraudulent transaction is included in the block and both the block and the small transaction are broadcast at the same time. Once the E-Wallet service sees the fraudulent transaction, the attacker immediately withdraws the large number of tokens that were credited to his account. Meanwhile, the rest of the network is much more likely to accept the small transaction, thus invalidating the large fraudulent transaction to the E-Wallet service.

2.6.6 Collusion attack

Perhaps the most well-known attack is the 51% attack due to its ability to completely subvert the blockchain. In this type of attack, the mining power of over 50% of the network is under the control of a single entity or group. Such a group

would be able to control the history of the blockchain. For example, if a double spend happens, the colluding miners may force the acceptance of the fraudulent transaction by including it in a block. Even if the rest of the network disagrees, the entire network will reach consensus when the 51% mining pool outpaces the mining output of the rest of the network until the fraudulent chain becomes longer than the legitimate chain. Figure 7 illustrates such a fork in which the colluding group will mine enough blocks to eventually dominate the chain. Any blocks not on the main chain (black) will become stale blocks (purple)

2.7 Malware attacks

Given the recent explosion of cryptocurrency value, whether real or perceived, it's no wonder that various malware has appeared to try to steal cryptocurrency or disable the blockchain network. One particularly disturbing malware that has been growing rapidly is malicious cryptocurrency mining software that operates covertly in JavaScript applications that are executed by the browser. Mining software, such as Coinhive, is often hidden in product ads, which ubiquitously

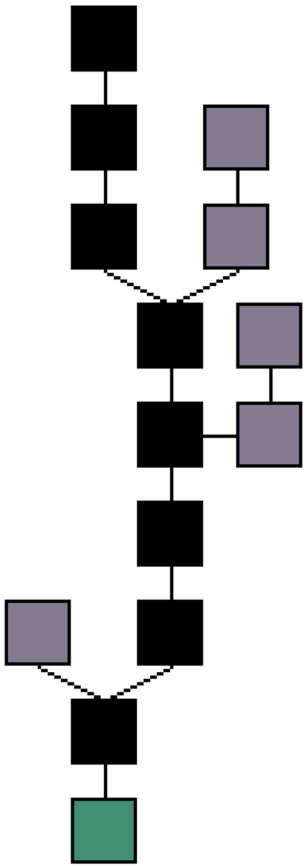

Fig. 7 An illustration of forks in a blockchain. The main chain is shown in black with stale blocks shown in purple

populate websites today. According to [28], near 55% of businesses have been affected by this type of mining software, including YouTube, Showtime, and others. Similar malware has been found in browser extensions and even using the NSA's leaked EternalBlue malware as a vector to a deliver cryptocurrency mining payload [21].

One unfortunate consequence of blockchain immutability, coupled with the ability to store arbitrary data on the blockchain, is that it is possible for malware to be stored on the blockchain. When such malware is included inside the blockchain, it may be difficult or impossible to remove later. As a result, every full node in the network will have the entire chain, including any malware that has been inserted into it. This is not only a concern with malware, but also with illegal, hateful, or defamatory content that could be placed on the chain without the possibility of removing it in the future.

Miners make a particularly tempting target for malware attacks. These nodes must validate and include transactions in blocks, create valid blocks using some consensus algorithm, and conduct various other administrative operations. There may be incentive for dishonest miners to attack other miners to attempt to cripple their ability to mine blocks, thus presenting a higher probability of reward to the dishonest miners. In 2017, a backdoor called Antbleed was introduced into the firmware of the hardware-based Antminer machines by the manufacturer of this equipment, Bitmain. According to [21], this backdoor might make it possible for Bitmain to disable up to 70% of the total mining equipment, as well as specifically targeted machines or customers. This backdoor could also be exposed to malicious parties through Man-in-the-Middle (MITM) attacks, DNS attacks, or domain hijacking [9].

2.8 Application vulnerability

By far the weakest link in blockchain security so far is the result of third-party applications that either run on or interact with the blockchain. Exchanges, wallets, and decentralized apps (dapps) have all fallen prey to various attacks, and though these attacks all come with the caveat that the underlying blockchain protocol is secure, the monetary losses and people affected are, of course, real.

2.8.1 Use case design flaw

The Ethereum blockchain is a powerful platform for creating and running smart contracts and dapps. A decentralized autonomous organization (DAO) is a smart contract-based system in which individuals may participate by contributing funds for the right to vote on proposals that are presented. The smart contracts that govern the system establish a set of rules that defines how users can interact with the system,

such as the percentage of votes required to acquire funds for a given proposal. "The DAO" is a particular DAO that is well known for being hacked using a bug in a feature of the DAO that would allow users to pull their funds back out of the DAO or even split a portion of the DAO into a child DAO. An attacker took advantage of this bug to drain over 3.6 million ether (the token for Ethereum) into a child DAO. The attack was possible because it was possible to recursively split the DAO into a child DAO many times before the balance of funds were actually transferred to the child DAO. To "fix" this issue, the Ethereum blockchain was forked into two chains, what is now call Ethereum, the chain in which this hack was rolled back and most funds were recovered, and Ethereum Classic, the original chain in which the DAO hack is still part of the chain's history.

2.8.2 Coding error

Several wallet applications have also been the target of attacks due to coding errors. In November of 2017, an individual under the name devops199 "accidentally" destroyed 513,743 ether, worth about 355 million at the time of this writing, due to a bug in the Parity wallet software. This was possible because Parity placed all multisig contracts inside a library, which is another smart-contract deployed on the Ethereum chain. Unfortunately, this library was flawed in such a way that it was possible for someone to initialize the library itself as a wallet, which would then give that person ownership of the library. Unfortunately, either by ignorance or intention, devops199 called this initialization function, then subsequently called a kill function that was built into this library. Since all multisig wallets depended on this library contract in the Parity system, killing that contract effectively made it impossible to recover the lost funds. One commenter relates this incident as analogous to going into the bank, noticing the vault door is open, walking into the vault, and burning all of the money.

