Blockchain And The Future of the Internet: A Comprehensive Review

Fakhar ul Hassan[1], Anwaar Ali[2], Siddique Latif[3], Junaid Qadir[4], Salil Kanhere[5], Jatinder Singh[6], and Jon Crowcroft[7]

[1,4]Information Technology University (ITU), Punjab, Pakistan
[2,6,7]Computer Laboratory, University of Cambridge, United Kingdom
[3]University of Southern Queensland, Australia
[5]University of New South Wales, Australia

Abstract—**Blockchain is challenging the status quo of the central trust infrastructure currently prevalent in the Internet towards a design principle that is underscored by decentralization and transparency. In ideal terms, blockchain advocates a decentralized, transparent, and more democratic version of the Internet. Essentially being a trusted and decentralized database, blockchain finds its applications in fields as varied as the energy sector, forestry, fisheries, mining, material recycling, air pollution monitoring, supply chain management, and their associated operations. In this paper, we present a survey of blockchain-based network applications. Our goal is to cover the evolution of blockchain-based systems that are trying to bring in a renaissance in the existing, mostly centralized, space of network applications. While reimagining the space with blockchain, we highlight various common challenges, pitfalls, and shortcomings that can occur. Our aim is to make this work as a guiding reference manual for someone interested in shifting towards a blockchain-based solution for one's existing use case or automating one from the ground up.**

I. INTRODUCTION

The paradigm shift entailed by blockchain's premise of decentralization envisages an eventual migration from the end-to-end principle to trust-to-trust principle [1]. According to this new design principle, a user should ideally have complete control over trust decisions particularly pertaining to user's data that powers a network application such as an online social network. This decentralization aspect forms the basis of the blockchain-based networks. This further paves the path for an era of distributed trust and consensus. This implies that large networks, in a peer-to-peer configuration, will guarantee the integrity of transactions (simply put interactions) among their peers without the involvement of any centrally trusted mediating third party. The provision of verifiable trust guarantees further entails that such networks can be audited in a trusted and transparent manner. This ability to audit is useful to hold a peer of a networked system accountable lest a dispute or malfunctioning of some other sort arises. Moreover, any application that requires interaction among various stakeholders for its operations in a mutually non-trusting environment (where the stakeholders do not have to or do not want to trust one another) can benefit from blockchain as it creates transparency and trust in interactions among the stakeholders without involving any third party. That is

the reason why industries such as transport, energy sector, insurance, finance, and logistics have started to show their interest in blockchain technology to automate their solutions [2]–[5].

It can be observed that although the onset of the Internet revolution heightened the societal collaboration among people, communities, businesses [6], however, many of the Internet applications (such as email and Domain Name System (DNS)) largely remain centralized as far as their management and core development are concerned. The centralized governing bodies are usually behind the trust guarantees associated with such online applications. Similarly, the issue of trust in cloud-hosted data storage is another contemporary challenge predicated on the inherent centralized nature of the Internet [1]. The clients of such online and cloud-based services, such as cloud storage and computation, usually put their trust in the claims put forward by the third party cloud providers. It raises the pressing need for *verifiability* that the cloud is not tampering with a client's stored data and is always returning correct results in response to the requested computation. A single instance of a data breach in cloud storage or a faulty execution of a requested set of computations can lead to disastrous ramifications for such a business. As it has been seen in a recent data breach that calls the trust in central management of online services such as Facebook (an online social network) into question [7]. Blockchain, on the other hand, with its premise of immutability, transparency, and peer-to-peer consensus can provide the means for a trusted audit of networked systems while at the same time giving much of the control back to the edges of a network.

A. Contribution of the survey

In this paper we provide a broad ranging survey of the implications of blockchain on the future of the Internet with a comprehensive take on their legal and regulatory ramifications as well. Instead of limiting ourselves to one particular use case or application (such as the Internet of things (IoT) [8], [9]), we cover a wide range of use cases and try to observe the common patterns, differences, technical limitations so that a more informed decision can be made by someone interested in deploying a use case from ground up or translating one's use

case to a blockchain-based solution. We provide a comparison of our paper with other recent blockchain-based surveys in Table I. Apart from encompassing most of the issues covered by recent survey literature, a clear distinguishing feature of this paper is that we also discuss a few of the most important legal and regulatory challenges and ramifications of deploying a blockchain-based solution. This is particularly important given the development of new data protection regulations (such as the advent of the General Data Protection Regulation (GDPR) in Europe), and regular reports of data breaches and government mass surveillance stories coming to light.

B. Structure of the survey

The rest of the paper is organized in three main sections. In the section titled *Background* (Section II), we provide the necessary background to understand the big picture of how blockchain works by introducing distributed ledger technology, distributed consensus, smart contracts, and public and private blockchains. In the next section (Section III) titled *Blockchain-based Network Applications*, we provide examples of how blockchain can be used to evolve trust mechanisms for the decentralized Internet, email, Internet of Things (IoT), content distribution, distributed cloud storage, online social networks, cybersecurity, public key infrastructure, and other miscellaneous applications. Thereafter in the section titled *Challenges and The Road Ahead* (Section IV), we discuss the current challenges facing blockchain and their various technical, legal, regulatory ramifications: in particular, we discuss governance, operational, and regulatory issues; scalability issues; security and privacy concerns; sustainability concerns; anonymity; the use of artificial intelligence (AI) and machine learning (ML); and issues related to usability and key management. Finally the paper is concluded in Section V.

II. BACKGROUND

In this section, we provide the necessary background to understand what blockchain is and how it works. Our discussion in this section follows an evolutionary approach which means we start with Bitcoin [21] (the first incarnation of a blockchain-based application) and discuss how the technology evolved giving rise to other concepts and systems along the way.

A. Blockchain and distributed ledger technology (DLT)

The original premise of blockchain is to establish trust in a peer-to-peer (P2P) network circumventing the need for any sort of third managing parties. As an example, Bitcoin introduced a P2P monetary value transfer system where no bank or any other financial institution is required to make a value-transfer transaction with anyone else on Bitcoin's blockchain network. Such a trust is in the form of verifiable mathematical evidence (more details on it follow in Section II-D). The provision of this trust mechanism allows peers of a P2P network to transact with each other without necessarily trusting one another. Sometimes this is referred to as the *trustless* property of blockchain. This trustlessness further implies that a party interested in transacting with another

entity on blockchain does not necessarily have to know the real identity of it. This enables users of a public blockchain system (see Section II-F for more details on public and private blockchains), such as Bitcoin, to remain anonymous. Further, a record of transactions among the peers are stored in a chain of a series of a data structure called *blocks*, hence the name blockchain. Each peer of a blockchain network maintains a copy of this record. Additionally, a consensus, taking into consideration the majority of the network peers, is also established on the state of the blockchain that all the peers of the network store. That is why, at times, blockchain is also referred to as *distributed ledger technology (DLT)*. Each instance of such a DLT, stored at each peer of the network, gets updated at the same time with no provision for retroactive mutations in the records.

B. A clever use of hashing

Now we take a closer look at how hashing is used to *chain* the blocks containing transaction records together and how such records are rendered immutable. A hash is defined as a unidirectional cryptographic function. A hash function usually takes an arbitrary input of an arbitrary length and outputs a seemingly random fixed-length string of characters. Each such output is unique to the input given to this function and can be considered the *footprint* for an input. If the input is even so slightly changed then the output of the hash function almost always completely changes in a random fashion (there are, however, rare occasions where a *collision* occurs when two distinct inputs to a hash function map to the same output) [22]. This way hash of a piece of data can be used to check the integrity of it. As an example Secure Hash Algorithm 256 (SHA256) is a member of the family of SHA2 hash functions which is currently deployed by many blockchain-based systems such as Bitcoin[1].

A simplified version of a blockchain is shown in Figure 1. It can be observed that there are four main fields shown in the figure for each block. In the *hash* field the hash value of all the contents (i.e., block number, *previous hash*, shown as *Prev* in Figure 1, and data) is recorded. The most important field is the *Prev* field. This field, in each block, contains the hash value of the block that comes before it. This chains the blocks together. Now, if the contents of a block are changed then this change is reflected, in addition to the hash of the block under consideration, in the portion of the blockchain that comes after the block being mutated. This way, hashing and the distribution of blockchain copies among the peers of a P2P network makes the records stored in a blockchain immutable. It can be noted in Figure 1 that the first block in a blockchain is sometimes referred to as the *genesis block* indicated by its Prev field initialized to contain all zeros.

C. A coin: Transaction chain

A transaction chain is shown in Figure 2. It should be observed here that there is a difference between a transaction

[1]https://web.archive.org/web/20130526224224/http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384-512.pdf

Papers/Books (Author)	Year	Blockchain Fundamentals	Challenges	Smart Contracts	Blockchain Applications	Future Trends	IoT	Blockchain Types	Blockchain Characteristics	Consensus Algorithms	RegulatoryIssues
Zibin et al. [10]	2016	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗
Ye et al. [11]	2016	✗	✓	✗	✓	✗	✗	✓	✗	✗	✓
Jesse et al. [12]	2016	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗
Marc et al. [13]	2016	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗
Michael et al. [14]	2017	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗
Zibin et al. [15]	2017	✓	✓	✗	✗	✓	✗	✓	✓	✓	✗
Iuon-Chang et al. [16]	2017	✓	✓	✓	✓	✗	✗	✗	✓	✓	✗
Mahdi et al. [17]	2018	✓	✗	✗	✓	✓	✓	✓	✗	✗	✗
Yong et al. [18]	2018	✓	✗	✗	✓	✗	✗	✗	✓	✗	✗
Muhammad et al. [8]	2018	✓	✗	✓	✗	✓	✓	✓	✓	✓	✗
Karl et al. [19]	2018	✗	✗	✓	✓	✗	✓	✓	✓	✗	✗
Salah et al. [20]	2019	✗	✓	✓	✓	✗	✓	✓	✓	✓	✗
Our Survey	2019	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓ (distinguishing feature)

TABLE I: Comparative analysis of our survey with the existing survey literature pool
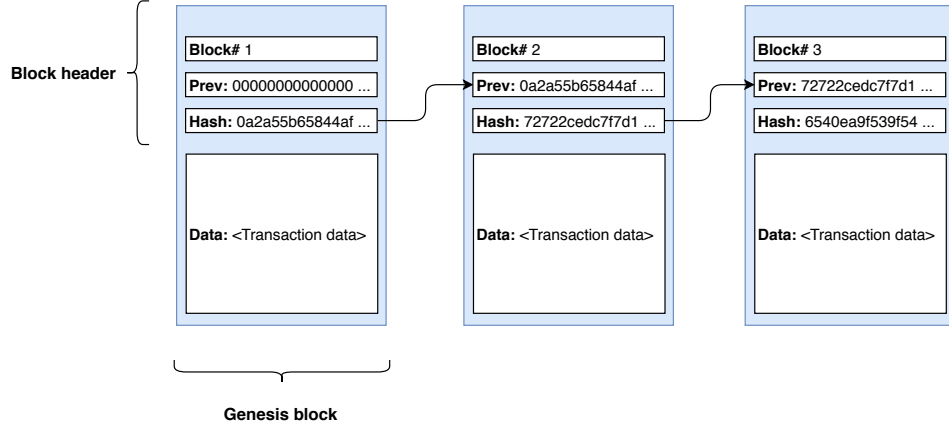

Fig. 1: Hashing chains the blocks together and renders them immutable

chain and a blockchain. Each block in a blockchain can contain multiple transaction chains. Each transaction chain in turn shows the value transferred from one peer of the network to another. Each such transaction chain is also sometimes referred to as a digital *coin* or more generally as a *token* (as an example Ethereum, discussed later, allows one to define a custom token[2]).

D. Distributed consensus

Blockchain systems, such as Bitcoin and Ethereum[3], make use of different consensus engines. These engines enable peers of the blockchain network to have a say about the overall state of the records stored in the blocks of a blockchain network. In this section, we discuss the most popular and widely adopted consensus protocol called Proof-of-Work (PoW). We also briefly discuss Proof-of-Stake (PoS) and Proof-of-Authority (PoA) based consensus engines, which are mostly in development phases but are poised to eventually replace the PoW-based energy-intensive consensus mechanism.

1) Proof-of-Work (PoW): PoW-based consensus mechanism was mainly popularized by Bitcoin [21]. PoW's main goal is to prevent double spending of a digital asset by providing a verifiable trust guarantee to a payee. Such a guarantee is

provided in the form of publishing an integer called a *nonce*. Finding a nonce is a computationally intensive process and is often referred to as *mining*. The peer of a blockchain network that finds a nonce is called a *miner*. Specifically, a nonce is an integer which, when hashed together with the contents of a block, outputs a hash matching a predefined pattern. Depending upon the underlying system, such a pattern is usually defined to start with a predefined number of zeros. The larger the number of leading zeros the harder (in computational terms) it is to find a nonce that hashes to match such a pattern. Any peer node of a blockchain network can perform mining (i.e., collecting a set of transactions and finding the relevant nonce). PoW is a lottery-based consensus mechanism, which implies that in a given large network, the peer who finds a nonce at a given time is decided randomly. Once a miner finds a nonce (or mines a block), the network awards such a node with a set number of *cryptocurrency tokens* (such as bitcoins). This is how cryptocurrency is minted in cryptocurrency networks and is put into circulation in such networks.

