Blockchain for decentralization of internet: prospects, trends, and challenges

Javad Zarrin[1] · Hao Wen Phang[1] · Lakshmi Babu Saheer[1] · Bahram Zarrin[2,3]

Abstract

Blockchain has made an impact on today's technology by revolutionizing the financial industry through utilization of cryptocurrencies using decentralized control. This has been followed by extending Blockchain to span several other industries and applications for its capabilities in verification. With the current trend of pursuing the decentralized Internet, many methods have been proposed to achieve decentralization considering different aspects of the current Internet model ranging from infrastructure and protocols to services and applications. This paper investigates Blockchain's capacities to provide a robust and secure decentralized model for Internet. The paper conducts a critical review on recent Blockchain-based methods capable for the decentralization of the future Internet. We identify and investigate two research aspects of Blockchain that provides high impact in realizing the decentralized Internet with respect to current Internet and Blockchain challenges while keeping various design in considerations. The first aspect is the consensus algorithms that are vital components for decentralization of the Blockchain. We identify three key consensus algorithms including PoP, Paxos, and PoAH that are more adequate for reaching consensus for such tremendous scale Blockchain-enabled architecture for Internet. The second aspect that we investigated is the compliance of Blockchain with various emerging Internet technologies and the impact of Blockchain on those technologies. Such emerging Internet technologies in combinations with Blockchain would help to overcome Blockchain's established flaws in a way to be more optimized, efficient and applicable for Internet decentralization.

Keywords Blockchain · Consensus algorithms · Decentralization · Decentralized cloud · Future internet

1 Introduction

Blockchain has been primarily associated with finance and cryptocurrency, but it has also been used for various other applications in several domains and industries including healthcare, supply chain management, asset tracking, energy management, smart home/city and Internet of Things (IoT) [1–7]. For such applications and industries, Blockchain can offer benefits including transparency, accountability, Integrity, scalability, cost-efficiency, security, and privacy. While there are several current works proposed to adapt and apply Blockchain based architecture for IoT, and interconnected devices on edge networks, there is a considerable lack of research to propose and apply Blockchain for the core networks of Internet and its protocols, applications and services.

Currently, the Internet suffers from various issues and challenges in all layers. Most of these issues such as transparency, data integrity, authenticity, data privacy and security have clear correlations with the current multi-faceted embedded centrality of Internet from the client-server communication structure to the Public Clouds and Cloud-based applications. Revitalization of Internet is required through a more extensible and scalable Internet architecture that can address such issues and incorporate a broader scope of functionality [8].

✉ Javad Zarrin
  javad.zarrin@aru.ac.uk

1 Anglia Ruskin University, East Rd, Cambridge CB11PT, UK

2 Department of Applied Mathematics and Computer Science, Technical University of Denmark, DTU Compute, 2800 KGS Lyngby, Denmark

3 Present Address: Microsoft, Kanalvej 7, 2800 Kongens Lyngby, Denmark

In the prospect of finding ways to further improve the existing Internet model, there are two major approaches being spearheaded for the development of future Internet: Semantic Web and Decentralized Internet, the former suggests to connect every piece of information entity via Semantic technology in a way to be united into a singularity [9]. The second generation of Web technology (Web2) introduced online services that brought in flaws of requiring centralized services, which is seen in client-server model. Semantic Web (Web3) aimed to extend Web2 using a data-driven model enabling integration across heterogeneous content, applications and systems through understanding data in machine-level. Semantic Web is progressing through heavily relying on machine learning and artificial intelligence (AI) methods to create more smart content and open Web applications for future Internet. However, the scope and the impact of Semantic Web is limited into application layer and it cant be relied as a complete solution to resolve some inherent Internet issues which have roots in centralized nature of current Internet.

The alternate approach is to decentralize and disseminate the Internet in all layers for equal role and authority power to prevent monopolization from online services [10]. Some decentralization approaches have already proposed in current literature to resolve Internet flaws originated from centralization [11–13]. Also, in recent years, the popularity of decentralization has been further glorified in Blockchain due to its success in decentralization for cryptocurrencies [10].

The centralization of the Internet is not accomplished from a single night, but the gradual development of the Internet and its services over the years. The introduction of centralized services provided convenience and accelerated the maturity of the Internet. This acceleration from centralization made it widely dependent throughout the Internet. Although these centralized services have provided numerous advancements that have made up the current Internet, the bottom line is that a centralized service would still exhibit a centralized network's vulnerabilities that would jeopardize the network. By having users relying on a centralized service, the users are opened to various types of attacks like Distributed Denial-of-service (DDoS) that could have been easily mitigated through decentralization.