2.8.3 Attack on exchanges

2.8.4 Past attacks (2014–2016)

Many cryptocurrency exchanges have also been subject to attack over the years. In November of 2014, Mt. Gox was handling over 70% of all Bitcoin transaction when it fell victim to an attack that cost 850,000 bitcoins, valued at 450 million at the time and 7.9 billion at the time of this writing. This attack was conducted over several years and was largely due to mismanagement and poor security practices. The attacker was able to access the private keys associated with many addresses stored in a so called hot wallet, meaning the wallet is accessible over the internet, as opposed to cold or offline wallet storage, and over time was able to simply withdraw the bitcoins that were deposited to those compromised addresses [56].

In January 2015, the Bitstamp exchange was compromised, causing a loss of about 19,000 bitcoins. This attack was the result of an extensive phishing campaign against the Bitstamp staff. Eventually, a Bitstamp system administrator fell victim to this attack, which led to the compromise and theft. Fortunately, most of Bitstamp's bitcoin reserves are stored offline, and even the 19,000 bitcoins that were stolen only amounted to about 10% of the bitcoins stored in hot wallets [46].

In an August 2016 attack, 120,000 Bitcoins was stolen from the Bitfinex exchange. The attack targeted a vulnerability in Bitfinex's multisignature wallets. A multisignature wallet is a wallet that requires multiple parties to sign any transaction involving that wallet. These wallets required three signatures, two of which would come from private keys held by Bitfinex and one signature from another company called BitGo. This was to act as an additional layer of security. The details of the attack are not entirely clear, as the BitGo servers were reportedly not compromised. To their credit, Bitfinex did reimburse all customer losses over time. Unfortunately, Bitfinex has more recently been accused of dubious behavior regarding artificially boosting Bitcoin prices by creating Tether coins, another cryptocurrency that is supposed to have a 1-to-1 ratio with US dollars in order to keep the value stable at 1.00, which would then be invested into Bitcoin, cashed out in USD when the price of Bitcoin rises, after which the process repeats.

2.8.5 Recent attacks

In December 2017, the FTC subpoenaed both Bitfinex and Tether and the situation is ongoing at the time of this writing. In January 2018, Coincheck, a Tokyo-based cryptocurrency, suffered an attack that rivals even the MtGox attack in magnitude. Over 500,000,000 NEM tokens were liberated from Coincheck wallets, totaling about 533 million. The details of this attack are unclear, as Coincheck has not publicly disclosed this information. However, this is yet another example of tokens being stolen from hot wallets.

2.8.6 Counter measure

The attacks on exchanges listed here are but several of the large scale attacks that have taken place. As the value of cryptocurrencies continues to increase, we will undoubtedly continue to witness these attacks taking place. This is also one time in which the immutability of the blockchain may not be desirable, as transactions can't simply be rolled back without creating a fork in the blockchain. It is unfortunate for those who are affected by these attacks, but it is

also impractical to fork any blockchain in which losses take place, splitting the community between the purists who are fully dedicated to the blockchains true history, good or bad, and the realists who do not want to take a hit for 533 million due to lax security and poor coding practices (Figs.8, 9).

3 Risks at blockchain application security

3.1 Network architecture vulnerability

3.1.1 Background

Vuln ID	Summary	CVSS Severity
CVE-2018-11687	An integer overflow in the distributeBTR function of a smart contract implementation for Bitcoin Red (BTCR), an Ethereum ERC20 token, allows the owner to accomplish an unauthorized increase of digital assets by providing a large address[] array, as exploited in the wild in May 2018, aka the "ownerUnderflow" issue. **Published:** August 15, 2018; 01:29:00 PM -04:00	(not available)
CVE-2018-13485	The mintToken function of a smart contract implementation for BitcoinAgileToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **Published:** July 09, 2018; 02:29:01 AM -04:00	V3: 7.5 HIGH V2: 5.0 MEDIUM
CVE-2016-10725	In Bitcoin Core before v0.13.0, a non-final alert is able to block the special "final alert" (which is supposed to override all other alerts) because operations occur in the wrong order. This behavior occurs in the remote network alert system (deprecated since Q1 2016). This affects other uses of the codebase, such as Bitcoin Knots before v0.13.0.knots20160814 and many altcoins. **Published:** July 05, 2018; 06:29:00 PM -04:00	V3: 7.5 HIGH V2: 5.0 MEDIUM
CVE-2016-10724	Bitcoin Core before v0.13.0 allows denial of service (memory exhaustion) triggered by the remote network alert system (deprecated since Q1 2016) if an attacker can sign a message with a certain private key that had been known by unintended actors, because of an infinitely sized map. This affects other uses of the codebase, such as Bitcoin Knots before v0.13.0.knots20160814 and many altcoins. **Published:** July 05, 2018; 06:29:00 PM -04:00	V3: 7.5 HIGH V2: 7.8 HIGH
CVE-2018-10831	Z-NOMP before 2018-04-05 has an incorrect Equihash solution verifier that allows attackers to spoof mining shares, as demonstrated by providing a solution with {x1=1,x2=1,x3=1,...,x512=1} to bypass this verifier for any blockheader. This originally affected (for example) the Bitcoin Gold and Zcash cryptocurrencies, and continued to be exploited in the wild in May 2018 against smaller cryptocurrencies. **Published:** May 09, 2018; 01:29:00 AM -04:00	V3: 7.5 HIGH V2: 5.0 MEDIUM
CVE-2018-6862	Cross Site Scripting (XSS) exists in PHP Scripts Mall Bitcoin MLM Software 1.0.2 via a profile field. **Published:** February 11, 2018; 10:29:00 PM -05:00	V3: 5.4 MEDIUM V2: 3.5 LOW
CVE-2018-1000022	Electrum Technologies GmbH Electrum Bitcoin Wallet version prior to version 3.0.5 contains a Missing Authorization vulnerability in JSONRPC interface that can result in Bitcoin theft, if the user's wallet is not password protected. This attack appear to be exploitable via The victim must visit a web page with specially crafted javascript. This vulnerability appears to have been fixed in 3.0.5.	V3: 5.3 MEDIUM V2: 2.6 LOW