As the mining process involves randomness, which implies that it is computationally very hard for an attacker to tamper with the stored data in blockchain if the majority of a network (in terms of computational resources) is honest. However, if an adversary (or a group of adversaries) gains more computational power than the honest portion of the network then it can

[2]https://www.ethereum.org/token
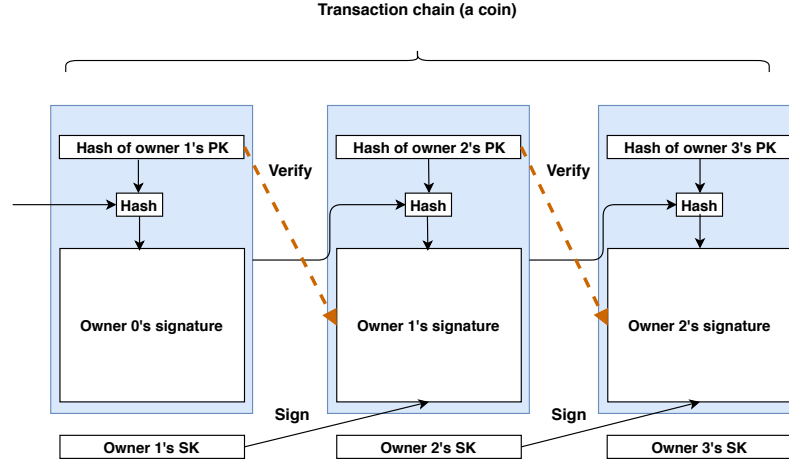[3]https://ethereum.org/

Transaction chain (a coin)

Fig. 2: Transaction chain or a coin. Figure adapted from [21]

potentially alter the records stored in a blockchain. Such an attack is sometimes referred to as a 51% *attack*. Figure 3 shows a chain of blocks with an extra field labeled as nonce. It should be noted in this figure that the hash of all the blocks (apart from the genesis block) starts from a set number of zeros.

2) Proof-of-Stake: Blockchain-based systems, particularly Ethereum[4], are considering to eventually shift to PoS from PoW. This is because of high computation, and in turn high energy, costs associated with finding a nonce through mining.

In the PoS mechanism, the nodes with the largest stake (in monetary terms) in the underlying network will have a greater say when it comes to proposing a block to be appended to a blockchain. The monetary worth owned by such nodes is put at stake in order for them to behave honestly. Since PoS is still in its development phase, it does come with its fair share of issues. Most notable is the mismatch between the actual interest of nodes with the same stake in the underlying network[5].

A variant of PoS is called Proof-of-Authority (PoA) which is mostly being used by the test networks mainly for experimentation (such as Rinkeby and Ropsten Ethereum networks). The idea of PoA is quite similar to PoS: in PoA it is the identity of nodes that is put at stake instead of the monetary value owned by the nodes. This implies that PoA is mostly used to establish permissioned blockchains (see Section II-F) where the identities of the peer nodes are known and they are given specific permissions to mine new blocks.

E. Smart contracts

One important aspect of blockchains is its use in enabling smart contracts [23]. Smart contracts can simply be viewed as algorithmic enforcement of an agreement among, often, mutually non-trusting entities. More technically, a smart contract is a program that executes on blockchain in a distributed manner and possesses unique identification. It contains functions and state variables. These functions receive input parameters of the contract and get invoked when transactions are made.

The values of state variables are dependent on the logic developed in the functions [24]. These functions are normally written in high-level languages (such as Solidity or Python) [25]. Compilers convert these programs into bytecode that is then deployed on blockchain network. These programs are invoked by receiving the user transactions for these smart contracts, which are posted by any user on the blockchain network [24]. Smart contracts help automate an arbitrary value transfer system in an immutable manner where conditional transactions are recorded, executed, and distributed across the blockchain network. These contracts not only reduce the legal and enforcement costs but also largely rule out the need for central trusted or regulating authority [26]. Smart contracts can create an environment of trust among the members of several contrasting and diverse communities [3].

Ethereum[6]: is the signature project that introduced and popularized the concept of smart contracts [27] [28]. It is an open-source, blockchain-based platform that enables one to develop and execute decentralized applications. One of Ethereum's goals is to ease the process of developing the decentralized applications called dApps [29] [30]. Ethereum can be considered as the next step, after Bitcoin, in the evolution of blockchain-based systems. Before Ethereum, most of the blockchain-based system, mainly cryptocurrency-based projects, revolved around expanding on Bitcoin's core protocol and focusing on one specific application. Ethereum, however, generalizes and allows multiple such projects to coexist on a broader underlying blockchain-based compute resource.

Operations on Ethereum are performed by utilizing the Ethereum Virtual Machine (EVM). EVM is the implementation of the Ethereum protocol responsible for handling state transitions and carrying out computation tasks [31]. EVM provides the runtime environment for the execution of smart contracts [24]. The EVM generated binary comprises smart contracts' (usually written in high-level languages such as Solidity[7] or Serpent[8]) opcode that gets deployed on the underlying blockchain.
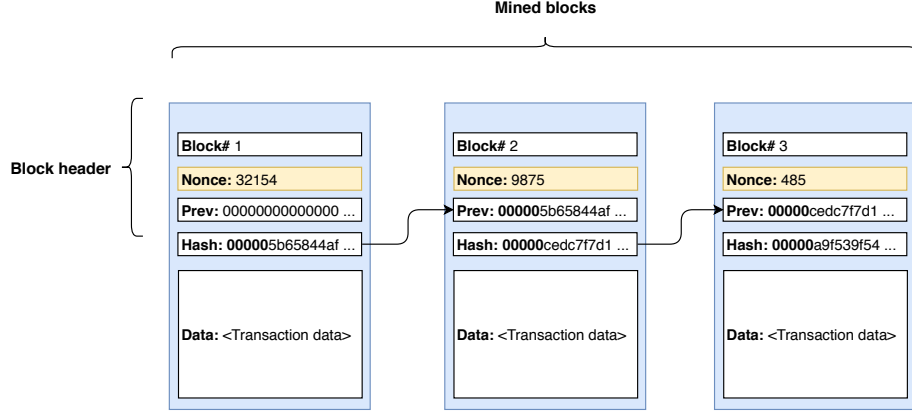
---

[4]https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs
[5]https://tinyurl.com/poa-network

[6]https://ethereum.org/
[7]https://solidity.readthedocs.io/en/develop/
[8]https://github.com/ethereum/wiki/wiki/Serpent

Mined blocks

Block header

| Block# 1 |
| Nonce: 32154 |
| Prev: 00000000000000 ... |
| Hash: 000005b65844af ... |
| Data: <Transaction data> |

| Block# 2 |
| Nonce: 9875 |
| Prev: 000005b65844af ... |
| Hash: 00000cedc7f7d1 ... |
| Data: <Transaction data> |

| Block# 3 |
| Nonce: 485 |
| Prev: 00000cedc7f7d1 ... |
| Hash: 00000a9f539f54 ... |
| Data: <Transaction data> |

Note: *The fields of **Nonce, Prev,** and **Hash** contain arbitrary values*

Fig. 3: Mined blocks in a blockchain. Hash in each block now starts with *five* zeros.

F. Public and private blockchains

The underlying blockchains of Bitcoin, Ethereum and, in general, of most cryptocurrencies are open and public. This implies that anyone can join the blockchain network and transact with any other peer of the network. Moreover, such networks also encourage peers to stay anonymous. As an example in Bitcoin's network, peers are assigned addresses based on the hash of their public keys instead of based on their actual identities.

On the other hand, there are permissioned and private variants of blockchains as well. This concept was particularly popularized by Linux Foundation's Hyperledger Fabric (HLF) platform [9]. This platform is proposed for business use cases where, in addition to data immutability and P2P consensus, transaction confidentiality is also required. Permissioned and private blockchain platforms such as HLF usually deploy a cryptographic membership service on top of their blockchain's immutable record keeping. Each peer in such a network can be uniquely identified based on its real-world identity. Proof-of-Authority (as discussed earlier) functions on the same principle of permissioned and private blockchains.

III. BLOCKCHAIN-BASED NETWORK APPLICATIONS

Other than cryptocurrencies, blockchain finds its applications in various other fields, particularly those that require more transparency and trust in their record-keeping. Some blockchain-based network applications with their platforms are shown in Fig. 4.

A. The Decentralized Internet

The Internet has enabled the evolution of a number of applications such as mobile health, education, e-commerce, online social systems, and digital financial services. However many parts of the world are still deprived of the Internet's boons due to the existence of a digital divide [52]–[55]. Moreover, the existing Internet infrastructure is predominantly centralized creating monopolies in the provision of services to

TABLE II Timeline: Evolution of Blockchain

Year	Event
2018	Blockchains potential got revamped by more investments in wide range of use cases [32]
2017	Seven European banks, announced their program to develop a blockchain-based trade finance platform in collaboration with IBM [33]
2016	Ethereum DAO code was compromised and hacked [34], Emergence of permissioned blockchain solutions [10]
2015	Blockchain trial was initiated by NASDAQ [35], Hyperledger project was started [36]
2014	With crowdfunding the Ethereum Project was started [37], Ethereum genesis block was created [38], [39]
2013	Ethereum, a blockchain-based distributed computing platform was proposed [40]
2012	Coinbase, started as brokerage for Bitcoin [41]
2011	Silk Road launched with Bitcoin as payment method [42], BitPay first Blockchain-based wallet [43], Emergence of other cryptocurrencies like Swiftcoin [44]–[46], Litecoin [47]
2010	First Bitcoin cryptocurrency exchange Mt. Gox started working [48], [49]
2009	First Bitcoin block was created [50], [51]
2008	Bitcoin's whitepaper was published by Satoshi [21]

its users [56], [57]. Distributed denial of service (DDoS) attacks on DNS servers[10], certificate authority compromises (as mentioned in Section III-H), cybersecurity-related incidents [58]–[60] and similar other service disruptions are rife mainly because of the largely centralized nature of the current Internet and the services that it provides [61]. Whereas, the decentralized approach to the online service provisioning gives more control to the users (or the edges of the Internet) and ensures fair participation and sharing of the resources. It is believed that decentralization of the communication infrastructure may

---

[9]https://hyperledger-fabric.readthedocs.io/en/release-1.3/blockchain.html

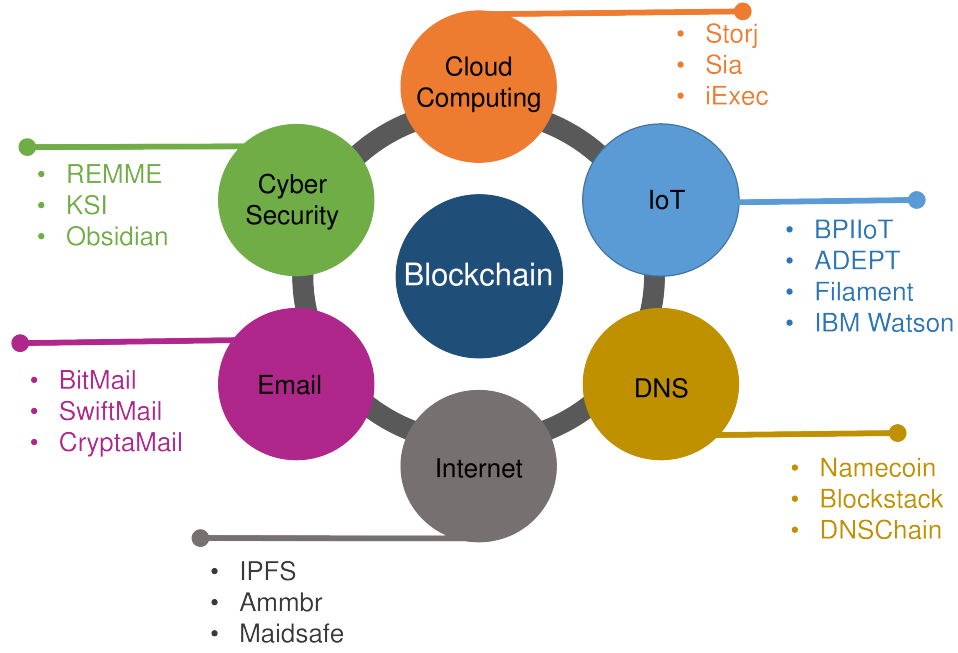[10]https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn

Fig. 4: Examples of blockchain-based network applications and their solutions

bridge the gap of the digital divide and make the Internet services reachable to the remaining unconnected portion of the planet [62].

In this section, we try to re-imagine different components of the Internet through the perspective of Blockchain's premise of decentralization and distributed trust.

1) Decentralized naming systems: Domain name system (DNS) is an example of online namespace system. Its primary goal is to resolve each unique hostname to an IP address(es) and vice versa. Presently, the largely centralized nature of DNS raises the odds for single-point failures and makes such systems prone to malpractice and malicious activities by the main stakeholders and governments. In the past, the seizure of hundreds of domain names by governments or the regulatory institutions have turned scientists, activists, and enthusiasts to think about possible alternatives to this largely centralized namespace system [63]–[67].

Most applications place a demand for a namespace system that can ensure security during the provision of such identifiers. Blockchain can enable a namespace system by making use of global, tamper-resistant, and append-only ledgers and thereby guarantee the integrity, availability, uniqueness, and security of name-value pairs. While some challenges remain to be solved, the blockchain technology can successfully provide the essential basis for the construction and governance of secure and distributed naming services [68]. Such blockchain-based networks further encourage the inclusion of honest network peers since for a sufficiently large blockchain network, it becomes very difficult and costly for the adversarial elements to tinker with the blockchain records [69].

In 2011, an experimental open-source startup called Namecoin came into being providing distributed DNS services based on blockchain technology with the aim of improved security

mechanism, decentralization, confidentiality, and agility [70], [71]. Namecoin is designed to work on top of a blockchain and as an alternative to the existing conventional DNS root servers for the storage of registered domain names [69]. Being a blockchain-based system (with secretly held private keys corresponding to the registered domain names) it is immune to censorship or seizure of the registered domain name accounts. Similarly, any change in domain names, recorded on a blockchain, requires proof-of-work by the longest chain of honest network peers (see Section II-D1 for details), which in turn is in control of the highest computing pool [67], [72].

Another blockchain-based namespace system called Blockstack, inspired by the Namecoin network, improves upon various performance limitations of Namecoin (for a detailed analysis of Namecoin, please see [67]) most importantly security and scalability [69]. The aspect of security was particularly improved by Blockstack by migrating from Namecoin's blockchain to Bitcoin's larger blockchain. The reason being the bigger size of Bitcoin's network, which makes it harder (as compared to Namecoin's relatively smaller network) for a 51% attack [73] (see Section II-D1). One of the distinguishing features of Blockstack system is the introduction of a *virtualchain* [74]. Virtualchain is a logical overlay layer that sits on top of a production blockchain such as Bitcoin. Virtualchain eases the process of modifying the underlying blockchain without requiring actual consensus-breaking changes to it. Blockstack system facilitates users to register unique human-readable usernames and employs the distributed PKI system to bind user identities with arbitrary data values. This new registration system thus functions without the requirement of any centrally trusted third party [61], [69]. Blockstack enables users to own and control their data and access to this data at all times.