The main motivation for this work came from the acknowledgment of reliance on centralized systems within the Internet [14]. It is clear that according to [15] there has been a push for the development of the Internet to be consolidated into a central overseeing figure for administration. This matter of consolidation with information data is further provoked by privacy concerns caused by large organizations as part of the Big Data scheme.

Combating this centralization is achievable through decentralization with Blockchain. Blockchain has always been classified as a disruptive technology due to its impact for providing a decentralized solution for communication and transaction. This brings us to Blockchain's consensus algorithms being capable of enforcing equal roles between peers. This enforcement would also keep these online services in check, preventing centralized power. The aspiration to obtain decentralization is broadened with the trend of implementing Blockchain into Internet Of Things (IoT), and to account for scaling to support the Big Data of the future Internet.

The Internet is a tremendously scaled, geographically distributed, global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) for communications across nodes and networks. It comprises various components, including infrastructures, hosts, devices, protocols, operating systems, services, and applications.

Throughout this paper, we frequently use the terms "decentralized Internet" and "Internet decentralization" to represent the concept of applying possible decentralized approaches in various levels and into any Internet components (e.g., decentralized protocols, applications, and infrastructure) in general and particularly for Web (so-called Decentralized Web, dWeb or Web 3.0). The original Web 1.0 introduced communication with Hypertext Transfer Protocol (HTTP) and established static web pages as content on the Web. Web 2.0 allowed users to collaborate and utilize server-side scripting to allow online services to proliferate. It is due to the growth of online services that led to the conceptualization of Web 3.0 being decentralized. Web 3.0 has been around as a concept since the early 2010s. The concept of Web 3.0 centers around user autonomy and not being reliant on centralized services, essentially having users be responsible for their data. The three generations of the Web can be seen in Fig. 1.

Current Internet model and architecture suffers from a large number of issues due to the impact of centralization. These issues include:

Scalability and availability Internet resources and services (e.g., computing, storage, network, and database resources ranged from single servers to large scale Cloud-based server-farms/datacenters) have limited capacity and cannot cope with the requirements of the increasing number of users without their direct contributions in providing resources. Large Internet companies may fail to provide resources to users in different geographical regions or over a specific time. This raises another issue, which is the availability of resources. In 2019, Microsoft Azure was reportedly running out of VMs for its customers in East U.S. [16]. Similarly, in March 2020, Azure has suffered from a shortage in data center capacity due to a large amount of demands resulted by Covid-19 pandemic [17].

Fig. 1 Generations of web technology
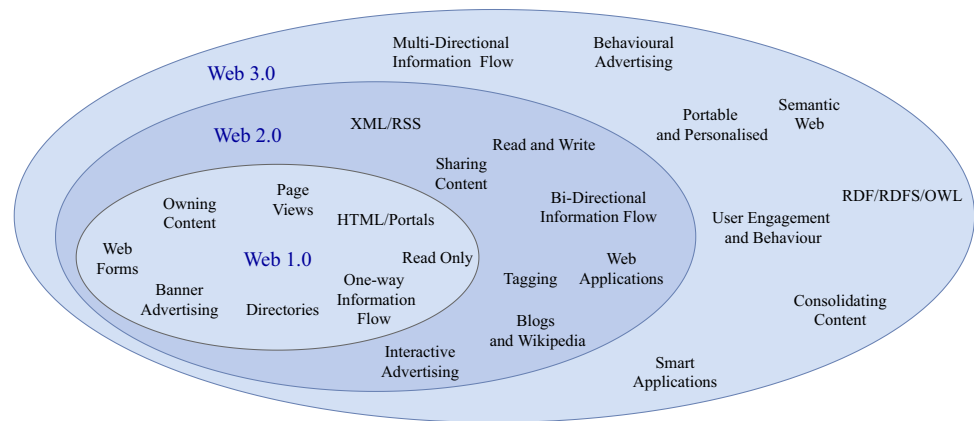
Reliability Services based on the client-server model are vulnerable to a single point of failure and bottleneck. They may fail to provide services due to problems like network or system failure.

Security and privacy Collecting user data by different service providers and storing them in a certain number of specific servers to support the hosting of various types of services and applications expose vulnerabilities and user data privacy to cybercriminals.