Fig. 8 Coding flow reported in bitcoin during 2018

Vulnerability	Types	Weakness	Counter	Vulnerability	Types	Weakness	Counter
Key	Cryptography operation	Vulnerable Cryptography algorithm	strong algorithm and powerful encryption	Manipulation	Eclipse	Network process	Network encryption
	Hashing Operation				Transection		
Quantum		Computer computational power increase	Quantum immune algorithm use		Timejacking		
Identity	Replay	Weak network access system	Stronger Authentication	Service	Race	Service speed vs time tradeoff	Trained userbase
	Impersonation				Ddos		
	Sybil				FinneyAttack		
Reputation		Weak monitoring	Overseeing user		Vector76		
Application	Desgin	Weak Development process	Better Design & Development		Collusion		
	Coding			Malware		Permission Control	Regular code patch
	Exchange						

Fig. 9 BlockChain vulnerability reason and counter

Blockchains run on a decentralized, peer-to-peer network in which all entities adhere to the same protocols, preventing any single entity from controlling the underlying infrastructure. Ideally, this open, decentralized, permissionless architecture prevents any individual, state, company, or other group from exerting regulatory pressures or otherwise interfering with blockchain operations. Some blockchains, such as Bitcoin, communicate over unencrypted channels. This is not beneficial for privacy as any entity such as Internet Service Providers (ISPs), government agencies, and individuals are able to monitor all traffic over the bitcoin network. This makes the task of deanonymization much easier for those parties interested in tracing transactions back to their physical users. Other blockchains were designed to use end-to-end encryption to avoid this issue. Bitcoin also has an update proposed to implement network encryption but has yet to do so.

3.1.2 Blockchain scalability and transaction rate

Many current blockchains suffer from limited scalability because block size and block time, or the average rate at which blocks are found, are necessarily limited. Figure 10 shows the number of pending transactions for the Bitcoin blockchain from April 24, 2016 to March 25, 2018. In May of 2017, there were nearly 200,000 pending transactions, resulting in slower confirmation time for each transaction and higher fees. Several proposals that seek to enhance scalability have been presented. One is to increase block size. Greater block sizes will allow room for additional transactions but may also hinder block propagation speed. In [10], Decker and Wattenhofer argue that certain factors such as network topology and the current block propagation method are non-optimal and may contribute to increased possibility of attacks. They argue that an increase in block size would further contribute to the possibility of easier attacks. Another proposal that has already been successful to some degree is called segregated witness or SegWit. Segregated witness segregates the transaction data from signature data used to verify those transactions (the witness data). Doing so frees up considerable space for additional transactions and more importantly fixes transaction malleability. However, block size increases and SegWit alone do not sufficiently address the scalability issue.

3.1.3 Counter measure

The lightning network opens new possibilities for dramatically increasing blockchain scalability, making payments instant, and allowing cross-chain transactions. As long as blockchains adhere to the same consensus rules, cross-chain transactions will be possible. The lightning network would be based on creating bidirectional payment channels based on smart contracts and would make it possible to process millions or billions of transactions per second, and without having to worry about block confirmation times [49].

3.2 Privacy issue

Though some believe Bitcoin and other blockchains are anonymous, this is not exactly true. Addresses are only loosely tied to physical identity, and therefore it may be difficult but not impossible to identify the real identity of a person based on their transaction history. The word "pseudonymous" is a more accurate description. Companies such as Chainalysis and Elliptic make a business of identifying the owners of digital wallets and tying wallet addresses to physical identities. In fact, the IRS has licensed and has begun using Chainalysis to find people cheating on their taxes by failing to report profits [52].

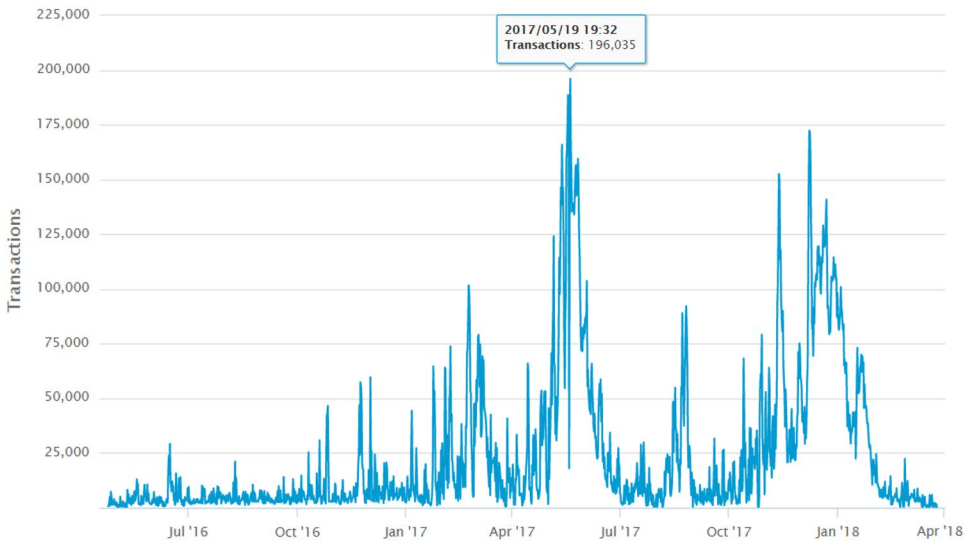

Fig. 10 Number of pending transactions in the Bitcoin network

In addition to software that tries to deanonymize cryptocurrency users, there are also services such as CoinJoin that anonymize Bitcoin transactions by mixing several accounts together and redistributing the coins in a pseudorandom fashion. For example, if 3 people want to hide their funds, they may use this service to pool all their bitcoins. The service then makes a number of new transactions to distribute the Bitcoins back to the original owners. Some blockchains were even created with enhanced privacy in mind. Dash, Zcash, and Monero address the problem of privacy by obfuscating transaction amounts, mixing transaction with decoys, and other methods. The transactions may still visible, but the details are hidden, making it more difficult to deanonymize users.