2) Routing in the decentralized Internet: The interoperability of many still distinct (and largely isolated and self contained) blockhain networks will pose a problem in future if they are to come together to enable a wide-spread adoption of blockchain-powered decentralized web. There is a need for a routing mechanism that can take into account different characteristics of different blockchain networks and route a transaction from one network to a potentially different one and back. The main problem in inter-blockchain network routing is of verification of blockchain records among different blockchain networks and the provision of communication between any two peers belonging to any two distinct blockchain networks. In a single network this problem gets trivial with all the peers agreeing to follow the same consensus protocol (for example PoW). The motivation to enable interoperability among different blockchain networks can be taken from the concept of a *lightweight client* of a blockchain network. Such clients are able to verify the existence of a record of a transaction in a blockchain network without downloading the entire bulk of blockchain data. The lightweight clients do so by making use of a technique called Simple Payment Verficiation (SPV)[11] [21] which allows a client to verify the existence of a transaction record only by downloading the, comparatively lightweight, block headers, in the form of a Merkle branch, in comparison to the entire blockchain data. Following a similar principle, *Blocknet*[12] proposes a solution for inter-blockchain routing infrastructure [75]. Blocknet achieves interoperability by making use of two main components namely XBridge and XRouter. XBridge is responsible for implementing the *exchange* functionality which implies enabling of atomic swaps of tokens between two blockchains. XRouter on the other hand implements *communication* functionality and in unison with XBridge and making use of SPV a transaction can then be performed between two peers belonging to different blockchain networks.

Another project that proposes a solution to enable cross-ledger payments is called *Interledger*[13] [76]. Interledger presents the concept of *connectors* that act as decentralized exchanges between two distinct blockchain ledgers and route transactions (or *packets of money* as per Interledger's vernacular). Interledger takes its inspiration from IP routing and instead of IP addresses it makes use of an ILP (Interledger packet) address. ILP packets differ from the *best-effort* IP routing in the way that ILP packets can not be lost or stolen since in the case of ILP, funds with real monetary value are transferred instead of data. This is achieved by making use of Hashed Timelock Agreements (HTLA)[14] in combination with SPV to settle cross ledger payment claims. HTLAs work across the ledgers and enable conditional transfers. Conditional transfers involve a *preparation step* whereby a transfer is first prepared which implies that a sender's funds are put on hold by a ledger's contract until a condition is met which manifests itself in the form of a digest of a cryptographic hash function. Its incumbent on a recipient to present this digest in the form

of a *preimage* within a certain time window. If the time expires the funds are automatically released to the sender. This way, by making use of HTLAs the funds can not be lost in transit.

In conclusion, we see the problem of blockchain interoperability as akin to the Border Gateway Protocol's (BGP) routing problem where different Autonomous Systems (ASes) interoperate with each other with a mutually agreed upon control plane information. In our opinion these two problems seem to fit well together. Both domains (i.e., BGP routing and blockchain interoperability) can motivate solutions in each other. As an example, in our opinion, it would be beneficial if BGP attributes such as AS prefixes with corresponding control plane information (such as peering agreements) are stored in an immutable manner in a blocckhain-based database for routing checks. There will, however, be scalability and latency concerns as a blockchain's transaction rate must keep up with the dynamic nature of the changing network topologies in different ASes. Still, storage of network topological graphs with peering agreements will create an opportunity for a more trusted, transparent, and auditable routing decisions with a lesser chance for censorship and collusion.

B. Decentralized Email

Today, electronic mail (email) is a common form of communication among many that usually consists of a mail client and an associated server. There are various protocols such as SMTP, ESMTP, POP, and IMAP for formatting, processing, delivering, and displaying email messages by ensuring interoperability among different mail clients and servers. The security of an email system relies on a continuous process of planning and management. Email messages pass through the non-trusted external networks that are often beyond the control of an email provider's security system. These email messages, without appropriate security safeguards, can potentially be read, modified, and copied at any point along their path [77]. Melissa, Sasser worm and other embedded hyperlinks and viruses have damaged millions of computers and their data [78]. Email solutions (such as Yahoo) have suffered from data breaches in the past and have resultantly urged their users to change their password keys [79]. In order to improve on these centralized email systems to better safeguard the users' private and sensitive information, a radical change in the underlying technology seems imperative.

One of the solutions to address the vulnerabilities of the email system described above can be in the form of a blockchain-powered decentralized and distributed email system. Email addresses, in a similar way to DNS address assignment as discussed in the last section, can be assigned to the users over blockchain technology. In this system, there is no centralized controlling server in order to gain access to personal data and records. Most importantly, email communication using blockchain technology is not under the influence of government authorities that could exploit the centralized email providers such as ISPs and technology giants such as Google, Amazon, and Facebook, etc. John McAfee Swiftmail[15] is a blockchain-based email solution with 256-bit

---

[11]http://docs.electrum.org/en/latest/spv.html

[12]https://blocknet.co/

[13]https://interledger.org/

[14]https://interledger.org/rfcs/0022-hashed-timelock-agreements/

[15]http://johnmcafeeswiftmail.com/

end-to-end encryption for the protection of data. CryptaMail[16] is another blockchain-based email service that claims 100% security based on the decentralized system without third party involvement. Gmelius blockchain architecture is a hybrid system that offers a scalable and cost-effective framework that anchors email associated data into the Ethereum [80].

C. Blockchain for the Internet-of-Things (IoT)

The Internet of Things (IoT) broadly speaking is a network of everyday objects in which the IoT devices capture or generate enormous amounts of data and send it over the network [81]. This interconnection of a large number of IoT devices is known to cause many privacy and security issues [82]–[85]. The IoT-based social, such as health-related, applications often end up monitoring and collecting sensitive personal information. When such information is exposed to third parties, such as health-care providers, the prospects of inadvertent or malicious privacy compromises become highly probable [86]. Compliance with the privacy and security rules and policies for a particular application is a significant challenge in IoT-based systems [87]. In such systems, blockchain-based solutions can help in addressing the issues related to security and privacy. Besides the by-design existence of some implementation constraints of energy, delay, and computation overhead in IoT devices, businesses have started initiatives to use blockchain into their various domains such as in production and supply chain management [88], [89]. For example, the IBM Watson IoT platform[17] empowers the users to put their data on blockchain ledgers, which can later be used in shared transactions among different members of an IoT-related business consortium. This way members of such consortium can take part in verifying transactions against IoT data, dispute resolution, and accountability mechanism in a trusted, transparent, and mutually agreed upon manner. The data collected from devices in an IoT network is formatted into such API formats that are understandable to blockchain smart contracts. The IBM Watson IoT platform enables a business solution to manage, analyze, and customize IoT data, according to a pre-agreed policy, to be shared among permissioned clients, members, and smart contracts [88].

The importance of IoT can be gauged by observing the manufacturing industry, which is increasingly adopting IoT-based solutions for machine diagnostics, manufacturing automation, and health management of industrial machines [24]. Cloud-powered manufacturing systems along with IoT technology help in the provisioning of manufacturing resources to the clients as per the existing demand. This usually requires the involvement of a centrally trusted third party. A blockchain-based platform called Blockchain Platform for Industrial Internet of Things (BPIIoT) is a trustless P2P network where the exchange of services may take place without the need for a central trusted third party [24]. BPIIoT provides a platform for the development of dApps pertaining to P2P manufacturing applications. BPIIoT improves on a similar project called

Slock.it[18], according to the authors of [24], being generic in terms of dApp development. BPIIoT's platform consists of a single-board computer that provides a bridge to both cloud and blockchain services. BPIIoT enables customer-to-machine and machine-to-machine transactions without the involvement of third parties. For more details on the applications of blockchain for the Internet of things (IoT), the interested readers are referred to a comprehensive survey on this topic [8].

Another IoT project, managed by IBM in collaboration with Samsung, is the blockchain-powered and Ethereum-based Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT) system. Ethereum is a blockchain-based generalized technology that can be considered as the compute framework for trustful messaging. Contracts authored under this framework endorse the rules designed for interaction between network nodes and thus are considered more secure. It also provides developers with a platform for building applications integrated with the Ethereum message passing framework [27]. ADEPT realizes a decentralized IoT solution by following the three principles: i) P2P messaging, ii) distributed file sharing, and iii) autonomous coordination among the devices of IoT network. ADEPT makes use of Telehash (an encrypted mesh networking protocol)[19], BitTorrent, and Ethereum respectively to realize the three principles just described. Ethereum's blockchain enables device owners of ADEPT's IoT network to automate rules of engagement, the registration and authentication processes, and interactions among themselves in a decentralized and trusted manner. This can be achieved in one of two ways namely: i) proximity-based: taking into consideration physical, temporal or social distance and ii) consensus-based: taking into consideration selection, validation, or blacklisting criterion [128]–[130].

Among other works is Filament, a blockchain-based technology stack that enables IoT devices to discover, register, manage, and communicate in a decentralized manner [131], [132]. In [133], a system named modum.io[20] has been presented, which utilizes blockchain-based IoT devices to ensure the immutability of the transactions related to physical products and facilitates in the regularization of the supply-chain management process in the various fields.

D. Blockchain-based Content Distribution

Content distribution networks (CDNs) are an effective approach to improve Internet service quality by replicating the content at different strategic geographic locations in the form of data centers. Users can request and access data from the closest replica server instead of always fetching it from the data-originating server. Generally, large companies such as Netflix and Google's YouTube service, have their own dedicated CDNs, while smaller organizations can rent CDN space from other companies like Akamai. BitTorrent is a P2P content distribution protocol that enables the propagation of data using networks of computers for downloading and

---

[16]http://www.cryptamail.com/
[17]ibm.co/2rJWCPC

[18]https://slock.it/landing.html
[19]http://telehash.org
[20]https://modum.io

Scope	Example(s)	Description
Cryptocurrency	Bitcoin, Bcash, Iota, OmiseGO, Litecoin, Ripple, Dash, Zcash, Monero	Decentralized peer-to-peer electronic cash system for online payments.
Smart Contract	Ethereum [27], Ripple [23]	Occurrence of certain events triggers transfers of different things, i.e., security deposit payment, saving wallets, decentralized gambling, wills etc.
Cloud Services	Abuse Prevention [90]	Defence to stop attacks and service abuses in cloud computing applications.
Message Exchange	Bitmessage [91]	Secure system to send and receive messages.
Identity and Privacy	ChainAnchor [92]	Trusted, privacy-preserving, identity management system.
Voting System	Electronic Vote [93]	Electronic vote transaction system for a voter to spend the vote in favor of one or more candidate recipients.
Digital Content	Content Distribution [94]	Decentralized and peer-to-peer digital content management system with rights management mechanism.
Health	Patient Data [95]	Patient data sharing system based on blockchain technology.
Transportation	Vehicle Communication [96]	Secure vehicle to vehicle communication system.
Agriculture	ICT E-Agriculture [97]	Distributed ledger system to safeguarded transparent data management.
Software	Software Connector [98]	Software components states sharing system without trusting a central integration point.
Micro Finance	Stellar [99]	Creates services and financial products using blockchain architecture.
E-Commerce	OpenBazaar [100]	Provides trading platform for users where they can make free transactions among themselves.
Mobile Banking	Atlas [101]	Atlas provides platform for mobile banking and connects world communities through it.
Storage	Sia [102]	A cloud storage platforms, enables anyone to make money.
DNS	Namecoin [103]	A blockchain-based domain name system.
Document Management	Blockcerts [104]	Issue and verify certificates for academic, professional, workforce and civic records.
Storage	BigchainDB, MaidSafe, Filecoin [105] [106] [107]	Scalable storage which supports diverse applications, platforms, industries and use cases.
Business and Economy	IBM Blockchain Platform [108]	Integrated platform designed for creation and acceleration of blockchain based businesses.
Internet of Things (IoT)	IBM Watson IoT [109]	Accountability and security in blockchain-based internet of things.

TABLE III: Examples of blockchain-based applications

Scope	Startups	Description
IoT and Economics	Chronicled [110]	Provides trusted data, ensures data provenance of IoT devices and helps in business process automation
Security and Intelligence	Elliptic [111]	Necessary intelligence information to security agencies and financial departments.
Data Security	LuxTrust [112]	Provides security to customer's electronic data and digital identity.
Regulatory Compliance	GuardTime [113]	Data protection regulatory compliance software.
Financial	Augur [114]	A market forecasting tool to increase profitability.
Transportation	Lazooz [115]	Real-time ridesharing services.
Property Records	Ubiquity [116]	Provide service for secure ownership record of property.
Process Compliance	Startumn [117]	Ensures process integrity and improves regulatory compliance.
Music	Mycelia [118]	Music industry online services.
Asset Management	Gem [119]	Secure identification of assets.
Data Security	Tieriom [120]	Data protection service.
Tracking and Ownership	Provenance [121]	Maintain digital history of things.
Music	Ujo Music [122]	An online music store.
Smart Contracts	SkuChain [123]	Offers services like: Smart contracts, provenance of things, Inventory Management.
Storage	Storj [124]	A distributed storage platform.
E-commerce	Gyft [125]	An online gift transfer platform.
Firearms	BlockSafe [126]	A secure and privacy enabled firearm solution.
Health and Environment	BitGive [127]	By using blockchain technology it works for the improvement of public health and environment worldwide.

TABLE IV: Examples of blockchain-based startups

uploading simultaneously without a central server [134]. Bit-Torrent's network consists of a large number of peers, which complicates the task of traffic management. The other major issue with the current CDNs is that the content creators receive an inadequate share of the revenue, especially in digital content distribution sector [135]. Similarly, the media sector is also significantly suffering because the content can be easily copied and distributed.