Trustability Large Internet corporations and service providers are trusted parties that can potentially maintain, control, and administrate user data, access, and activities. While this can bring benefits for the users, it potentially can be used as a source of control to apply surveillance or censorship, or it can lead to abusing trustability [18]. In this paper, we provide a systematic review of the potentials and capabilities of Blockchain-based solutions which can efficiently be used for any aspect of the Internet decentralization. There are several other approaches for decentralizing the Internet, such as projects seen in Sect. 2.3. However, our focus in this paper centers around using Blockchain to decentralize the Internet. Also, it must be taken into account that Blockchain for IoT security is out of the scope of this paper due to space limitations.

In this paper, we consider the popularity of Blockchain for decentralization and the aforementioned Internet issues and provide the following contributions: (a) We identify that the current Internet is highly centralized, and we review challenges of centralized Internet and methods for Internet decentralisation. (b) We provide a detailed review on opportunities and challenges to use Blockchain as a key enabler for decentralization of Internet. (c) We explore and assess various Blockchain components, methods, techniques and algorithms with respect to the Internet open issues and provide a detailed review on Blockchain potentials to resolve the problem on centralization in current Internet. (d) We also provide a review on other emerging Internet relevant technologies to identify how

they can be combined with Blockchain, covering its drawbacks to create a better solution for future Internet.

The rest of this paper organized as follows: Sect. 2 provides an overview of the current Internet architecture and what Blockchain is facing against, Sect. 3 revolves around understanding Blockchain's components and challenges it would face on decentralization, Sect. 4 presents a list of consensus algorithms that have the potential to be a candidate for reaching consensus within the Internet, Sect. 5 discusses the emergence of future and old technologies that can be integrated with Blockchain, Sect. 6 presents a discussion of current and future technologies that can impact and benefit Blockchain in decentralizing the Internet, and finally Sect. 8 concludes the paper and discusses future works.

2 Understanding the contemporary internet architecture

The Internet architecture has amassed to a tremendous scale where it encompasses many systems, services, protocols, architecture, and hardware to use on such an extensive scale. It is nearly impossible to cover every intricacy of the Internet. However, instead, this section mainly considers the macro-scale of the Internet's model and generally discusses why it is centralized and challenges caused by current centralized Internet architecture This section is followed by summarizing the types of decentralization that can be achieved with the Internet. Only to finish on why Blockchain is the choice for decentralizing the Internet.

2.1 Current internet is centralized

The current Internet is centralized due to the unusual architecture that has been designed to route users to pass through a singular point before the users can interact on the

Internet. This singular point on the Web can be seen in many forms, such as Domain Name System (DNS), where it acts as a translator for IP addresses and Domain names for human and computer readability. The DNS was implemented in a distributed way in Web 2.0, but traces of centralization are observed in domain name servers, namespace governance and operation [13, 19]. This centralization is further supported by the monopolization of DNS generation and distribution on the web by the Internet Corporation for Assigned Names and Numbers (ICANN) [12]. Internet Service Providers (ISP) are another centralized point, as users need to establish a connection with an ISP before the user can interact with the Internet. This allows ISPs to have control over the Internet traffic and allow third-party organizations to have access and control Internet traffic flow. The fact that the Internet is heavily dependent on DNS and ISPs to operate, proves our reasoning of centralization that occur within the Internet architecture.

2.2 Challenges of centralized internet

The Transmission Control Protocol/Internet Protocol (TCP/IP) is synonymous with the Internet when discussing how the Internet communicates [20]; this brings up the question of decentralization compatibility. Considering the fact that TCP/IP has been the catalyst for the Internet since the very beginning, most improvements to the Internet appear to be revolved around TCP/IP. In the continuation of this section, we discuss the issues related to each OSI layer as well as the infrastructure issues.

2.2.1 Application layer

The Application layer is the standardizing layer to enforce and conform applications, such as web-browsers and web-servers to allow end-users to communicate between each-other through the Internet. HTTP and its secure successor Hypertext Transfer Protocol Secure (HTTPS) are well-known examples of protocols placed on the application layer. These protocols are fundamental to the Web, and is implemented all over the Internet with reliance on the client-server networking model (a centralized architecture). Blockchain can be considered an alternate solution of communication to decentralize HTTPS. However, Blockchain is an entirely different system that communicates using its own standards and protocols, meaning that a communication method between HTTPS and Blockchain needs to be established. Furthermore, Blockchain employs completely different security measures compared to HTTPS. This difference in security lies in HTTPS using a multi handshake protocol [21], while Blockchain uses a cross-referencing method.