Because blockchain transactions are immutable and permanent, the entire history of the blockchain available to any parties that wish to look at it. Addresses that are publicized online, addresses used in purchasing cryptocurrencies through online exchanges, activity that is traced through ISPs, and other tracing methods may all be used to build a database of identities and transaction histories. This history creates a potential issue that may affect the fungibility of a digital asset, which is to say that one unit of the asset carries the same value as another similar unit. In this case of Bitcoin, the complete history of each bitcoin, millibitcoin, bit, and satoshi is publicly available. This has given rise to the concept of "clean bitcoins", which may be obtained through mixing services and which are worth slightly more than other coins in the network because they lack that history. Further, exchanges may blacklist specific wallet addresses, making any coins to and from those wallets essentially worthless [7].

In blockchains such as Ethereum that provide not just a cryptocurrency but a framework for smart contracts and dapps, privacy is a critical issue. Many entities engaging in transactions may not wish for their business to be public. In [8], Vitalik Buterin discusses methods of keeping smart contracts private and secure. In one scheme, the contract would store a hash of the contract code. The participants would send their funds to this contract. Upon completion of the conditions of the contract, either party could submit the result of the contract code and the other party could send an additional transaction to agree to the result, after which the funds would be distributed.

3.2.1 Cryptojacking

For definition, we can say that "Remotely using someone else owned computing machine for mining for blockchain based cryptocurrency without permission". There are several Cryptojacking tools available for someone to use. Most common way to do crypto jacking is browser-based [22]. Browser companies are relentlessly trying to protect their user from releasing blocking programs, In a paper, Marius Musch et al. [44] propose a web miner detection model to identify crypto hijacker. Using CPU consume rate and machine learning,some researcher in Mcafee antivirus trying to solve the crypto jacking.

4 Recent works

4.1 In new application area

In the article written by researchers from Northumbria University [37] found eight categories where some kind of blockchain implementation has already happened or at least have some proof of concepts, These are smart energy; smart cities and the sharing economy; smart government; smart homes; intelligent transport; building information modeling (BIM) and construction management; and business models and organizational structures. In Fig. 11 shows the number of recent last(3 year paper) published with some implementation examples from Google Scholar and IEEE search results. In paper on new business model based on blockchain [45] researcher Nowiski shows that blockchain innovation may influence differing measurements of plans of action in different businesses. But also warns that this technology may be most useful if the trust in the authenticity of products is an important element of value for customers. Also if advantages receive from its application will be way better if transaction costs are relatively more as compared to margins of transactions (Fig. 12).

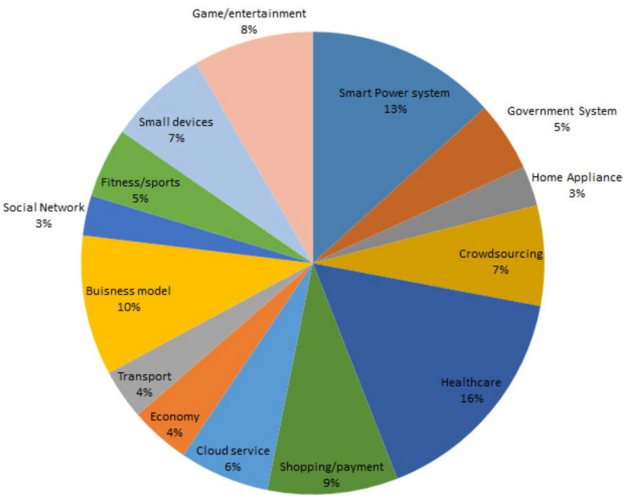

Fig. 11 Published journal in last 3 years with a proof of concept in blockchain

Field	BlockChain Framework	Field	BlockChain Framework	Field	BlockChain Framework
Big Data	ProvChain	Social Network	Indorse	Education	DISCIPLINA
	BBDS		Sapien		edChain
	DataBlockChain.io		Steemit		EdgeCoin
	Dxchain		Sola		SkillChain
	Zebi.io		ong.social	Entertainment	Steem.io
Medical	MedicalChain	Sports	DYNO		Livepeer
	Healthureum		BlocSide Sports		Slate.io
	IRYO.IO		EtherSport	Finance	ChronoBank.io
	trustedhealth.io		Sportie		Aniko
	Clinicoin	Shopping	CryptCard		Symbiont
	MedCredits		Bitit		LAPO Blockchain

Fig. 12 Various blockchain frameworks for different purposes

4.2 For solving challenges in blockchain

4.2.1 Security challenges

LNSC protocol [30] has been introduced and was able to solve key attack , replay attack, impersonation attack, modification attack and man in the middle attack. Another resistant protocol name BSeIN protocol [40] was introduced recently which uses blocksize limitation with attribute based signatures and multi receivers encryption, It makes this protocol to resistance against DDoS/DoS attack, replay, impersonation, modification and man in the middle attack. A new blockchain named Trustchain [47] shows effectiveness with solving the Hiding Blocks and Refusal to Sign problem for blockchain. Its all very much effective to prevent Sybil attack. Wang et al. also discuss the tempering attack, double spending attack and overlay attacking his article [63] Preserving transaction privacy in bitcoin. He proposed some solutions to mitigate these attacks.

4.2.2 Privacy challenges

In paper [24], showed that hyper ledger of blockchain technology can be effectively added in vehicle to grid networks, It introduces a registration and data maintenance process , which ensures the anonymity of user payment data while enabling payment auditing by privileged users.A research to secure Privacy for protecting user files using blockchain was described in a paper recently [33], where it was showed that their developed process 'Seguro', utilises the security capabilities of hyper-ledger technology to ensure the user's privacy with respect to his/her documents while also implementing an efficient, easy-to-use sharing mechanism that facilitates document verification at any third party during the registration or any other process.

For blockchain based identification system Lee et al. proposed the BIDas framework [36] which use block chain based id as a service. In this service authentication can be achieved without having any preregistered information of users.

A similar work was also done by [35] Kim et al., where a blockchain based secure authentication management system was proposed which is using human-centric scheme for trusting mobile computing data.

Another important work was [17] recently done by Dagher et al., for making health data securing with block chains, other previous attempt was failed due to implementing block chain make its hard to retrieve files while securing the privacy. Their framework, named Ancile, utilizes smart contracts in an Ethereum-based blockchain for heightened access control and obfuscation of data, and employs advanced cryptographic techniques for further security. This framework is able interact with the different needs of patients, providers, and third parties, and to understand how the framework could address longstanding privacy and security concerns in the healthcare industry.