Blockchain technology can be the solution with the necessary ingredients to significantly resolve the challenges related to content distribution. It can stabilize the rights management related issues for studios and artists by providing a better way of content control. This can enable a more agile method for content delivery with a more trusted, autonomous, and intelligent network. In a blockchain-based CDN, the participants can independently verify a record and its origin without the need for a centralized authority for verification. Blockchain can store all the record related to the content (e.g., its origin), and share over the network in an immutable form along with the provision of enabling a monetization system to empower the content creators.

DECENT[21], as an example, is a blockchain-based CDN that provides secure content distribution and maintains the reputations of the content creator with a mechanism for the payment between authors and client nodes also in place. Content (e.g., ebooks, videos, and audio) is released cryptographically over the global DECENT network and other nodes can then purchase them with DECENT tokens. SingularDTV[22] is a media industry initiative in which an Ethereum-based entertainment studio is developed that can enable rights management as well as P2P distribution to empower artists and creators.

E. Distributed Cloud Storage

Today, consumers and enterprises face the storage and management problems caused by an ever-increasing volume of data on non-volatile data storage systems. Despite the popularity of cloud storage solutions (such as Dropbox and Google Drive), the control, security, and privacy of data remain major concerns [136]. It is largely due to the current model being adopted by the cloud storage systems that often puts

[21] https://decent.ch/
[22] https://singulardtv.com/

them under a centralized institutional authority. In this model, data is transferred over TCP/IP from a client to the host servers in the legacy client-server model [137]. The information thieves, censorship agencies and spies can potentially tamper with or copy the stored confidential files from hosting servers through technological means, legal tactics and political strategies [138]–[142].

Such problems, mostly caused by central and identifiable points in the current cloud storage systems[23], can potentially be solved using decentralization and (transparent and trusted execution in the form of) automation based on a trust agreement between a client and a host service provider. There exist some storage solutions such as MaidSafe[24] and Tornet[25] that outline possible alternatives for a decentralized cloud, but security, scalability, and cost efficiency of these solutions still remain in question. Therefore, a cloud storage system with trusted and verifiable security guarantees, high redundancy, and scalability, is required that should be economically viable while being practical at the same time. Blockchain-based cloud storage solutions inherit characteristics such as decentralization, anonymity, and trusted execution of transactions among the members of a trust agreement and can pave the way for a verifiable and trusted cloud computing era.

Storj[26] is a blockchain-based P2P distributed data storage platform that enables users to tailor their data sharing and storage as per individual agreements with other network peers and the third party service providers. Entities can earn cryptocurrency-based micro-payments by sharing the unused disk space and Internet bandwidth of their computing devices. In the context of distributed cloud, Dong et al. [143] proposed a game-theoretic, smart-contract-based verifiable cloud-computing framework. This enables the clients to analyze collusion between two different clouds by making them perform the same computing task. In this framework, the users use smart contracts to simulate distrust, tension, and betrayal between the clouds to detect, and in turn, avoid cheating and collusion. Similarly, Sia[27] is another blockchain-based cloud storage platform. Sia platform automates trusted service level agreements (SLAs) between a user and storage provider using smart contracts. It is an open source platform that splits users' data into encrypted fragments and distributes them across a P2P network that increases network resilience and reduces downtime. Unlike the traditional storage solutions, the data in this scheme becomes more secure in the sense that one can only access this data if in possession of associated cryptographic keys. Another important work is Filecoin [144]. Filecoin realizes the concept of distributed storage network in terms of an algorithmic marketplace for storage. Filecoin is built as an incentive layer on top of another distributed file system called Inter-Planetary File System (IPFS). The miners in Filecoin host the storage space with the mining capability determined by the storage capacity a miner possesses. Filecoin enables verifiable markets, which dictates how and where data is written to and read from. Each read/write transaction is powered by the underlying cryptocurrency called Filecoin.

F. Applications in Online Social Networks

The engagement of people with online social networks (OSNs) has increased greatly in recent years [145]. Users often put trust in these OSNs and share their personal details with their online social community. Privacy and security concerns however still remain an issue with many OSNs. Any breach of trust has the potential to detriment a user's virtual and, often in turn, real-world identities [146]. As an example, in one of the biggest data breaches[28], a data firm named Cambridge Analytica got the access to personal information of more than 50 million Facebook (an online social network) users during 2016 US presidential campaign. The firm provided software tools to analyze/predict American voters' behavior/personalities and influenced their choices of the ballot[29].

Decentralization, transparency, and P2P consensus gives blockchain the potential to address most of these aforementioned security and privacy concerns prevalent in OSNs [147]. As an example, a blockchain-based social media platform named "Steem"[30] gives online community an opportunity to have a say on the nature of the content that gets popular on a social network. Steem enables users to earn rewards on the basis of votes received by the community against their contributions [148]. This encourages an honest participation of community peers in maintaining the quality of the overall network. Such OSN systems can further be made self-healing by a blockchain-based "reputation system", such as the one proposed by Dennis et al. [149]. This system keeps records of users' reputation based on their transaction history. In our opinion, such techniques, while not being free of some ethical concerns, greatly reduce the snooping and policing by the centralized authorities such as governments[31].

G. Cybersecurity

A study on cybercrime [150] conducted on some organizations, says that information loss remained the major cost component and increased from 35% in 2015 to 43% in 2017. Blockchains in particular can be a costly target for cyberattacks [151], [152]. As an example, DDoS attacks on a blockchain system can take the form of flooding the network with small transactions. Still such transactions must be paid for (in the units of gas) in order for them to be confirmed by the network [151]. The operations that require very (disproportionately) low gas costs are vulnerable to exploitation by attacker[32]. However, when it comes to the execution of smart contracts then there is a large attack surface area. This is because, often, a set of smart contracts is deployed to automate an application with all of its members working in unison. If one member of

---

[23]https://newsroom.fb.com/news/2018/09/security-update/
[24]https://maidsafe.net
[25]https://github.com/bytemaster/tornet
[26]https://storj.io
[27]https://sia.tech

[28]https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html
[29]https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
[30]https://steem.io
[31]https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
[32]https://www.coindesk.com/so-ethereums-blockchain-is-still-under-attack/

such a set malfunctions it can then trigger a domino effect rendering the whole set malfunction [151]. As an example an ambitious ethereum-based project implemented called decentralized autonomous organization (DAO) got hacked resulting in the theft of about 60M Ether[33]. Such attacks can further be avoided by providing further trust guarantees for the code and logic of the smart contract itself. For instance, Tezos proposes the concept of a *self amending ledger* and to make the deployment of a smart contract more trusted it provides formal proofs of the code of a smart contract in order to secure the trust of all the parties interested in the execution of this smart contact [153].

Based on blockchain technology, REMME[34] is a password authentication system for safeguarding the confidential credential information from cyberattacks and at the same time disregarding the need to remember passwords [154].

Estonian cryptographer Ahto Buldas co-founded an information security company named Guardtime[35] in 2007. This company has been working to secure sensitive records using blockchain technology. The company has designed a Keyless Signature Infrastructure (KSI) [155] against the commonly used Public Key Infrastructure (PKI). In this new infrastructure, centralized Certificate Authority (CA) uses asymmetric encryption and manages public keys. Thus helping in reducing the risk of informational asset loss from cybersecurity-related incidents.

Obsidian[36] is also blockchain technology based platform for secure message exchange without any provisioning of centralized management mechanism. In this system, the metadata about the undergoing communications is spread out in distributed ledgers and cannot be collected at centralized locations. Hence, in the context of cybersecurity, it decreases the chance of surveillance or tracking and in this way addresses privacy issues [156].

H. Public Key Infrastructure (PKI): Certificate Authority (CA)

Public Key Infrastructure (PKI) establishes a link between identities like domain names to a cryptographic public key with help of certificates [157]. Among traditional approaches to PKIs, the most common choice is the use of Certificate Authority (CA) that serves as a trusted third party and manages the distribution digital certificates over the network. This creates a single point of failure in such PKIs in practice [158]. There have been many incidents when these centralized CA's have been compromised—e.g., the DigiNotar attack: 531 fraudulent certificates issued [159] [160]; Trustwave's issuance of digital "skeleton key" for surveillance [161]; Debian's predictable random number generator in the OpenSSL package [162]; Stuxnet malware: compromise on code-signing certificates [163] [164]; Duqu malware: stealing of digital certificates along with the private keys [165]–[168]; and the console hacking of Playstation 3 with compromised private keys [169].

Developing a blockchain-based PKI is a feasible alternative to the existing PKIs, which can provide the required security properties [170]. In a blockchain-based implementation of the PKI system, the user identities are bound to public-keys using distributed public ledgers [69]. A blockchain-based decentralized PKI system called "CertCoin" for secure identity management and retention has been in use. This system trusts the majority of peer network users instead of any central trusted party. It has two different mechanisms for verification of the known public key and the lookup for a new public key, which are supported by decentralized efficient data structures [158]. In [171], another blockchain-based distributed PKI scheme has been proposed that resolves the single point failure issue. This scheme ensures validity and ownership consistency of public-key certificates by miner's proof-of-work. It uses Merkle Patricia tree (see for details [172]) for efficient accessibility of certificates without relying on any central trusted third party. Similarly other blockchain-based PKIs have been discussed in [173]–[176].

I. Other Applications

Using the blockchain technology, a company named Factom has started a land registration project with the Government of Honduras to ensure integrity and correctness of the information. Using the same technology, they have engaged in projects related to smart cities, document verification, and the finance industry [177].

In another application, a blockchain-based startup Everledger is working on bringing transparency to the supply chain of diamonds, which was previously perceived as complex, risky and prone to carrying false and incomplete information. Everledger has been designed to reduce fraudulent modifications in the records to help financial institutions, businesses, and insurance companies with actual details of information [178].

A bitcoin-based startup Abra for transferring money to anyone with minimal charges of transaction. No intermediate party gets involved in this transaction [179]. Blockchain is being considered as a novel software connector, which can provide a decentralized alternative to existing centralized systems resulting in quality attributes. For example, Xu et al. [98] found that blockchain can improve information transparency and traceability as a software connector.

Openchain[37] is a distributed ledger based system, which helps in the management of digital assets while ensuring their robustness, security, and scalability. AKASHA[38] provides people with a platform to publish and share their content online. Participants of this system get rewarded for their content based on the votes against their entries.

OpenBazaar[39] is a blockchain-based platform, which facilitates people to make transactions freely among themselves. Users of this system cannot censor the transactions or freeze the payments. Users also enjoy the flexibility of sharing information as much as they want. However, the buyers and

---

[33]https://tinyurl.com/DAOattack
[34]https://www.remme.io
[35]https://guardtime.com
[36]https://obsidianplatform.com

[37]https://www.openchain.org
[38]https://akasha.world
[39]https://www.openbazaar.org

sellers can engage intermediate moderators to resolve any dispute that may arise between the involved parties [99].

IV. CHALLENGES AND THE ROAD AHEAD

The blockchain is expected to drive economic changes on a global scale by revolutionizing industry and commerce by redefining how digital trust mechanisms through distributed consensus mechanisms and transparent tamper-evident record-keeping. The disruption of blockchain is evident, and people are beginning to adopt this distributed ledger technology. There are, however, various hurdles that are slowing down the rate of blockchain's adoption. Some of these challenges are discussed below and with pointers to how these challenges might find a solution in the future.

A. Governance, Operational & Regulatory Issues

Blockchain has great potential to enable efficient and secure real-time transactions across a large number of industries by providing financial services visibility along a supply chain and streamlining government authorities and consumers. Blockchain technology is still far from being adopted en masse due to some unsolved challenges of standards and regulation. Although its hard to regulate the development of the blockchain technology itself, blockchain-based activities (such as financial services, smart contract, etc.) should be regulated [180]. To support its emergence and commercial implementation, the development of standards and regulations are required to establish market confidence and trust. These regulations can also be used for law enforcement to monitor fraudulent activities e.g., money laundering.

In May 2016, a complex set of smart contracts named Decentralized Autonomous Organization (DAO) was built on top of Ethereum blockchain. It was a crowd-funding platform for defining organization rules[40]. After this smart contract's creation, there was a period of funding during which users could earn its restrictive ownership by purchasing Ether (i.e., the underlying cryptocurrecy). After the completion of that funding period, the DAO started its operation in which the restrictive owners (also called members) casted their votes for the usage of collected funds. Initially, this operation was very successful and raised over $150M from 11,000 members within a one month duration [181]. In June 2016, almost $70M were drained after a hack making use of a recursive call exploit. The hackers used this exploit to get Ether back from DAO repeatedly before its actual balance update[41]. Another such incident happened in May 2017, when the WannaCry ransomware cyberattack targeted computers, encrypted their data and demanded the ransom money in cryptocurrency. In total, an amount higher than £108,000 was paid in Bitcoin cryptocurrency by the victims. The impact of this cyberattack was reportedly seen in 150 countries worldwide[42].

If blockchain is to get widely adopted, centralized regulatory agencies, such as governmental agencies and multinational corporations, may be unable to control and shape the activities based on blockchain technology [182]. Because blockchain has no specific location and each node may subject to a different geographic jurisdiction and therefore different applicable laws and legal requirements. There is no central administration for each distributed ledger, therefore, territorial regulations constitute a problem [183]. As a result, there is an increased need to focus on the regulation of this cross-border nature of technology.

In the *Roadmap for Blockchain Standards Report* [184], it has been emphasized that there is a need to establish international standards regarding blockchain terminology, interoperability (between blockchain systems), user privacy, security, user identity, governance and risk related issues so that people's confidence in blockchain-based businesses may be developed. The report has further highlighted the need for collaboration among committees and experts in order to further strengthen the regulated use of the blockchain technology.

In [185], it has been described that there are many interpretations of the blockchain technology in literature and formal blockchain terminologies are yet to be defined, i.e., permissioned blockchains vs. private distributed ledgers are few of those used interchangeably. In this [186] literature, the importance of standards in paving the way for interoperability between multiple blockchain platforms and applications, have been discussed. The author is of the view that developing such standards for ensuring interoperability can help in minimizing the risk of fragmented blockchain systems.