The DNS is an application layer service which is used to resolve names to addresses or vice versa. It is a vital protocol within the Internet model that translates unique IP addresses to human-readable addresses [22]. Security is an essential aspect in DNS, and methods of providing security such as extensions like Domain Name System Security Extensions (DNSSec) are used [23] to mitigate against DDoS, configuration tampering, DNS poisoning, and information leakage as well as countless other DNS vulnerabilities [23]. The DNS in the current Web 2.0 is centralized as discussed in Sect. 2.1; this brings up the question of how can we decentralize DNS while maintaining the same functionality of translation. The solution to that centralization is a decentralized name system. The decentralization of the naming system can be seen with numerous proposals, where each employs Blockchain and Peer-to-Peer (P2P) technology to achieve decentralization.

SocialDNS [19] employs short-names for resources in a localized area network while using a rank-based mechanism to handle name conflicts. SocialDNS uses P2P to enable virtual organization of the domain names, without the need of a central authority. BlockDNS [13] is another solution for decentralizing the name system, as it allows users to apply domain names while maintaining authoritative server information in a decentralized way. BlockDNS employs the use of a lightweight verification system that can cut the overhead of data authenticity verification to a few hundred bytes, allowing the BlockDNS to handle more DNS queries in the DNS cache. ConsortiumDNS [12] is another DNS to consider. It resolves the limitation of storage in a blockchain by using a three-layer architecture with external storage. This design in ConsortiumDNS allows indexing of transactions and Blockchain blocks for increased performance of domain name resolution. Last of the proposal is Bitforest, which uses a partially trusted centralized name server in a Blockchain with cryptocurrency to achieve decentralized trust and security. Bitforest [24] is capable of the same performance and scalability of centralized Public Key Infrastructures (PKI) in client validation and verification of name bindings. Bitforest's architecture maintains decentralization by not allowing the administrator to violate identity retention.

2.2.2 Transport layer

The transport layer encompasses communication protocols to provide end-to-end communication services such as reliability, traffic, and flow control to applications running on hosts [20]. Its services has been the same since early days of the Internet, which is to offer a connection between hosts. Over the years, flaws and limitations have been uncovered for the transport layer, from enumeration attacks for extracting information about the targeted system and

network, using fingerprinting techniques to uncover open ports of a system for infiltration, to SYN flood attacks to overwhelm a system. Due to this uncertainty of security created from the flaws in the transport layer, an alternative security solution should be sought. There are two options that can resolve the problems presented in the transport layer. The first option revolves around [25] by greenfielding and implement a policy-based security module into TCP/IP. This greenfield option would use four-way handshaking and public-key cryptography to ensure a secure entity that would maintain and monitor the security in the system. The second option would be to follow [26] and brownfield it by transitioning TCP/IP into Named Data Network (NDN). NDN is the contending winner, as it is robust enough to offer enhanced performance for the network traffic. More of NDN will be discussed on the Sect. 5.

2.2.3 Network layer

The network layer is one of the major backbones with many inner mechanisms working in conjunction with this layer within the Internet architecture. This layer allows communication protocols such as IP for the delivery of packets since IP as by itself does not guarantee the delivery of the packets to the intended destinations. The network layer cooperates with the transport layer to deliver the packets via TCP, guaranteeing the arrival of packets on the destination node. Hosts on the Internet use names (i.e., domain names for the servers) or numbers (IP addresses for both servers and clients) or both of them together to communicate across the Internet. Client hosts need to resolve server names to IP addresses before being able to initiate requests for communications.

Internet Protocol Version 4 (IPv4) has an issue of address space limitation where it is not able to accommodate future IP addresses due to exhaustion of usable addresses [27–29]. Internet Protocol Version 6 (IPv6) has always been regarded as a successor towards IPv4. IPv6 is able to solve the issue of address space limitation in IPv4 by increasing the size from 32 to 128 bits [27] and also solving many of the limitations and security issues within IPv4. Having a full transition from existing IPv4 addresses to IPv6 address is near impossible due to the high cost of replacing existing IPv4 Internet infrastructures e.g., IPv4 routers. One important aspect within the arsenal of IPv6 is the ability of "tunneling" between IPv4 and IPv6. Tunneling allows IPv6 to encapsulate itself into an IPv4 address and cross-communicate with the existing IPv4 addresses [30]. The tunneling feature would be an essential component in the implementation of Blockchain for the Internet, as the Blockchain's domain consists of multiple interoperable smart contracts. Without this tunneling feature, nodes would only be able to communicate with IP

versions that is supported. Not being able to communicate with other versions of IP would result in blocking off the other half of the Internet to communicate with. As of June 27th 2020, Google has collected statistics across the Web and have shown that 67.08% of the web is still in IPv4, while the remaining 32.92% has migrated to IPv6 [31].