Chrisitan writh et al., also showed [66] how blockchain design can be compatible with General Data Protection Regulation (GDPR) act.

4.2.3 Power consumption challenge

Alexde Vries recently published a paper on blockchain cryptocoins specially bitcoin power consumption problem, His paper [19] has marked several methods that are currently used in determining the current and future electricity consumption of the Bitcoin network. From his methods we can get some insights such as

- Electricity current consumption 2.55 GW.
- Daily bitocin transaction is 1,400,000 per week.
- Average electricity consumed per transaction equals at least 300 kWh.
- 900 kWh will be needed by 2019 for per transaction.

To solve this problem a lightning network is trying to establish by a bit coin community. But still this will be remain a big problem for blockchain based cryptocurrency.

4.2.4 Scalability challenges

To solve the scalability problem in blockchain several research work is being progressed. Recently one of the patents [31] filed where Guerney et al. invented a way to vynamic recording of blockchain transactions to optimize performance and scalability. They created a lattice structure containing the proposed transactions for the blockchain block, the lattice structure comprising a top and a bottom and a plurality of nodes representing the proposed transactions, determining an order of execution of the proposed transactions for the blockchain block via the lattice structure, and processing the proposed transactions in the lattice structure in parallel based on a configuration of the lattice structure.

Another recent work was done by Zang et al. [67] where he analyze the scalability problem of blockchain and proposed some solution. In paper [50] Prinz et al. shows the relation between blockchain with CSCW and CSCB and how it can solve scalability problem, In Fig. 13 this comparison can be viewed.

4.2.5 Computation challenges

Recently another group of researchers led by Nojoumian et al. [39] tried to resolve the concern of the blockchain mining related issues by proposing to incentivizing blockchain miners to detect dishonest mining strategies. In 2018 June another patent was filed to increase blockchain security by Carey and Gerard. They proposed a new method called interlocked blockchains to increase blockchain security [12]. Their method claimed to preventing vulnerabilities in a blockchain due to a period of quiescence. To solve fault injection in Digital node [6] Boireu et al. proposed a solution in his article securing the blockchain from hacker where multi signature idea is discussed.

	Blockchain	CSCW	CSCB
Consensus building	Proof of work / proof of Stake; competition based approaches by means of local algorithms	Collaborative editing: operation transformation; context based approaches by means of distributed algorithms	Proof of collaboration awareness based on a distributed algorithm that validates transactions based on their cooperation context.
Smart contracts	Irreversible program code as integral part of a transaction	Participative and user centric design requires agile software engineering methods.	Understanding smart contracts as cooperation patterns that are governed by versioned and flexible cooperation rules
Reputation and trust	Irreversible transaction records and smart contracts	User reputation and recommendation	Uptake of the transaction records into reputation management approaches. Building blocks for decentralized shareconomy networks.
Affordance	Affordance for trust and comprehensibility	Affordance for seamless cooperation	Affordance for trusted cooperation in a decentralized network

Fig. 13 Blockchain with CSCW and CSCB and how it can solve scalability problem [50]

4.3 Big data area

4.3.1 Background

From recent bigdata survey [2], We can see that maintaining big data center is increasing operational cost worldwide and this cost getting higher day by day, no matter how much cheaper the data medium or bandwidth speed increase. On average each of the 24 firms had 16 data center sites.It stated that "The companies with the broadest data center footprint are the leading cloud providers—Amazon/AWS, Microsoft, IBM and Google. Each has 45 or more data center locations with at least three in each of the four regions—North America, APAC, EMEA and Latin America. Oracle and Alibaba also have a notably broad data center presence. The remaining firms tend to have their data centers focused primarily in either the US (Apple, Twitter, Facebook, eBay, LinkedIn, Yahoo) or China (Tencent, Baidu)" [2].

In Fig. 14 we can see the paradox of Bigdata investment

- Every 1.2 years total business data get double.
- 20–35% of operating revenue can lost due to poor data management.
- From the survey of top executives of fortune 500 companies, it was reported that current data amount is serious problem in IT world. 55% of survey participants reporting IT systems is slowing down and 47% mentions data security problems
- 76.

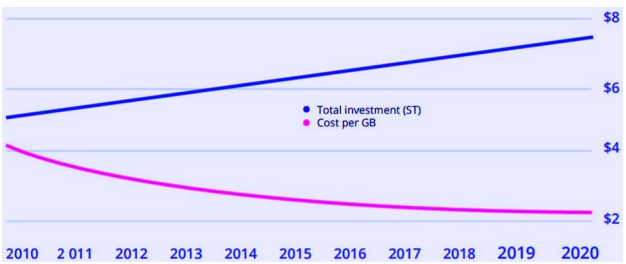

Fig. 14 Bigdata investment and cost paradox [32]

- 76% participants in Avalande survey anticipated their data increase rate is at least 2× per year.

4.3.2 Blockchain research on bigdata

Now blockchain framework implementing to reduce bigdata computation cost seems inevitable but still there needs a lots obstacle to solve. Some researchers are trying to pave the way notably Vo et al. [61]. They highlighted the common issues in data management and key problems. Some very notable work has been done by Bennet et al. [4] in his paper about blockchain with land data and noSQL.The common goal is to replace the big data center using power of distributed computing which can easily be enable by blockchain. Data privacy is the big issue here to tackle this problem Jain et al. [33] proposed a Digital storage system name Seguro, which has addressed some of the concerns of blockchain based database (Figs. 15, 16).

4.4 Social network and crowd sourcing

4.4.1 Background

Blockchain can be also be used in social network as anonymity and trust is now a big issue in social network. Specially, recent fake data scandal and responsibility of rumor in social media debate create an atmosphere for blockchain implementation [3]. The same research also applied when we need to make reliable crowd sourcing. Verify reliability but keeping person anonymous feature becomes very useful when it is comes to crowd sourcing. There is some new research on crowd sourcing with blockchain has done.