At first, the organizations who have been governing the Internet, considered blockchain technologies as beyond their scope but this opinion changed later [187]. The World Wide Web Consortium (W3C) has been discussing online payments by utilizing the blockchain's potential[43]. The Internet Governance Forum (IGF) has been arranging sessions on blockchain technology to devise a distributed governance framework[44]. The Her Majesty's Revenue and Customs (HMRC) issued a policy paper describing the tax treatment for the income earned from Bitcoin (blockchain-based cryptocurrency) and other cryptocurrencies-related activities [188]. The Financial Crimes Enforcement Network (FinCEN) has recommended that decentralized currencies should follow the money laundering regulations [189] [190].

The European Securities Market Authority (ESMA) has issued a paper [191] in which the benefits and risks of the blockchain technology in securities markets have been discussed. The UK Treasury has issued a report [192], which has emphasized the need for Government to make efforts for the necessary regulatory framework in parallel to new blockchain-based developments. Moreover, other US regulatory authorities and agencies like Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC), Internal Revenue Service (IRS) and Federal Trade Commission (FTC) have been working to make regulations

---

[40]https://www.coindesk.com/understanding-dao-hack-journalists
[41]https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork
[42]https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs

[43]https://goo.gl/NjVLri
[44]https://goo.gl/9pPeiQ

pertaining to blockchain-based businesses and applications [30].

1) Blockchain and GDPR: The European General Data Protection Regulation (GDPR) was adopted in 2016 by the European Parliament and the European Council [193]. Since then, two years were given to the businesses to prepare themselves to comply with the regulation. In this section, we discuss where does the compliance with GDPR put the blockchain technology? Will the original premise of decentralization and immutability be able to sustain under the GDPR ramifications particularly when we consider the *right to be forgotten* clause of GDPR? In what follows we first provide a brief overview of the GDPR, the duties it puts on businesses, the rights it gives to the users', and finally what are its ramifications on the blockchain technology in general?

After its legislation, the GDPR came into effect on May 25, 2018, and is applicable to any kind of information that can be associated with an either identified or identifiable living person[45]. Some of the examples of identifiable information include names, unique code number, IP address, single or multiple identifying characteristics. Further, GDPR applies throughout the lifecycle of personal data i.e., from data collection, to data processing through to the ultimate disposal of this data. GDPR-compliant businesses are bound to collect only data for the clearly stated purposes and process it with the users' consent. After the use of personal data for the said purpose, according to GDPR, the businesses are incumbent to delete the personal information from their local storage. However, this excludes data pertaining to a deceased person and processing of such data is at the disposal of local policies in place at a particular geographic region [193].

GDPR gives users certain rights when they interact with businesses which provide a service based on their personal data collection and processing. These rights include:

1) **Awareness:** This entails that the users' must be informed about how their personal data will be used;
2) **Access:** The users must be able to access copies of their data collected by a business or a service provider free of charge;
3) **Correction:** If a user finds some inaccuracies in her data held by a company then she must be able to flag it as disputed;
4) **Deletion:** A user must be able to make a company delete all the information pertaining to her whenever she chooses. (This right is sometimes referred to as the *right to be forgotten*);
5) **Restriction:** If a user is in a process of assessing the accurateness of her data use she must be able to restrict the access to her data during the process;
6) **Objection:** A user must be able to object to the uses of her data if she disagrees with some of the automated decisions involving her (such as marketing ads or shopping recommendations).

It can be observed that many of these rights seem to fit quite well with the blockchain's premise of decentralization,

tamper-evident record keeping, transparency, and auditability. There are however a few nuances which we discuss next.

There are two important terms that GDPR defines namely *data controller* and *data processor* which require special attention when dealing with blockchain-based projects. Both of these entities take part in users' personal data processing with their specific consent. There is, however, a nuance in the way these two entities function. Controller is an entity which sets the purposes and means for data processing. Controllers can take the shape of a natural or legal person, authority, or an agency. Data processors, on the other hand, is similarly a natural or legal person, authority, or an agency that processes personal data on a controller's behalf strictly following the rules specified by the corresponding controller. There should also be an agreement between a controller and a processor clearly defining their roles and functions [194]. Given the users' rights, as mentioned above, one of the underlying principles of GDPR is auditability which provides the provision to hold the process and the entities involved in personal data processing accountable for their responsibilities, functions, and actions[46]. In the decentralized environment of blockchain the important issue is related to specifying who gets to be a data controller and who a processor [194], [195].

In terms of blockchain, we consider a number of scenarios (self open, self private, open, private, consensus protocols) to answer the questions related to deciding the roles of controllers and processors. First, an entity (a business for instance) can choose to make use of the open and permissionless blockchain. In this scenario, such an entity can potentially write the core blockchain protocol and make it open source. Further, such entities can also deploy a set of smart contracts defining data processing rules and interactions among nodes of the network. We conjecture that this way such an entity can assume the role of data controller. Further, anyone can download the client software and become a node in the overall blockchain's P2P network. It has been a common practice that the open and public blockchains make use of PoW-based consensus mechanism. This implies that any node in the network can process transactions and validate them by including them in a mined block and ultimately appending that block to the overall blockchain. As we discussed earlier that PoW-based mining is a lottery-based process which means that it is a random event that a node in a network finds a nonce hence mining and ultimately appending this block to the blockchain. In this scenario, it is not a trivial task to decide who is the processor. Since potentially all the nodes in such a PoW-based network process data at the same time. We conjecture, either the whole network should be considered as a processor or the responsibility of being a processor should be weighted as per the processing power of either individual nodes or pool of such nodes (which are sometimes referred to as mining pools).

The second scenario is of private and permissioned blockchain. In this scenario, a number of entities can come together to form a consortium and then automate the dynamics of such a consortium using a permissioned version of

---

[45]https://gdpr-info.eu/art-4-gdpr/

[46]https://thenextweb.com/syndication/2018/07/26/gdpr-blockchain-cryptocurrency/

blockchain. In this setup the entities can make use of a PoA-based consensus mechanism or Hyperledger's channel-based permissioned blockchain [47]. Further, such entities can rent storage and computational resources from a third party cloud provider and hence rendering them as data processors. On the other hand, the consortium as a whole can assume the role of a data controller. Again, we conjecture, if the consortium makes use of a consensus mechanism such as PoS then as far as accountability is concerned then each node can be held accountable according to the stake value that such node holds in the overall network.

2) Right to be forgotten: Although many of the principles outlined in GDPR such as data auditability fit quite well with blockchain's premise, the main bone of contention, however, in the way of making blockchain-based decentralized solutions in compliance with GDPR is the so called *right to be forgotten*. This right dictates that a user must be able to instruct a business at any time to remove personal data pertaining to her. Further, as discussed above, the businesses are incumbent to delete personal data after a set duration of time. This right seems at odds with the blockchain's data integrity guarantees. The situation gets worse as blockchain-based solutions are usually distributed with multiple copies of the records stored at different nodes of the network.

As paradoxical as deletion and integrity seem at first glance there are, however, proposals to reconcile these two seemingly opposing principles[48]. One of the solutions could be to encrypt each data entry in blockchain with a key pair and only store the ciphertext on a blockchain. This way deletion can be achieved by simply deleting the corresponding private key while still preserving the ciphertext on blockchain. In some geographical jurisdictions (such as in Britain[49]) the interpretation of GDPR does recognize such methods of digital deletion. However, such techniques do not provide a future-proof guarantee since with the advent of new and faster technologies and techniques such as quantum computing, such encryption methods pose a risk for future data breaches[50].

Another proposal is to only store hashes of data on blockchain while storing the actual data in an off-chain storage. This way the deletion can be achieved by deleting the off-chain stored record while keeping the hash of it intact on blockchain. An argument against this technique is that the hash of a blob of data can still qualify as personal data since if an entity possesses this blob then she can easily reconstruct the hash and decipher what was stored on blockchain in the first place. To get around this problem, we can use *hash peppering* whereby a random and secretly kept nonce is appended to the blob of data before taking its hash and storing it on blockchain. This, however, implies keeping the nonces well protected and secret and does imply some level of trust on third parties that are responsible for peppered hashing of data.

Another way can be to make use of a technique similar to the way *channels* are implemented in Hyperledger Fabric[51]. Channels can be understood as confidential and permissioned islands of smaller blockchain instances on top of a larger blockchain infrastructure. A blockchain instance pertaining to a channel can be audited in the same way a public and open blockchain opens itself to auditing. However, the actual contents of transactional records are encrypted and one can not decipher the nature of the business being automated in a channel's instance of blockchain. This way by deleting the cryptographic information related to such a channel the whole instance of the corresponding blockchain can be rendered redundant.

B. Scalability Issues

Scalability is one of the major concerns in the way of wide spread adoption of blockchain-based technological solutions. We discuss this concern with following three different perspectives.

1) Transaction throughput: Although the Bitcoin is a popular blockchain-based global cryptocurrency, scaling it to handle the large transaction volumes worldwide raises some concerns. Among other things, the transaction processing rate of Bitcoin is affected by (1) the available network bandwidth, and (2) the network delay affects. Miners with high bandwidth and with less network delay can broadcast their blocks among peer nodes with ease and speed, while on the other hand low bandwidth miners with limited computational resources possess less probability of getting their fair share in a successful execution of proof-of-work [196].

Bitcoin has seen an increasing interest, which has raised questions about its scalability. Scalability was one of the reasons that led to the creation of Bitcoin Cash[52]; a forked version of Bitcoin but with a larger block size to allow more transactions per block.

The blockchain-based systems are usually self-managed and accept transaction blocks after approximate intervals of time. The throughputs of these transactions are mainly based on block interval and maximum block size [197]. It has been predicted that if the blocks size were to continue to grow at the same rate then it might attain a value close to its maximum capacity level by 2017 and this could be a significant scalability concern [198].

Increasing the block size does imply a higher transaction throughput, however, this will also mean that the larger blocks would require more time to reach to the peer nodes of the network resulting in higher latency when it comes to proposing new blocks or reaching consensus on the state of a blockchain. On the other hand, the latency would decrease with decreased block interval but at the cost of potential disagreement in the system [199]. Similarly, other consensus protocols such as PoS-based consensus (as meniotned in Section II-D2) are in development phase which are aimed to addressed the scalability and energy concerns.

---

[47]https://hyperledger-fabric.readthedocs.io/en/release-1.3/channels.html

[48]https://thenextweb.com/syndication/2018/07/26/gdpr-blockchain-cryptocurrency/

[49]https://bit.ly/1VBf6Y8

[50]https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf

[51]https://hyperledger-fabric.readthedocs.io/en/release-1.3/channels.html

[52]https://www.investopedia.com/tech/bitcoin-vs-bitcoin-cash-whats-difference/

2) Storage: In addition to the block size scalability concern, the storage capacity of peer nodes is another issue. The transaction rate has a direct relation with the storage capacity of the participating nodes. With more nodes joining the network, the transaction rate would likely be higher and will require more storage space on the peer nodes, which might be seen as a limitation from the perspective of the consumers [200].

It has been identified that blockchain technology is not limited to cryptocurrencies, but there are various blockchain-based prototype applications that are being used in domains such as IoT, Botnet, P2P broadcast protocols, smart property, and others. This shows the potential of blockchain technology for various other industries. Currently, the size of blockchain-based applications, in terms of their user base, is relatively small. Bitcoin is the largest solution based on the blockchain, but the transaction rate in bitcoin's network in comparison to the traditional digital payment solutions is considerably lower. However, in future, blockchain-based solutions could be used by millions or trillions of individuals and the number of transactions would increase drastically. Because of the distributed storage characteristic inherent in blockchains, it will put increasing pressure on storage nodes, which could result in increased synchronization delay, power consumption, and server costs. We believe that more research is required in order to address these these scalability issues.

3) The Lightning Network and Sharding: The scalability issue can, up to some extent, be addressed by distributing the transaction execution process into multiple steps. To ensure scalability, the execution of transactions can be performed outside the blockchain, whereas the validation should take place within the blockchain network. This would decrease the transaction confirmation time. For example, the Lightning Network is able to perform 45000 transactions per second by executing the transactions outside the blockchain [201].

Another possible solution could be a decentralized database that can be used by both public and private blockchain and deploying sharding (which implies horizontal partitioning of records given large databases) and then merging the shardes at regular intervals[53] [202], [203]. A decentralized database would be able to process millions of writes per second with the storage capacity of petabytes and latency in sub-seconds. This will also allow more nodes to be added to the platform, which would increase the performance and make the capacity scalabile.

C. Security and Privacy Concerns

Besides security being in the system by design of the blockchain-based transactions, privacy remains a concern in applications and platforms [204]. The blockchain technology has been considered as privacy-preserver and rated well in this context [205] [206] [207]. However, third-party web trackers have been observed deanonymizing users of cryptocurrencies. These trackers fetch user's identity and purchase information from shopping websites to be used for advertisement and analysis purpose. Normally, these trackers have sufficient

---

[53]https://medium.com/edchain/what-is-sharding-in-blockchain-8afd9ed4cff0

information required to uniquely identify the blockchain-based transaction along with user's identity [208].

It has been widely believed that blockchain is safe as its transactions are executed with generated addresses instead of real identities [10]. Besides this, in [209] [28], it has been shown that the blockchain transactions do not ensure privacy since the transaction balances and values against public key(s) remain available for all.

In addition to the privacy-related issues, there are some security concerns related to blockchain technology. There are certain scenarios that may affect the expected behavior of the blockchain system. Consider the case where a miner-A successfully generates two blocks but does not disclose it to the peer honest network nodes, instead withholds these. We may call these as secret/hidden or private blocks. The miner-A releases these secret blocks when some honest nodes complete mining of a new block (say grey block). After the release of secret blocks, the miner-A successfully adds his two secret blocks in the blockchain network (since the miner-A holds the the longest chain of honest network nodes), whereas the newly added grey block does not remain a part of honest blockchain because the grey block does not hold the longest chain of honest network nodes [210] [211]. This type of attack is called selfish mining attack (see Figure 5) and this results in the undermining of the fair share of the block mining rewards

51% attack [12], [212], [213] is another type of attack on blockchain systems. In this attack, a miner having more than half (i.e, 51%) of network node's computational resources dominates the blockchain system in terms of transaction generation, approval, and verification and thus paves the way for fraudulent transactions generation [214].