2.2.4 Data-link layer

Lastly, the data-link layer in the TCP/IP model consists of OSI's data-link layer and a physical layer. The physical part of this layer establishes the hardware needed for interchangeability and interconnection of the network link between hosts, routers, and switches. The software uses protocols to encapsulate packets received from the network layer into other frames with Media Access Control (MAC) address and prepares it for transmission. The data-link layer also provides synchronization and validation for the frames, as it transfers receiving packets with the corresponding and correct MAC address to the network layer. The service that this layer uses consists of WLAN, LAN, Ethernet, and other similar network devices to overcome the limitations of the network layer [32].

The TCP/IP model may also include the 5th physical layer which encompasses the hardware needed for sustaining the network [20, 33]. This physical layer can be seen as a segregation of the data-link layer to establish clarity between hardware and software. However, this hardware layer could be prominent in the future with IoT, as computers are increasingly prevalent in terms of everyday usage over time.

2.2.5 Internet infrastructure

As illustrated in Fig. 2, a centralized point is seen with each respective ISP. Users are provided access to the Internet through centrally administrated entities, which are so-called ISP networks. We understand that ISP plays the man-in-the-middle for computers to communicate with the Internet, which resulted in this centralized Internet traffic route. A centralized infrastructure is always ideal in a private network for allowing a governing entity to easily administrate and have an overview of the network and its connections. There is also the case of fault tolerance systems where it accounts for preventing disruption on the network from a single component failure that has experienced prolonged continuity of operation. This allows for the lowered costs for IT equipment, expenditures, and maintenance. But this lowered cost would enable the architecture to have a decreased level of maintainability and accommodate more expansion [35].

Single point of failure is a major flaw in a centralized network, as it is caused by the need to trust a central entity
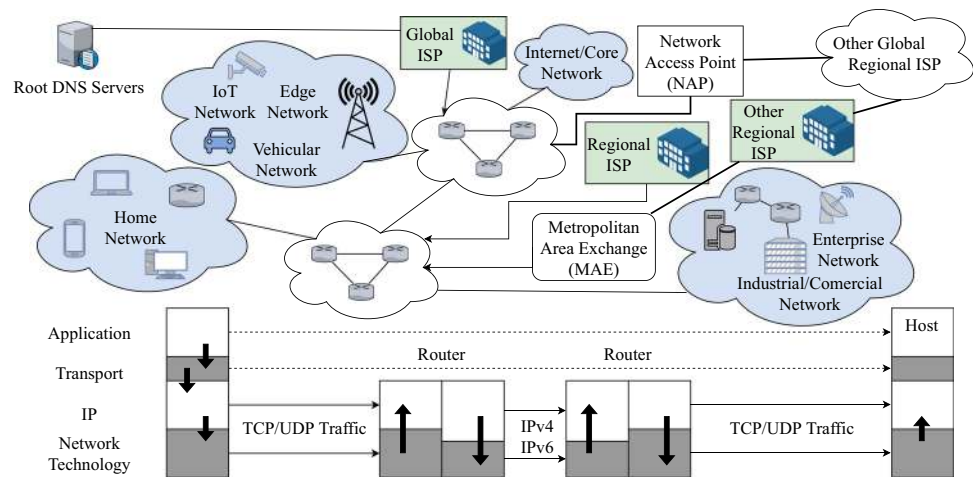
[36]. This singular point of failure can also be reflected as a singular point of control, where the central system can have total control of the network and its participating nodes due to its converging point of contact. Security risks are another flaw, due to the possibility of compromised entry points into the infrastructure. These entry points would ensure a major risk for both the network and the databases. The second major flaw is caused due to the exponential growth of information data on the Internet. This exponential growth would cascade into the need for expanded capacity for data storage [37] to respond against the increasing information data. This need for increased storage data ties heavily to Big Data with extensive information data needing to be stored, resulting in a scalability issue. The scalability issues mainly come from using legacy databases that lack the efficiency and performance to respond to the ever-increasing information data needing to be stored across various devices on the Internet. To counteract this, implementing IoT into the Blockchain would allow it to cope against scalability issues by designing a new consensus algorithm that increases the throughput to handle the large information data, or locates the databases in a private or consortium Blockchain where it can process the database at a much higher speed[38]. The current security with Alt-Svc that was introduced for HTTP [39] has many underlying vulnerabilities such as bypassing black-listed sites, distributed port-scanning and DDoS of non-HTTP sites. This makes Alt-Svc highly abusable for malicious purposes, and would be a critical issue.