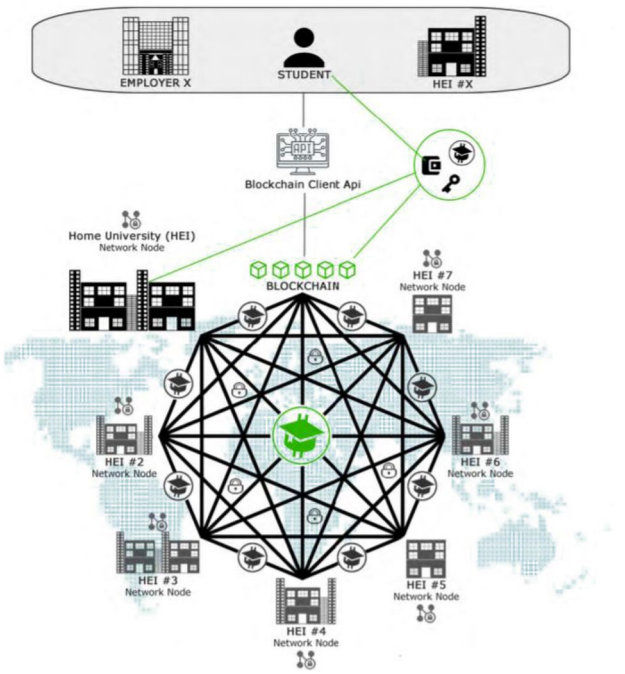

Fig. 16 EduCTX platform [59]

4.4.2 Social network

Swan et al. [58] proposed an algorithm to build economic networks and algorithm trust which is based on game theory

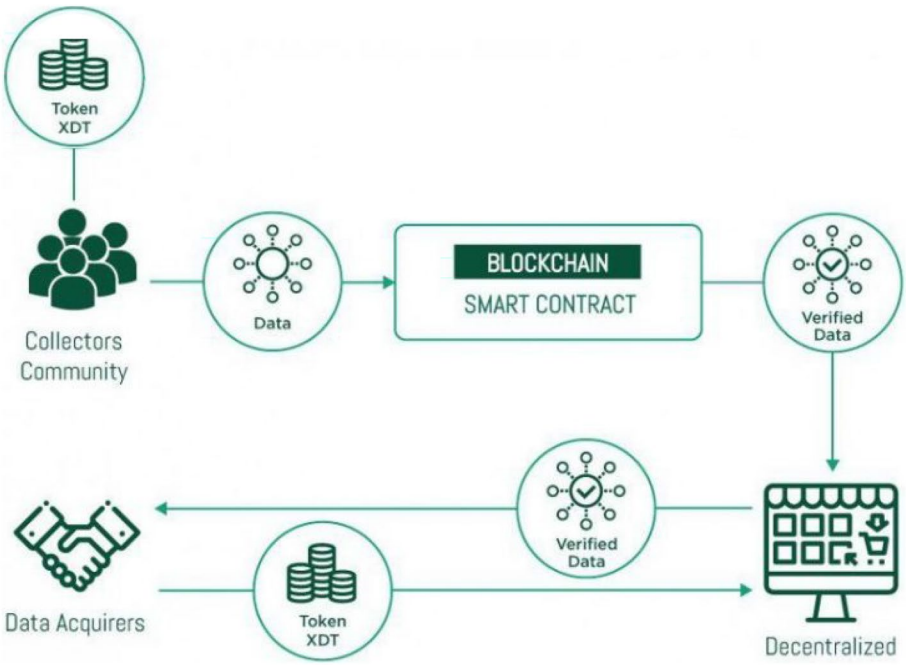

Fig. 15 CrowdSource using blockchain by Dataeum [18]

and networked games, Similar of this work, Qin et al. developed a blockchain network RPCHAIN [51] which presented a blockchain based academic social network and they proposed a new algorithm for consensus name proof by reputation (PoRe).

To improve social networks Chen proposed a trusted social networks using blockchain technology [13]. Which does peer to peer information exchange to ensure privacy. For similar goal another research team led by Yutao et al. [34] worked with blockchain which maximize the social welfare while making sure computational efficiency and privacy concern keep addressed.

4.4.3 Crowd sourcing

Recently many works has been done in this area notable work from Wang et al. [64] where they worked on Crowdsourced Energy Systems, another important approach provided by ZebraLancer [41]. They are their first private and anonymous blockchain network. They make the user unlinkable by separating certificate generator from blockchain. For reviewing using the power of crowdsource a system has been proposed by Shah [55] where he proposed a blockchain system which can use to review document based on artificial scoring computed from textual and visual feedback. CrowdBC [38] is one of the prominent framework of blockchain for crowd sourcing. They resolve the high transaction fees in their framework. And their framework is not vulnerable to DDos or Sybil attack.

4.5 Health care

Health Care has many areas which are still waiting to be digitalized, but already digitalized fields are suffering with many concerns . HIPPA in USA and GDPR in Europe are very strict on medical data digitalization. Blockchain has so many opportunities in this areas. Already several important work done with blockchain in health care [28]. Some field blockchain is using are

- Medical data keeping.
- Health insurance provider.
- Pharmaceutical industry.
- Medical data processing using AI.

In paper by Kevin et al. [16] it seems there are lot of new company expanding in health sector. Company name FarmaTrust Made a block chain for pharmaceutical supply chain. For health research, blockchain is now using for Diabetes health care and management [14], Most notable recent research has done by Zhao et al. [68] for securing health care data using blockchain. They developed a body sensor network with high performance and connected with blockchain.

4.6 LifeStyle

In our daily life, so many fields blockchain can integrated and make our life easier, Such as it can use for education, fitness, sports, media, video, shopping, finance etc etc. A framework name Edutex [59] proposed to use blockchain for education system. Where student will get token for completed course. To educate health professional researcher Funk et al., proposed a data framework and discuss the potential of blockchain in health education [23]. In "Proceedings of 1st ERCIM blockchain workshop 2018" [25] proposed a life long learning system using blockchain. They visualize blockchain to filter our forgery of certificate and support the records of education for long time.