D. Sustainability Issues

Blockchain has attained an extraordinary amount of interest and attention and a large number of industries are adopting this virtual digital ledger. However, it is still unclear that any particular solution of blockchain can attain a certain level of adoption for their sustainability. As a new technology, blockchain still facing operational, technical and its adoption-related issues. Similarly, there are also some aspects of blockchain technology that may need further modification or development to attain its anticipated potential. For example, although blockchain does provide a reliable cryptocurrency mechanism, it also adds latency to the network since the verification of the transaction requires consensus, which requires a certain amount of computation and a certain amount of time.

The sustainability of blockchain is still uncertain for international development projects, especially in developing countries. These projects require a very large infrastructure and involve various stakeholders, cross-border organizations, governments, and public or private parties. In these scenarios, the practicality of blockchain is unclear and it is the time to explore how blockchain will facilitate and sustain in such projects. Therefore, sustainability scientists and blockchain developers must discuss problems and solutions. More research is needed to find energy efficient approaches for Bitcoin mining. Behavioral and psychological research is required to
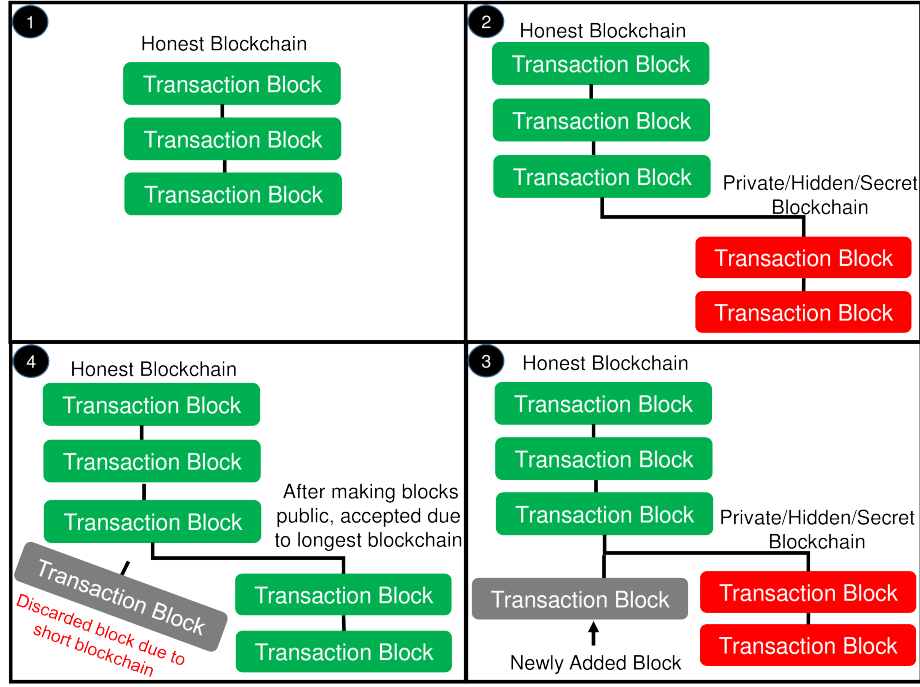
Fig. 5: Workflow of selfish mining attack

F. Use of Artificial Intelligence and Machine Learning

Recent advancements in blockchain technology are making new ways for the involvement of AI and machine learning (ML) that can help to solve many challenges of blockchain with several important future applications. Blockchains is a technology that is being used to verify, execute and record the transaction. AI can help in understanding, recognizing, assessment decision making in the blockchain. Whereas ML techniques could help to find ways to improve decision making and smart contracts. For instance, AI can help to build an intelligent oracle without the control of the third party. This would learn and train itself to make the smart contract smarter [10]. The integration of AI and ML with blockchain will potentially create a new paradigm by accelerating the analysis enormous amount of data. Examples include automation of tokens creation, recommender systems, security enhancement, etc.

1) Use of Big Data Analytics: Recently, many companies are focusing to adopt the blockchain technology in their frameworks. This is creating new types of data for analysis by the powerful tools of big data. There are a huge number of blocks—increasing rapidly and constantly throughout the globe. Each block is full of information (i.e., details of every financial transaction) that can be used for analysis to explore thousands of patterns and trends. The blockchain is a technology that provides integrity, but not analysis. By using big data, it will be possible to detect nefarious users with whom business would be dangerous. Big data can also provide real-time fraud detection based on the users' records and history. The risky transactions or malicious users can be detected quickly by using big data analytics. This will result in cost reduction for real-time transaction [218]. Further, user

attain people's trust in technology for cryptography. Most importantly, lawyers and programmers must collaborate to formulate smart contracts and dictionaries will be necessary that connect computer codes and legal languages.

E. Anonymity

In a blockchain system, the users utilize generated addresses, which are mostly in the form of public keys, for their unique identification over the blockchain network. The blockchain users can generate their multiple addresses in order to avoid the revelation of their real identities. These addresses are generated in the form of cryptographic keys. The said keys are then used to send and receive blockchain based transactions [215].

Moreover, there is no central storage system for preserving the user's private identification details in the blockchain network. By this way, the privacy in blockchain system is maintained up-to certain extent, however, the user's privacy protection is not guaranteed since the transaction amount details and the blockchain-based cryptographic keys (i.e., used for user identification) along with their respective balances, are publicly visible [10].

The blockchain-based applications still do not completely guarantee the preservation of transactional anonymity. The transactional transparency is impacted due to the lack of strong anonymity support for the end users [206]. In [209], the author showed that the movements of blockchain-based transactions are traceable and thus do not possess enough anonymity [216]. Few other anonymity tracing techniques are discussed in [217] [48].

trading patterns can also be used to predict trading behaviors and potential partners for trade with the help of big data analytics [10]. A good resource to conduct big data analysis on (real-time updated) data related to Ethereum and Bitcoin's blockchain is by using Google's BigQuery[54],[55]. For more details on the applications of blockchain for enabling AI, the interested readers are referred to a comprehensive survey on this topic [20].

G. Usability and Key Management

One of the primary challenges that any new technology faces is the usability. This issue is more acute in blockchain because of new architecture and high stakes. The transaction flow should be visible to users to analyze the whole transaction flows. This will improve the usability and help the individuals to understand and analyze the whole blockchain network [12]. There are some systems such as Bitconeview [219] and Bitiodine [220] that proved to be very effective for the detection and analysis of blockchain-related patterns. These systems also help to improve security and privacy-related concerns.

It has also been reported in the challenges and limitations of blockchain that the bitcoin API is difficult to use for the developments [3]. Bitcoin users have to deal with public key cryptography that differs from the password-based authentication system. The usability of bitcoin key management also presents fundamental challenges for end users [221]. This requires more research in the future to provide more ease to the end users and the developers.

V. CONCLUSION

In this paper, we provide a study on blockchain-based network applications, discuss their applicability, sustainability and scalability challenges. We also discuss some of the most prevalent and important legal ramifications of working with blockchain-based solutions. Additionally, this paper suggests some future directions that will be helpful to support sustainable blockchain-based solutions. At the time of writing, we believe that, blockchain is still in its infancy implying there will be sometime spent before it gets ubiquitous and widely adopted. However, the aim of this study is to provide a guiding reference manual in a generic form to both the researches and practitioners of the filed so that a more informed decision can be made either for conducting similar research or designing a blockchain-based solution.

REFERENCES

[1] Muneeb Ali. *Trust-to-trust design of a new Internet*. PhD thesis, Princeton University, 2017.

[2] Elyes Ben Hamida, Kei Leo Brousmiche, Hugo Levard, and Eric Thea. Blockchain for enterprise: Overview, opportunities and challenges. *ICWMC 2017*, page 91, 2017.

[3] Melanie Swan. *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc., 2015.

[4] Taketoshi Mori. Financial technology: blockchain and securities settlement. *Journal of Securities Operations & Custody*, 8(3):208–227, 2016.

[5] Don Tapscott and Alex Tapscott. Realizing the potential of blockchain: A multi stakeholder approach to the stewardship of blockchain and cryptocurrencies. http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf. (Accessed on 06-Oct-2018).

[6] Gareth W Peters and Efstathios Panayi. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In *Banking Beyond Banks and Money*, pages 239–278. Springer, 2016.

[7] Nadeem Badshah. Facebook to contact 87 million users affected by data breach. https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach, April 2018. (Accessed on 06-Oct-2018).

[8] Muhammad Salek Ali, Massimo Vecchio, Miguel Pincheira, Koustabh Dolui, Fabio Antonelli, and Mubashir Husain Rehmani. Applications of blockchains in the internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 2018.

[9] Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee, Abdelouahid Derhab, Leandros Maglaras, and Helge Janicke. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet of Things Journal*, 2018.

[10] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, and Huaimin Wang. Blockchain challenges and opportunities: A survey. *Work Paper*, 2016.

[11] Ye Guo and Chen Liang. Blockchain application and outlook in the banking industry. *Financial Innovation*, 2(1):24, 2016.

[12] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. Where is current research on blockchain technology?—a systematic review. *PloS one*, 11(10):e0163477, 2016.

[13] Marc Pilkington. 11 blockchain technology: principles and applications. *Research handbook on digital transformations*, page 225, 2016.

[14] Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. Blockchain. *Business & Information Systems Engineering*, 59(3):183–187, 2017.

[15] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *Big Data (BigData Congress), 2017 IEEE International Congress on*, pages 557–564. IEEE, 2017.

[16] Iuon-Chang Lin and Tzu-Chun Liao. A survey of blockchain security issues and challenges. *IJ Network Security*, 19(5):653–659, 2017.

[17] Mahdi H Miraz and Maaruf Ali. Applications of blockchain technology beyond cryptocurrency. *arXiv preprint arXiv:1801.03528*, 2018.

[18] Yong Yuan and Fei-Yue Wang. Blockchain and cryptocurrencies: Model, techniques, and applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 48(9):1421–1428, 2018.

[19] Karl Wüst and Arthur Gervais. Do you need a blockchain? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 45–54. IEEE, 2018.

[20] K. Salah, M. H. Rehman, N. Nizamuddin, and A. Al-Fuqaha. Blockchain for AI: Review and open research challenges. *IEEE Access*, pages 1–1, 2019.

[21] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[22] Phillip Rogaway and Thomas Shrimpton. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In *International workshop on fast software encryption*, pages 371–388. Springer, 2004.

[23] Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. Making smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 254–269. ACM, 2016.

[24] Arshdeep Bahga and Vijay K Madisetti. Blockchain platform for industrial Internet of Things. *J. Softw. Eng. Appl*, 9(10):533, 2016.

[25] Solidity solidity 0.4.20 documentation.

[26] Dylan Bargar. *The Economics of the Blockchain: A study of its engineering and transaction services marketplace*. PhD thesis, Clemson University, 2016.

[27] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151:1–32, 2014.

[28] Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *IEEE Symposium on Security and Privacy (SP), 2016*, pages 839–858. IEEE, 2016.

[29] Ethereum community. Ethereum homestead documentation. https://goo.gl/gNJuqz, March 2017. (Accessed on 06-Oct-2018).

---

[54]https://cloud.google.com/blog/products/gcp/bitcoin-in-bigquery-blockchain-analytics-on-public-data

[55]https://cloud.google.com/blog/products/data-analytics/ethereum-bigquery-public-dataset-smart-contract-analytics

[30] Hossein Kakavand and Nicolette Kost De Sevres. The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies. 2016.

[31] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. *White Paper*, 2014.

[32] us-fsi-2018-global-blockchain-survey-report.pdf. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-2018-global-blockchain-survey-report.pdf. (Accessed on 12/17/2018).

[33] Ibm news room - 2017-06-26 seven major european banks select ibm to bring blockchain-based trade finance to small and medium enterprises - united states. https://www-03.ibm.com/press/us/en/pressrelease/52706.wss. (Accessed on 12/04/2018).

[34] Sergei Tikhomirov. Ethereum: state of knowledge and research perspectives. In *International Symposium on Foundations and Practice of Security*, pages 206–221. Springer, 2017.

[35] Huasheng Zhu and Zach Zhizhong Zhou. Analysis and outlook of applications of blockchain technology to equity crowdfunding in china. *Financial innovation*, 2(1):29, 2016.

[36] Ori Jacobovitz. Blockchain for identity management. *The Lynne and William Frankel Center for Computer Science Department of Computer Science. Ben-Gurion University, Beer Sheva Google Scholar*, 2016.

[37] Liudmila Zavolokina, Mateusz Dolata, and Gerhard Schwabe. Fintech transformation: How it-enabled innovations shape the financial sector. In *International Workshop on Enterprise Applications and Services in the Finance Industry*, pages 75–88. Springer, 2016.

[38] Kazım Rıfat Özyılmaz and Arda Yurdakul. Integrating low-power iot devices to a blockchain-based infrastructure: work-in-progress. In *Proceedings of the Thirteenth ACM International Conference on Embedded Software 2017 Companion*, page 13. ACM, 2017.

[39] Launching the ether sale. https://blog.ethereum.org/2014/07/22/launching-the-ether-sale/. (Accessed on 12/05/2018).

[40] History of ethereum ethereum homestead 0.1 documentation. http://ethdocs.org/en/latest/introduction/history-of-ethereum.html. (Accessed on 12/05/2018).

[41] Coinbase. https://www.investopedia.com/terms/c/coinbase.asp. (Accessed on 12/05/2018).

[42] Joshua R Hendrickson, Thomas L Hogan, and William J Luther. The political economy of bitcoin. *Economic Inquiry*, 54(2):925–939, 2016.

[43] bitpayapi-0.3.pdf. https://bitpay.com/downloads/bitpayApi-0.3.pdf. (Accessed on 12/06/2018).

[44] Cryptocurrencies timeline: a history of digital money. https://www.telegraph.co.uk/technology/digital-money/the-history-of-cryptocurrency/. (Accessed on 12/17/2018).

[45] Bnak launches swiftcoin, electronic currency that is safer than cash — business wire. https://www.businesswire.com/news/home/20121119005937/en/BNAK-Launches-Swiftcoin-Electronic-Currency-Safer-Cash. (Accessed on 12/17/2018).