2.3 Types of decentralization

The original network design of the Web with HTTP by Tim Berners-Lee was envisioned to be a decentralized infrastructure [40]. However, throughout its lifespan, as stated by [10], the Internet has developed into a centralized infrastructure. The decentralized network option has been

gaining traction, as the idea emphasizes on developing new protocols and underlying technologies through Peer-to-peer (P2P) technology for a shared data layer within the architecture [10]. A decentralized Internet would be able to give resiliency for data security, which would offer incentives for users to cooperate and further expand [37, 38]. This would increase scalability to support complex transactions of information data. Examples of decentralized Internet can be seen on projects like The Onion Route (TOR), Zeronet, and The Invisible Internet Project (I2P) [41–43]. The goal of these projects is to allow users to surf the Internet anonymously anywhere on the Internet while reducing their footprints.

Based on our current research, there are currently two types of decentralized networks that can achieve the ideal decentralized Internet.

The first method involves a completely decentralized network by [36] where "trust" and controls are spread across anonymous users. These "trust" ensures controls are from each individual users and not from a centralized point. But one drawback with this method, is that it requires the need of standardization for network systems. This would come as a possible challenge due to the divergence of operating systems and how networks are being configured in the proceeding future. Additionally, utilizing a fully decentralized network comes with the risk of losing the conveniences provided by Internet services that have been developed with centralization technology in Web 2.0.

The other type of decentralization method is utilizing a distributed network. The distributed network ensures that every participating computer is inter-connected and is co-dependent with each other. This inter-connectivity between computers would allow legacy centralized systems to run within the network in a pseudo-decentralized way. To completely transform the current Internet to be completely decentralized and autonomous would be near impossible

with its current expansion rate of network. But this method of distributed network would be efficient in converting existing webs to be decentralized and allow legacy centralized networks to exists in a decentralized manner.

2.4 Blockchain for decentralization

Blockchain allows the Internet to achieve a distributed state of the network by allowing "trust" to be shared across the connecting networks. This "trust" gives the notion of web of trusts between nodes in the Blockchain. Furthermore, Blockchain has ties to the mentioned decentralized Internet projects in Sect. 2.3. Those projects have some peculiar traits, whereby P2P, data storage, and encryption play an essential role in each project. Blockchain also parallels these traits; therefore, we consider it as the most prominent option for Internet decentralization throughout this paper. The way Blockchain is able to accomplish these features is due to its components that are shown in Fig. 3, which will be further explored in Sect. 3.

3 Understanding blockchain-based decentralization

3.1 What is blockchain?

Blockchain is described as a database that is used as a storage for a decentralized network [44]. It is usually seen in its popularized usage on cryptocurrencies like Bitcoin, Ethereum, ,Litecoin, and Dogecoin. The Blockchain is not limited within the boundaries of financial usage, as it can be expanded further upon to encompass other types of systems, applications, and make a decentralized network [45]. Asymmetric cryptography and distributed consensus
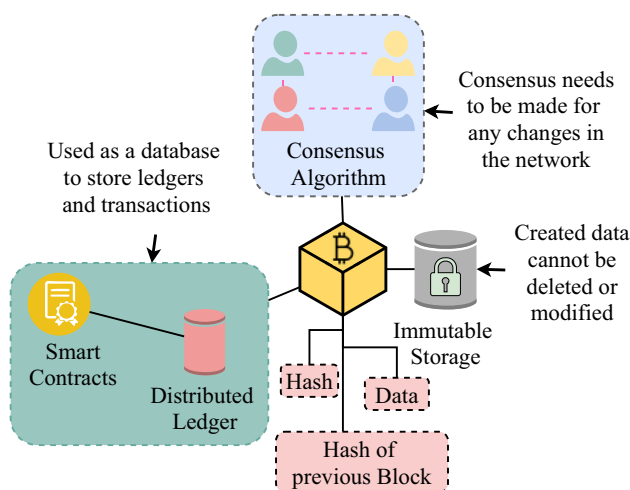
algorithms are part of the systems within Blockchain, which provide user security and ledger consistency [46]. In summary, Blockchain is a decentralized, and immutable database that facilitates its chain network with its participating nodes through a voting scheme.

As seen on Fig. 4, where it demonstrates the overall Blockchain process. The process begins with the request of a transaction from a node, which would be packed into a block. It would then broadcast the block to other nodes within the Blockchain network for validation and verification. When that block has been successfully verified, it would then be appended at the end of the Blockchain to be stored and finally finishes the transaction.