4.7 New area to research on

In recent survey several open question has been Amine et al. [1] and considered as new research challenges,

- Resiliency against combined attacks.
- Dynamic and adaptable security framework.
- Compliance with GDPR.
- Energy efficient mining.
- Social network and trust management.
- Blockchain specific infrastructure.
- Vehicular cloud advertisement dissemination.
- Skyline query processing.

5 Summary

This survey focused on blockchain security issues for different aspects (theory to implementation) these issues are classified to eight type and explain here with the reason of these concerns and what can be done to prevent these issues. We noted that recent blockchain are using improved policy and procedure to resistance from cyber attacks. Some of the vulnerability we identified could be obsolete upcoming days and some new vulnerability could be discovered. We also presented new research trends in the blockchain technology, while it seems mostly healthcare, cloud service and finance is going after blockchain mostly, but also many sectors of our lives are now under research to add the advantages of the blockchain.

We hope this paper will help someone to understand what is at stake when developing a new blockchain and also what sectors of fields are getting powered by blockchain. We also expect that this review will give developers and implementors some guidance to deploy secure blockchain technology.

References

1. Amine Ferrag M, Derdour M, Mukherjee M, Derhab A (2018) Blockchain technologies for the internet of things: research issues and challenges. IEEE, New York
2. Avanade (2018) Cloud solutions that deliver the speed you need to become a digital business. Avanade, Seattle
3. Bahri L, Carminati B, Ferrari E (2018) Decentralized privacy preserving services for online social networks. Online Soc Netw Media 6:18–25
4. Bennett R, Pickering M, Sargent J (2018) Innovations in land data governance: unstructured data, nosql, blockchain, and big data analytics unpacked. In: Land and poverty conference 2018. Land governance in an interconnected world, Washington, DC, 19–23 Mar 2018
5. Bernstein DJ, Lange T (2014) Safecurves: choosing safe curves for elliptic-curve cryptography. University of Illinois, Chicago
6. Boireau O (2018) Securing the blockchain against hackers. Netw Secur 2018(1):8–11
7. Buntinx J (2017) What is bitcoin fungibility. The Merkle, London
8. Foundation E (ed.) (n.d.) Privacy on the Blockchain. Retrieved November 01, 2018, from https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/
9. Buterin V (n.d.) Ethereum Project. Retrieved November 1, 2018, from http://www.ethereum.org/
10. Decker C, Wattenhofer R (2013) Information propagation in the Bitcoin network. IEEE P2P 2013 Proceedings, pp. 1–10
11. Choo R, He X, Lin C, He D, Vasilakos AV (2018) Bsein: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. Netw Comput Appl 116:42–52
12. Carey JE, Gerard SN (2018) U.S. Patent Application No. 15/374,493
13. Chen Y, Li Q, Wang H (2018) Towards Trusted Social Networks with Blockchain Technology. arXiv preprint: arXiv:1801.02796
14. Cichosz SL, Stausholm MN, Kronborg T, Vestergaard P, Hejlesen O (2018) How to use blockchain for diabetes health care data and access management: an operational concept. J Diab Sci technol. https://doi.org/10.1177/1932296818790281
15. Cimpanu C (2017) 74% of all Bitcoin-Related Sites Suffered a DDoS Attack. Retrieved November 1, 2018, from https://www.bleepingcomputer.com/news/security/74-percent-of-all-bitcoin-related-sites-suffered-a-ddos-attack/
16. Clauson KA, Breeden EA, Davidson C, Mackey TK (2018) Leveraging blockchain technology to enhance supply chain management in Healthcare. Blockchain in Healthcare Today
17. Dagher GG, Mohler J, Milojkovic M, Marella PB (2018) Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain Cities Soc 39:283–297
18. Dataeum: First Blockchain Solution that Produces 100% Accurate Data through Crowdsourcing (2018) Retrieved November 1, from https://www.cnbcafrica.com/apo/2018/04/12/dataeum-first-blockchain-solution-that-produces-100-accurate-data-through-crowdsourcing/
19. de Vries A (2018) Bitcoin's growing energy problem. Joule 2(5):801–805
20. Android random number flaw implicated in Bitcoin thefts (2013) Retrieved November 1, 2018, from https://nakedsecurity.sophos.com/2013/08/12/android-random-number-flaw-implicated-in-bitcoin-thefts/
21. Ducklin P (2018) What are "WannaMine" attacks, and how do I avoid them? Retrieved from https://nakedsecurity.sophos.com/2018/01/31/what-are-wannamine-attacks-and-how-do-i-avoid-them/
22. Eskandari S, Leoutsarakos A, Mursch T, Clark J (2018) A first look at browser-based cryptojacking. arXiv preprint arXiv:1803.02887
23. Funk E, Riddell J, Ankel F, Cabrera D (2018) Blockchain technology: a data framework to improve validity, trust, and accountability of information exchange in health professions education. Acad Med 93(12):1791–1794
24. Gao F, Zhu L, Shen M, Sharif K, Wan Z, Ren K (2018) A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. IEEE Network, New York
25. Gräther W, Kolvenbach S, Ruland R, Schütte J, Torres C, Wendland F (2018) Blockchain for education: lifelong learning passport. In: Proceedings of 1st ERCIM blockchain workshop 2018. European Society for Socially Embedded Technologies (EUSSET)
26. Grover LK (1996) Fast quantum mechanical algorithm for database search. In: ACM symposium on the theory of computing, pp 212–219
27. Grover LK (1997) Quantum mechanics helps in searching for a needle in a haystack. Phys Rev Lett 78:325–328
28. Hegadekatti V, Hegadekatti K (2018) Blockchain applications in medical sciences. Int J Sci Res 7(4)
29. Heilman E, Zohar A, Goldberg S (2015) Eclipse attacks on bitcoin's peer-to peer network. In: USENIX conference on security symposium, pp 129–144
30. Huang X, Xu C, Wang P, Liu H (2018) LNSC: a security model for electric vehicle and charging pile management based on blockchain ecosystem. IEEE Access 6:13565–13574
31. Hunt GD, Koved L (2018) U.S. Patent Application No. 15/372,068
32. IDC (2012) Executive summary: a universe of opportunities and challenges. IDC, Framingham
33. Jain A, Jain A, Chauhan N, Singh V, Thakur N (2018) Seguro Digital storage of documents using Blockchain
34. Jiao Y, Wang P, Niyato D, Xiong Z (2018) Social welfare maximization auction in edge computing resource allocation for mobile blockchain. In: 2018 IEEE international conference on communications (ICC), pp 1–6. IEEE, New York
35. Kim H-W, Jeong Y-S (2018) Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain. Hum-Centric Comput Inf Sci 8(1):11
36. Lee J-H (2018) Bidaas: blockchain based id as a service. IEEE Access 6:2274–2278
37. Li GD, Jenni Kassem M (2018) Blockchain in the built environment: analysing current applications and developing an emergent framework. Northumbria, Newcastle
38. Li M, Weng J, Yang A, Lu W, Zhang Y, Hou L, Liu J-N, Xiang Y, Deng RH (2017) Crowdbc: a blockchain-based decentralized framework for crowdsourcing. In: Technical report, IACR Cryptology, ePrint archive, University of California, Santa Barbara, vol 444
39. Liang X, Shetty S, Tosh D, Kamhoua C, Kwiat K, Njilla L (2017) Provchain: a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In: Proceedings of the 17th IEEE/ACM international symposium on cluster, cloud and grid computing, pp 468–477. IEEE Press, New York
40. Lin C, He D, Huang X, Choo K-KR, Vasilakos A V (2018) Bsein: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. J Netw Comput Appl 116:42–52
41. Lu Y, Tang Q, Wang G (2018) Zebralancer: private and anonymous crowdsourcing system atop open blockchain. arXiv preprint: arXiv:1803.01256
42. Maria A, Zohar V (2017) Hijacking bitcoin: routing attacks on cryptocurrencies,. In: IEEE symposium on security and privacy, pp 375–392