[46] Daniel B Bruno. System and method for providing a cryptographic platform for exchanging debt securities denominated in virtual currencies, July 27 2017. US Patent App. 15/483,190.

[47] Yingjie Zhao. Cryptocurrency brings new battles into the currency market. *Future Internet (FI) and Innovative Internet Technologies and Mobile Communications (IITM)*, 91, 2015.

[48] Dorit Ron and Adi Shamir. Quantitative analysis of the full bitcoin transaction graph. In *International Conference on Financial Cryptography and Data Security*, pages 6–24. Springer, 2013.

[49] David Yermack. Is bitcoin a real currency? an economic appraisal. In *Handbook of digital currency*, pages 31–43. Elsevier, 2015.

[50] Luqin Wang and Yong Liu. Exploring miner evolution in bitcoin network. In *International Conference on Passive and Active Network Measurement*, pages 290–302. Springer, 2015.

[51] Bitcoin's quirky genesis block turns eight years old today - bitcoin news. https://news.bitcoin.com/bitcoins-quirky-genesis-block-turns-eight-years-old-today/. (Accessed on 12/06/2018).

[52] Sèna Kimm Gnangnon and Harish Iyer. Does bridging the Internet access divide contribute to enhancing countries' integration into the global trade in services markets? *Telecommunications Policy*, 2017.

[53] Michael Nekrasov, Lisa Parks, and Elizabeth Belding. Limits to Internet freedoms: Being heard in an increasingly authoritarian world. In *Proceedings of the 2017 Workshop on Computing Within Limits*, pages 119–128. ACM, 2017.

[54] Nils B Weidmann, Suso Benitez-Baleato, Philipp Hunziker, Eduard Glatz, and Xenofontas Dimitropoulos. Digital discrimination: Political

bias in internet service provision across ethnic groups. *Science*, 353(6304):1151–1155, 2016.

[55] Sora Park. Digital inequalities in rural Australia: A double jeopardy of remoteness and social exclusion. *Journal of Rural Studies*, 54:399–407, 2017.

[56] Hans Klein. Icann and internet governance: Leveraging technical coordination to realize global public policy. *The Information Society*, 18(3):193–207, 2002.

[57] Prabir Purkayastha and Rishab Bailey. US control of the Internet: Problems facing the movement to international governance. *Monthly Review*, 66(3):103, 2014.

[58] Scott Jasper and James Wirtz. Cyber security. In *The Palgrave Handbook of Security, Risk and Intelligence*, pages 157–176. Springer, 2017.

[59] Harold Patrick and Ziska Fields. A need for cyber security creativity. *Collective Creativity for Responsible and Sustainable Business Practice*, pages 42–61, 2017.

[60] Solomon Karchefsky and H Raghav Rao. Toward a safer tomorrow: Cybersecurity and critical infrastructure. In *The Palgrave Handbook of Managing Continuous Business Transformation*, pages 335–352. Springer, 2017.

[61] Blockstack, building the decentralized Internet. https://blockstack.org/. (Accessed on 06-Oct-2018).

[62] Ammbr whitepaper v1.0. http://ammbr.com/docs/20171018/Ammbr_Whitepaper_v2.1_18Oct2017.pdf. (Accessed on 06-October-2018).

[63] Wikileaks.org taken down by US DNS provider — netcraft. https://goo.gl/Fge1Y7. (Accessed on 06-Oct-2018).

[64] Four rounds of ice domain name seizures and related controversies and opposition berkeley technology law journal. https://goo.gl/HakBpu/. (Accessed on 06-Oct-2018).

[65] Ralf Bendrath and Milton Mueller. The end of the net as we know it? deep packet inspection and internet governance. *New Media & Society*, 13(7):1142–1160, 2011.

[66] Laura DeNardis. Hidden levers of internet control: An infrastructure-based theory of internet governance. *Information, Communication & Society*, 15(5):720–738, 2012.

[67] Harry A Kalodner, Miles Carlsten, Paul Ellenbogen, Joseph Bonneau, and Arvind Narayanan. An Empirical Study of Namecoin and Lessons for Decentralized Namespace Design. In *WEIS*. Citeseer, 2015.

[68] Stefano Angieri, Alberto García-Martínez, Bingyang Liu, Zhiwei Yan, Chuang Wang, and Marcelo Bagnulo. An experiment in distributed Internet address management using blockchains. *arXiv preprint arXiv:1807.10528*, 2018.

[69] Muneeb Ali, Jude C Nelson, Ryan Shea, and Michael J Freedman. Blockstack: A global naming and storage system secured by blockchains. In *USENIX Annual Technical Conference*, pages 181–194, 2016.

[70] Namecoin. https://namecoin.org/. (Accessed on 06-Oct-2018).

[71] Wikipedia article on namecoin. https://en.wikipedia.org/wiki/Namecoin. (Accessed on 06-Oct-2018).

[72] Adam Back et al. Hashcash-a denial of service counter-measure, 2002.

[73] Joshua A Kroll, Ian C Davey, and Edward W Felten. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In *Proceedings of WEIS*, volume 2013, page 11, 2013.

[74] Stephen S Kirkman and Richard Newman. Using smart contracts and blockchains to support consumer trust across distributed clouds.

[75] Dan Metcalf Arlyn Culwick. The blocknet: Design specification. https://www.blocknet.co/wp-content/uploads/whitepaper/Blocknet_Whitepaper.pdf. (Accessed on 11/01/2019).

[76] Evan Schwartz Stefan Thomas. A protocol for interledger payments. https://interledger.org/interledger.pdf. (Accessed on 11/01/2019).

[77] Kevin Stine and Matthew Scholl. E-mail security. an overview of threats and safeguards. *Journal of AHIMA*, 81(4):28–30, 2010.

[78] Aaron J Ferguson. Fostering e-mail security awareness: The west point carronade. *Educase Quarterly*, 28(1):54–57, 2005.

[79] Cindy Taylor. Blockchain & email, access date: 06-Oct-2018. http://finteknews.com/blockchain-email/, 2016.

[80] Florian Bersier and Raphael Bischof. Email stamping: Gmelius blockchain architecture. https://gmelius.com/email-stamping-blockchain.pdf, 2017. (Accessed on 06-Oct-2018).

[81] Feng Xia, Laurence T Yang, Lizhe Wang, and Alexey Vinel. Internet of things. *International Journal of Communication Systems*, 25(9):1101, 2012.

[82] Ali Dorri, Salil S Kanhere, and Raja Jurdak. Blockchain in Internet of things: challenges and solutions. *arXiv preprint arXiv:1608.05187*, 2016.

[83] Abdul Wahab Ahmed, Mian Muhammad Ahmed, Omair Ahmad Khan, and Munam Ali Shah. A comprehensive analysis on the security threats and their countermeasures of IoT. *International Journal of Advanced Computer Science and Applications*, 8(7):489–501, 2017.

[84] Jo Ann Oravec. Emerging cyber hygiene practices for the internet of things (IoT): Professional issues in consulting clients and educating users on IoT privacy and security. In *Professional Communication Conference (ProComm), 2017 IEEE International*, pages 1–5. IEEE, 2017.

[85] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. Security, privacy and trust in internet of things: The road ahead. *Computer Networks*, 76:146–164, 2015.

[86] Arijit Ukil, Soma Bandyopadhyay, and Arpan Pal. IoT-privacy: To be private or not to be private. In *Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on*, pages 123–124. IEEE, 2014.

[87] Thomas Pasquier, Jatinder Singh, Julia Powles, David Eyers, Margo Seltzer, and Jean Bacon. Data provenance to audit compliance with privacy policy in the internet of things. *Personal and Ubiquitous Computing*, 22(2):333–344, 2018.

[88] Nir Kshetri. Can blockchain strengthen the internet of things? *IT Professional*, 19(4):68–72, 2017.

[89] Steve Huckle, Rituparna Bhattacharya, Martin White, and Natalia Beloff. Internet of things, blockchain and shared economy applications. *Procedia computer science*, 98:461–466, 2016.

[90] Jakub Szefer and Ruby B Lee. Bitdeposit: Deterring attacks and abuses of cloud computing services through economic measures. In *Cluster, Cloud and Grid Computing (CCGrid), 2013 13th IEEE/ACM International Symposium on*, pages 630–635. IEEE, 2013.

[91] Jonathan Warren. Bitmessage: A peer-to-peer message authentication and delivery system. *white paper (27 November 2012), https://bitmessage.org/bitmessage.pdf*, 2012.

[92] David Shrier, Deven Sharma, and Alex Pentland. Blockchain & financial services: The fifth horizon of networked innovation, 2016.

[93] Pierre Noizat. Blockchain electronic vote. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, page 453, 2015.

[94] Junichi Kishigami, Shigeru Fujimura, Hiroki Watanabe, Atsushi Nakadaira, and Akihiko Akutsu. The blockchain-based digital content distribution system. In *Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conference on*, pages 187–190. IEEE, 2015.

[95] Kevin Peterson, Rammohan Deeduvanu, Pradip Kanjamala, and Kelly Boles. A blockchain-based approach to health information exchange networks. In *Proc. NIST Workshop Blockchain Healthcare*, volume 1, pages 1–10, 2016.

[96] Sean Rowan, Michael Clear, Mario Gerla, Meriel Huggard, and Ciarán Mc Goldrick. Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels. *arXiv preprint arXiv:1704.02553*, 2017.

[97] Yu-Pin Lin, Joy R Petway, Johnathen Anthony, Hussnain Mukhtar, Shih-Wei Liao, Cheng-Fu Chou, and Yi-Fong Ho. Blockchain: The evolutionary next step for ict e-agriculture. *Environments*, 4(3):50, 2017.

[98] Xiwei Xu, Cesare Pautasso, Liming Zhu, Vincent Gramoli, Alexander Ponomarev, An Binh Tran, and Shiping Chen. The blockchain as a software connector. In *13th Working IEEE/IFIP Conference on Software Architecture (WICSA), 2016*, pages 182–191. IEEE, 2016.

[99] Juri Mattila et al. The blockchain phenomenon–the disruptive potential of distributed consensus architectures. Technical report, The Research Institute of the Finnish Economy, 2016.

[100] Openbazaar: Online marketplace — peer-to-peer ecommerce. https://www.openbazaar.org/. (Accessed on 06-Oct-2018).

[101] Atlas. https://atlas.money/. (Accessed on 06-Oct-2018).

[102] Sia. http://sia.tech/. (Accessed on 06-Oct-2018).

[103] HU Wei-hong, AO Meng, SHI Lin, XIE Jia-gui, and LIU Yang. Review of blockchain-based dns alternatives. Ł, 3(3):71–77, 2017.

[104] Home — blockchain education network (ben). https://blockchainedu.org/. (Accessed on 06-Oct-2018).

[105] Bigchaindb the scalable blockchain database. https://www.bigchaindb.com/. (Accessed on 06-Oct-2018).

[106] Maidsafe - the new decentralized internet. https://maidsafe.net/. (Accessed on 06-Oct-2018).

[107] Filecoin. https://filecoin.io/. (Accessed on 06-Oct-2018).

[108] Ibm blockchain. https://www.ibm.com/blockchain/. (Accessed on 06-Oct-2018).

[109] Ibm watson IoT—private blockchain. https://www.ibm.com/internet-of-things/platform/private-blockchain/. (Accessed on 06-Oct-20187).

[110] Chronicled. https://www.chronicled.com/. (Accessed on 06-Oct-2018).

[111] Elliptic. https://www.elliptic.co/. (Accessed on 06-Oct-2018).

[112] Luxtrust. https://www.luxtrust.lu/. (Accessed on 06-Oct-2018).

[113] Data-centric security — guardtime industrial blockchain. https://guardtime.com/. (Accessed on 06-Oct-2018).

[114] Decentralized prediction markets — augur project. https://augur.net/. (Accessed on 06-Oct-2018).

[115] Lazooz. http://lazooz.org/. (Accessed on 06-Oct-2018).

[116] Ubitquity - the first blockchain-secured platform for real estate record-keeping. https://www.ubitquity.io/web/index.html. (Accessed on 06-Oct-2018).

[117] Stratumn — trust the process. https://stratumn.com/. (Accessed on 06-Oct-2018).

[118] Mycelia for music - for a fairtrade music industry. http://myceliaformusic.org/. (Accessed on 06-Oct-2018).

[119] Introducing gemos, your blockchain operating system. https://gem.co/. (Accessed on 06-Oct-2018).

[120] Tierion - blockchain proof engine — api. https://tierion.com/. (Accessed on 06-Oct-2018).

[121] Provenance — technology. https://www.provenance.org/technology. (Accessed on 06-Oct-2018).

[122] Ujo. https://ujomusic.com/. (Accessed on 06-Oct-2018).

[123] Skuchain - turn information into capital — turn information into capital. http://www.skuchain.com/. (Accessed on 06-Oct-2018).

[124] Storj - decentralized cloud storage. https://storj.io/. (Accessed on 06-Oct-2018).

[125] Gyft block - building gift cards 2.0 on blockchain technology. https://block.gyft.com/. (Accessed on 06-Oct-2018).

[126] Blocksafe - blockchain centric enhanced firearm network. http://www.blocksafefoundation.com/. (Accessed on 06-Oct-2018).

[127] Bitgive foundation. https://www.bitgivefoundation.org/. (Accessed on 06-Oct-2018).

[128] IBM. Empowering the edge. https://tinyurl.com/IBM-edge-report. (Accessed on 06-Oct-2018).

[129] Adept tech paper v10.3. https://tinyurl.com/adept-white-paper. (Accessed on 06-Oct-2018).

[130] Jan Johan Karst and Guillaume Brodar. Connecting multiple devices with blockchain in the internet of things.

[131] Filament foundations.pages. https://tinyurl.com/filament-report. (Accessed on 06-Oct-2018).

[132] Dominic Wörner, Thomas Von Bomhard, Yan-Peter Schreier, and Dominic Bilgeri. The bitcoin ecosystem: Disruption beyond financial services? 2016.

[133] Thomas Bocek, Bruno B Rodrigues, Tim Strasser, and Burkhard Stiller. Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In *Integrated Network and Service Management (IM), 2017 IFIP/IEEE Symposium on*, pages 772–777. IEEE, 2017.