Blockchain exhibits the following key characteristics [45, 46]:

Decentralization, where each transaction in the network is done only by two nodes at a time and does not need a third-party validation. Decentralization allows the Blockchain to be non-reliant on a central authority. This enables nodes to essentially have equal voting rights within the network, which is then utilized with the consensus algorithm to dictate the Blockchain.

Persistency, refers to each transactions must be validated by trusted miners. Persistency ties into the technology of immutability to ensure the ledgers stored within the nodes are absolute and not modifiable nor be deleted.

Anonymity, refers to each miner uses a generated address as a unique ID. Although not all Blockchains are entirely anonymous and some practice pseudo-anonymity such as Ethereum and Bitcoin, where the addresses are generated for each transactions in the Blockchain. However, the core principle maintains, as it is to ensure miners within the network can remain anonymous.

Auditability, refers to having a reference point for each transaction within the Blockchain, which is also imprinted into the nodes of the Blockchain. These reference points are used to enable each transactions that has been verified and enacted within the Blockchain to be traceable. This
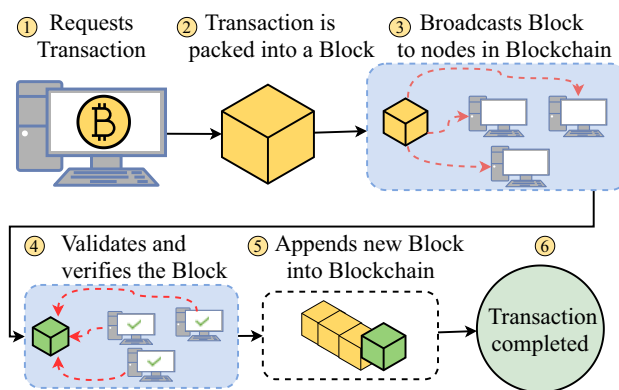
Fig. 3 Blockchain components

Fig. 4 Blockchain process

"Auditability" can be seen as the characterization of verification and leaving behind a footprint of the transaction in the Blockchain network.

Despite the extensive scope that may be provided from understanding these aforementioned characteristics. They are nevertheless, out of the scope of this paper, as the priority is on decentralization.

3.2 Components of blockchain

Three main components run within the Blockchain system. All three components are required to work together, as these components give the pillars of support in ensuring decentralization for the Blockchain network [47].

3.2.1 Distributed ledger

Distributed ledgers offers a distributed database [47] that forms a network connection between users, and the computers that are used by these users to connect are referred as nodes. Within these nodes are ledgers, which are ordered list of transactions with timestamps. These ledgers can only be appended within the database [48–51], ensuring a secure way to track transactions without the need of a central figure for verification [40]. Initial process of transactions were done in a P2P manner, only to be facilitated by Smart Contracts during the 2nd generation of Blockchains [49]. Smart Contracts are transaction protocols that controls the transmission of the ledgers between nodes. Consequently, an alternate technology to replace distributed ledger is by using the browser as a lightweight middleware[52], but it is still in its testing phase.

3.2.2 Immutable storage

The Immutable Storage is a component that refers to the nodes having the ability to be unalterable. Each database is retained in every node and has a reference of itself in the Blockchain as an immutable history [46, 48, 53]. Immutable Storage provides the encryption function to maintain the integrity of ledgers within the nodes. The Immutable Storage guarantees no other medium altering the content of the transaction, it would establish an increase of incentives and trust within the Blockchain.

3.2.3 Consensus algorithm

The consensus algorithm is used to achieve consensus between nodes for alteration or modification of existing ledgers [48, 54], only to append them into a new block at the end of the chain within the Blockchain. The consensus algorithm moderates the Blockchain by dictating the nodes on how to achieve an agreement and update the Blockchain

network [48]. We further discuss Consensus Algorithm in Sect. 4.

3.3 Types of blockchains

Table 1 compares properties of three types of Blockchain, including public Blockchain, consortium (hybrid) Blockchain, and private Blockchain, for different criteria [46, 55–57]:

Public Blockchain is opened for everybody to participate in the verification and consensus process within the Blockchain. The Public Blockchain is a permissionless Blockchain, where public nodes can join the Blockchain without needing permissions. Nodes in a Public Blockchain have full read and write permissions. Examples of Public Blockchain can be seen with Bitcoin and Ethereum. These cryptocurrency's development are open source, which can be viewed or modified by anybody.