43. Menn J (2013) Exclusive: secret contract tied NSA and security industry pioneer. Retrieved November 1, 2018, from https://www.reuters.com/article/us-usa-security-rsa/exclusive-secret-contract-tied-nsa-and-security-industry-pioneer-idUSBRE9BJ1C220131220
44. Musch M, Wressnegger C, Johns M, Rieck K (2018) Web-based cryptojacking in the wild. arXiv preprint: arXiv:1808.09474
45. Nowiński W, Kozma M (2017) How can blockchain technology disrupt the existing business models? Entrep Bus Econ Rev 5(3):173–188
46. List Of High Profile Cryptocurrency Hacks So Far (August 24th 2017). (2017, August 24). Retrieved November 1, 2018, from http://storeofvalueblog.com/posts/cryptocurrency-hacks-so-far-august-24th/
47. Otte P, de Vos M, Pouwelse J (2017) Trustchain: a sybil-resistant scalable blockchain. Future Gener Comput Syst
48. Keutmann (2018) Keutmann/Trustchain. Retrieved November 1, 2018, from https://github.com/keutmann/Trustchain
49. Poon J, Buterin V (2017) Plasma: Scalable autonomous smart contracts. White paper
50. Prinz W (2018) Blockchain and CSCW—shall we care? In: Proceedings of 16th European conference on computer-supported cooperative work-exploratory papers. European Society for Socially Embedded Technologies (EUSSET)
51. Qin D, Wang C, Jiang Y (2018) Rpchain: a blockchain-based academic social networking service for credible reputation building. In: International conference on blockchain. Springer, New York, pp 183–198
52. The IRS Has a Way to ID Bitcoin Tax Cheats (n.d.) Retrieved November 1, 2018, from http://fortune.com/2017/08/22/irs-tax-cheats-bitcoin-chainalysis/
53. Schneier on Security (2007) Retrieved November 1, 2018, from https://www.schneier.com/essays/archives/2007/11/did_nsa_put_a_secret.html
54. Schneier NFB (2003) Practical cryptography. Wiley, Indianapolis
55. Shah SN (2018) Distributed electronic document review in a blockchain system and computerized scoring based on textual and visual feedback, 16 Jan 2018. US patent 9870591
56. Nilsson K (2017) Breaking open the MtGox case, part 1. Retrieved November 1, 2018, from https://blog.wizsec.jp/2017/07/breaking-open-mtgox-1.html
57. Stevens M, Pierre K, Albertini A, Markov Y, Bursztein E (2017) The first collision for full SHA-1. In: Katz J, Shacham H (eds) Advances in cryptology–crypto 2017. Springer, New York
58. Swan M, Brunswicker S (2018) Blockchain economic networks and algorithmic trust. In: AMCIS 2018
59. Turkanović M, Hölbl M, Košič K, Heričko M, Kamišalić A (2018) Eductx: a blockchain-based higher education credit platform. IEEE Access 6:5112–5127
60. University Stanford (2011) Pertinent side channel attacks on elliptic curve cryptographic systems. Stanford University, Stanford
61. Vo HT, Kundu A, Mohania MK (2018) Research directions in blockchain data management and analytics. In: EDBT, pp 445–448
62. Wang F (2015) Eclipse attacks on bitcoin's peer-to-peer network. https://medium.com/mit-security-seminar/eclipse-attacks-on-bitcoin-s-peer-to-peer-network-e0da797302c2
63. Wang Q, Qin B, Hu J, Xiao F (2017) Preserving transaction privacy in bitcoin. Future Generation Comput Syst. https://doi.org/10.1016/j.future.2017.08.026
64. Wang S, Taha A, Wang J (2018) Blockchain-assisted crowdsourced energy systems. arXiv preprint: arXiv:1802.03099
65. Weaknesses. (n.d.). Retrieved November 1, 2018, from https://en.bitcoin.it/wiki/Weaknesses
66. Wirth C, Kolain M (2018) Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data. In: Proceedings of 1st ERCIM blockchain workshop 2018. European Society for Socially Embedded Technologies (EUSSET)
67. Zhang R (2018) Blockchain scalability: prospective solutions for bitcoin, ethereum, and other blockchain networks
68. Zhao H, Bai P, Peng Y, Xu R (2018) Efficient key management scheme for health blockchain. CAAI Trans Intell Technol 3(2):75–82