[134] Johan Pouwelse, Pawel Garbacki, Dick Epema, and Henk Sips. The bittorrent P2P file-sharing system: Measurements and analysis. In *IPTPS*, volume 5, pages 205–216. Springer, 2005.

[135] Roger Aitken. Can decent's 'crypto-fuelled' blockchain revolutionize content & data distribution? accessed on 06-Oct-2018. https://goo.gl/hCtEm1, 2017.

[136] Michael Crosby, Pradan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. Blockchain technology: Beyond bitcoin. *Applied Innovation*, 2:6–10, 2016.

[137] Shawn Wilkinson, Jim Lowry, and Tome Boshevski. Metadisk a blockchain-based decentralized file storage application. Technical report, Technical Report, Available: http://metadisk.org/metadisk.pdf, 2014.

[138] Lori M Kaufman. Data security in the world of cloud computing. *IEEE Security & Privacy*, 7(4), 2009.

[139] Balachandra Reddy Kandukuri, Atanu Rakshit, et al. Cloud security issues. In *Services Computing, 2009. SCC'09. IEEE International Conference on*, pages 517–520. IEEE, 2009.

[140] Subashini Subashini and Veeraruna Kavitha. A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, 34(1):1–11, 2011.

[141] Qian Wang, Cong Wang, Jin Li, Kui Ren, and Wenjing Lou. Enabling public verifiability and data dynamics for storage security in cloud computing. *Computer Security–ESORICS 2009*, pages 355–370, 2009.

[142] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou. Privacy-preserving public auditing for data storage security in cloud computing. In *Infocom 2010*, pages 1–9. IEEE, 2010.

[143] Changyu Dong, Yilei Wang, Amjad Aldweesh, Patrick McCorry, and Aad van Moorsel. Betrayal, distrust, and rationality: Smart counter-collusion contracts for verifiable cloud computing. *arXiv preprint arXiv:1708.01171*, 2017.

[144] Filecoin: A decentralized storage network, access date: 06-Oct-2018.

[145] Statista. Number of social media users worldwide 2010–2021. https://tinyurl.com/statista-worldwide. (Accessed on 06-Oct-2018).

[146] Michael Fire, Roy Goldschmidt, and Yuval Elovici. Online social networks: threats and solutions. *IEEE Communications Surveys & Tutorials*, 16(4):2019–2036, 2014.

[147] David Shrier, Weige Wu, and Alex Pentland. Blockchain & infrastructure (identity, data security). https://www.getsmarter.com/career-advice/wp-content/uploads/2017/07/mit_blockchain_and_infrastructure_report.pdf, 2017. (Accessed on 06-October-2018).

[148] Steemwhitepaper.pdf. https://steem.io/SteemWhitePaper.pdf. (Accessed on 06-Oct-2018).

[149] Richard Dennis and Gareth Owen. Rep on the block: A next generation reputation system based on the blockchain. In *10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 131–138. IEEE, 2015.

[150] Accenture. 2017 cost of cyber crime study. https://tinyurl.com/CostCyberCrimeStudy. (Accessed on 06-Oct-2018).

[151] Deloitte. Blockchain & cyber security. https://goo.gl/2BXkDb, 2017. (Accessed on 06-Oct-2018).

[152] Steve Myers. Block-by-block: Leveraging the power of blockchain technology to build trust and promote cyber peace. *Yale JL & Tech.*, 19:334–334, 2017.

[153] Tezos: A Self-Amending Crypto-Ledger, access date: 06-Oct-2018. https://tezos.com/static/papers/position_paper.pdf, 2014.

[154] White paper_v.0.1.pdf - google drive. https://drive.google.com/file/d/0B1jTRGmj_3khUV9RTERnYzNvaE0/view. (Accessed on 06-Oct-2018).

[155] Ksi data sheet. https://tinyurl.com/KSI-data-sheet. (Accessed on 09/16/2017).

[156] Obsidian platform whitepaper. https://tinyurl.com/obsidian-white-paper. (Accessed on 06-Oct-2018).

[157] George C Polyzos and Nikos Fotiou. Blockchain-assisted information distribution for the internet of things.

[158] Conner Fromknecht, Dragos Velicanu, and Sophia Yakoubov. A decentralized public key infrastructure with identity retention. *IACR Cryptology ePrint Archive*, 2014:803, 2014.

[159] JR Prins and Business Unit Cybercrime. Diginotar certificate authority breachoperation black tulip, 2011.

[160] Dennis Fisher. Final report on diginotar hack shows total compromise of CA servers. *ThreatPost, Oct*, 31, 2012.

[161] Trustwave sold root certificate for surveillance — zdnet. http://www.zdnet.com/article/trustwave-sold-root-certificate-for-surveillance/. (Accessed on 06-Oct-2018).

[162] Debian – security information – dsa-1571-1 openssl. https://www.debian.org/security/2008/dsa-1571. (Accessed on 06-Oct-2018).

[163] Nicolas Falliere. w32_stuxnet_dossier.pdf. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, February 2011. (Accessed on 06-Oct-2018).

[164] Larry Seltzer. Securing your private keys as best practice for code signing certificates, 2013.

[165] Boldizsár Bencsáth, Gábor Pék, Levente Buttyán, and Márk Félegyházi. Duqu: A stuxnet-like malware found in the wild. *CrySyS Lab Technical Report*, 14:1–60, 2011.

[166] Boldizsár Bencsáth, Gábor Pék, Levente Buttyán, and Mark Felegyhazi. The cousins of stuxnet: Duqu, flame, and gauss. *Future Internet*, 4(4):971–1003, 2012.

[167] Boldizsár Bencsáth, Gábor Pék, Levente Buttyán, and Márk Félegyházi. Duqu: Analysis, detection, and lessons learned. In *ACM European Workshop on System Security (EuroSec)*, volume 2012, 2012.

[168] Mohammad Faisal and Mohammad Ibrahim. Stuxnet, duqu and beyond. *International Journal of Science and Engineering Investigations*, 1(2):75–78, 2012.

[169] Markus Schmid. ECDSA-application and implementation failures. https://tinyurl.com/SchmidProject, accessed on 6-Oct-2018.

[170] Louise Axon. Privacy-awareness in blockchain-based PKI. *Oxford University Center for Doctoral Training (CDT) in Cyber Security: CDT Technical Paper*, 2015.

[171] Bo Qin, Jikun Huang, Qin Wang, Xizhao Luo, Bin Liang, and Wenchang Shi. Cecoin: A decentralized PKI mitigating MitM attacks. *Future Generation Computer Systems*, 2017.

[172] Ethereum. https://github.com/ethereum/wiki/wiki/Patricia-Tree. (Accessed on 06-Oct-2018).

[173] LM Axon and Michael Goldsmith. PB-PKI: a privacy-aware blockchain-based PKI.

[174] Mustafa Al-Bassam. SCPKI: A Smart Contract-based PKI and Identity System. In *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, pages 35–40. ACM, 2017.

[175] Hitesh Tewari, Arthur Hughes, Stefan Weber, and Tomas Barry. X509Cloud-Framework for a Ubiquitous PKI.

[176] Stephanos Matsumoto and Raphael M Reischuk. IKP: Turning a PKI Around with Blockchains. *IACR Cryptology ePrint Archive*, 2016:1018, 2016.

[177] Sarah Underwood. Blockchain beyond bitcoin. *Communications of the ACM*, 59(11):15–17, 2016.

[178] Peter Yeoh and Peter Yeoh. Regulatory issues in blockchain technology. *Journal of Financial Regulation and Compliance*, 25(2):196–208, 2017.

[179] Abra. https://www.abra.com/. (Accessed on 06-Oct-2018).

[180] Javier Sebastian Cermeño. Blockchain in financial services: Regulatory landscape and future challenges for its commercial application. Technical report, Working Paper, 2016.

[181] Karan Bharadwaj. Blockchain 2.0: Smart contracts. 2016.

[182] Aaron Wright and Primavera De Filippi. Decentralized blockchain technology and the rise of lex cryptographia. 2015.

[183] Javier Sebastian et al. Blockchain in financial services: Regulatory landscape and future challenges. Technical report, 2016.

[184] Varant Meguerditchian. Roadmap_for_blockchain_standards. https://goo.gl/zbv6p6, March 2017. (Accessed on 06-Oct-2018).

[185] Joost de Kruijff and Hans Weigand. Understanding the blockchain using enterprise ontology. In *International Conference on Advanced Information Systems Engineering*, pages 29–43. Springer, 2017.

[186] Advait Deshpande, Katherine Stewart, Louise Lepetit, and Salil Gunashekar. Understanding the landscape of distributed ledger technologies/blockchain. 2017.

[187] Don Tapscott and Alex Tapscott. *Blockchain Revolution: How the technology behind Bitcoin is changing money, business, and the world*. Penguin, 2016.

[188] Government of UK HMRC. Revenue and customs brief 9 (2014): Bitcoin and other cryptocurrencies - gov.uk. https://goo.gl/QSz2GL, March 2014. (Accessed on 06-Oct-2018).

[189] Financial Crimes Enforcement Network. Application of fincens regulations to persons administering, exchanging, or using virtual currencies. *United States Department of the Treasury, March*, 18, 2013.

[190] Andres Guadamuz and Chris Marsden. Blockchains and bitcoin: Regulatory responses to cryptocurrencies. *First Monday*, 20(12), 2015.

[191] European Securities and Markets Authority. Discussion paper: The distributed ledger technology applied to securities markets. https://goo.gl/jHncDb, June 2016. (Accessed on 06-Oct-2018).

[192] M Walport. Distributed ledger technology: Beyond blockchain. uk government office for science. Technical report, Tech. Rep, 2016.

[193] Official GDPR Document. Official Journal of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. (Accessed on 08-Nov-2018).

[194] Jean Bacon, Johan David Michels, Christopher Millard, and Jatinder Singh. Blockchain demystified. *SSRN: https://ssrn.com/abstract=3091218*, 2017.

[195] Commision Nationale Informatique. Blockchain. https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf. (Accessed on 20/01/2019).

[196] Yonatan Sompolinsky and Aviv Zohar. Accelerating bitcoins transaction processing fast money grows on trees. *Not Chains*, 2016.

[197] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, et al. On scaling decentralized blockchains. In *International Conference on Financial Cryptography and Data Security*, pages 106–125. Springer, 2016.

[198] Tradeblock blog. https://tinyurl.com/tradeblock-blog. (Accessed on 6-Oct-2018).

[199] Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, and Robbert Van Renesse. Bitcoin-ng: A scalable blockchain protocol. In *NSDI*, pages 45–59, 2016.

[200] Christian Decker Roger Wattenhofer. A fast and scalable payment network with bitcoin duplex micropayment channels.

[201] Sofia. How the bitcoin lightning network could solve the blockchain scalability problem, access date: 06-Oct-2018. https://goo.gl/SqpMX4, 2016.

[202] Ian Allison. Meet bigchaindb: the scalable blockchain database' hitting one million writes per second, access date: 06-Oct-2018. https://goo.gl/iBWb0Y, 2016.

[203] Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, and Prateek Saxena. A secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 17–30. ACM, 2016.

[204] Carol Davids, Vijay K Gurbani, Gaston Ormazabal, Andrew Rollins, Kundan Singh, and Radu State. Research topics related to real-time communications over 5g networks, 2016.

[205] Evan Duffield and Kyle Hagan. Darkcoin: Peertopeer cryptocurrency with anonymous blockchain transactions and an improved proofof-work system. *Mar-2014 [Online]. Available: https://cryptopapers.info/assets/pdf/darkcoin.pdf [Accessed: 06-Oct-2018]*, 2014.

[206] Primavera De Filippi. The interplay between decentralization and privacy: the case of blockchain technologies. 2016.

[207] Huaiqing Wang, Kun Chen, and Dongming Xu. A maturity model for blockchain adoption. *Financial Innovation*, 2(1):12, 2016.

[208] Steven Goldfeder, Harry Kalodner, Dillon Reisman, and Arvind Narayanan. When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. *arXiv preprint arXiv:1708.04748*, 2017.

[209] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference*, pages 127–140. ACM, 2013.

[210] Rafael Pass and Elaine Shi. Fruitchains: A fair blockchain. In *Proceedings of the ACM Symposium on Principles of Distributed Computing*, pages 315–324. ACM, 2017.

[211] Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security*, pages 436–454. Springer, 2014.

[212] Danny Bradbury. The problem with bitcoin. *Computer Fraud & Security*, 2013(11):5–8, 2013.

[213] Martijn Bastiaan. Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin.

[214] Jennifer J Xu. Are blockchains immune to all malicious attacks? *Financial Innovation*, 2(1):25, 2016.

[215] Philip Koshy, Diana Koshy, and Patrick McDaniel. An analysis of anonymity in bitcoin using p2p network traffic. In *International Conference on Financial Cryptography and Data Security*, pages 469–485. Springer, 2014.

[216] Jordi Herrera-Joancomartí. Research and challenges on bitcoin anonymity. In *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*, pages 3–16. Springer, 2015.

[217] Fergal Reid and Martin Harrigan. An analysis of anonymity in the bitcoin system. In *Security and privacy in social networks*, pages 197–223. Springer, 2013.

[218] Introduction to Blockchains & What It Means to Big data, access date: 06-Oct-2018. https://www.kdnuggets.com/2017/09/introduction-blockchain-big-data.html, 2017.

[219] Giuseppe Di Battista, Valentino Di Donato, Maurizio Patrignani, Maurizio Pizzonia, Vincenzo Roselli, and Roberto Tamassia. Bitconeview: visualization of flows in the bitcoin transaction graph. In *Visualization for Cyber Security (VizSec), 2015 IEEE Symposium on*, pages 1–8. IEEE, 2015.

[220] Michele Spagnuolo, Federico Maggi, and Stefano Zanero. Bitiodine: Extracting intelligence from the bitcoin network. In *International Conference on Financial Cryptography and Data Security*, pages 457–468. Springer, 2014.

[221] Shayan Eshkandary, David Barrera, Elizabeth Stobert, and Jeremy Clark. A first look at the usability of bitcoin key management. *NDSS Symposium 2015*, 2015.