Consortium Blockchain only chooses selected nodes from a public or private branch of the Blockchain to handle the verification and consensus process in the Blockchain. This type of Blockchain is a hybrid between public and private Blockchain, it is also labeled as a permissioned Blockchain due to utilizing the same logic of authorization where few select nodes have read and write permission in the Blockchain. Examples of Consortium Blockchains are seen in the financial and health industry with Hashed Health and IBM/Maersk.

Private Blockchain utilizes private nodes from an organization or group that is restricted from the public to handle the verification and consensus process of the Blockchain. Additionally, not every node can participate in both the processes, even if the nodes are from the same organization or group. The Private Blockchain is a permissioned Blockchain with the same principle of selected authoritative nodes, as it functions similarly to a Private Blockchain. The difference lies in that Consortium's authoritative nodes are not consolidated from a single group, but consist of multiple different groups. Examples of Private Blockchain are seen with Corda and Hyperledgers, where few nodes are only allowed modified.

Blockchains can be categorized into two groups in terms of user access. The permissionless Blockchain allows for open participation where every user has an equal vote (P2P). The permissioned Blockchain uses distributed mechanisms with a trusted third-party to have a shared mediating state between the exchanges of stakes. This permissioned Blockchain governs the consensus by restricting the access of the consensus protocol to the selected few governing nodes which can result in a centralized scenario. However, there is an issue with permissioned Blockchains where it formed a dependency with the governing nodes that forms the consensus. This causes an

Table 1 Properties of blockchain

Properties	Public blockchain	Consortium blockchain	Private blockchain
Determination of consensus	All miners	Selected nodes	An organization
Read permission	Public	Public or private	Public or private
Immutability	Close to full immutability	Can be tampered	Can be tampered
Efficiency	Low	High	High
Decentralization	Yes	Partial centralization	No
Consensus process	Permissionless	Permissioned	Permissioned
Examples	Bitcoin (BTC), Ethereum (ETH)	Bankchain, R3	Hyperledgers, PBFT, Quorum

issue with trustworthiness, as nodes would need to trust these governing nodes to make the consensus for the Blockchain. However a permissionless Blockchain, in our opinion, would result in a lawless Blockchain where the consensus can be monopolized through majority votes. Despite the issue of dependability and trustworthiness in permissioned Blockchain, this can be solved by providing the governing nodes to be chosen in a decentralized and autonomous way [36].

3.4 Generations of blockchain

Blockchain is a developing technology, and developments in the next generation of Blockchain are already underway [48]. The first-generation of Blockchain brought the concept of public ledgers for supporting a cryptocurreny network eco-system with PoW consensus (see Table 2). This concept gave us the creation of the first cryptocurreny with Blockchain, Bitcoin. The second-generation of Blockchain is rooted in cryptocurrency [48] and brought the innovation of Smart Contracts, which was discussed in Sect. 3.2.1. There are already proposals of third-generation Blockchain in the market where it prioritizes providing support for different Blockchain data structures, interchain and intrachain proof protocols [37]. The applications of the third-generation Blockchain have evolved to a state where it can be considered as a decentralized software architecture, as it would have the scalability to handle large amounts of

transactions with higher efficiency than the previous generations. The main attraction to achieving the decentralized Internet stems from the third-generation of Blockchain. The fourth-generation has yet to be clearly defined yet, as developments are prioritized in the contemporary third-generation of Blockchain. What is being discussed within the community now is the possibility of implementation with other technologies such as AI or properties such as time, which is further explored in Sect. 5. A proposal that is currently being developed for the fourth-generation Blockchain can be seen in SOOM, a developing Blockchain that utilizes time/space for increased security and processing speed.

3.5 Limitations of blockchain

Blockchain is not a fully decentralized system by design. It is considered as a partially decentralized system [44]. There are simulations done on Blockchain where results have shown natural pressures of forming centralized nodes within the network [11, 46, 58]. This slight centralization leads to a bigger picture of limitations and flaws inherent with the current second-generation of Blockchains. While Blockchain is a prominent emerging technology which has proved its efficiency in several areas, it also comes with its own set of challenges. These limitations and challenges include:

Table 2 Generations of blockchain

Properties	Gen 1	Gen 2	Gen 3
Innovations	Distributed Ledger and Cryptocurrency	Smart Contracts, Decentralized Applications (dApp) and Digital Assets	Application in the industry
Design	Setup a shared public ledger to support cryptocurrency networks & P2P	Security for transactions	Decentralized software architecture
Examples	Bitcoin, Litecoin, Dogecoin	Ethereum, Neo	IOTA, Holochain, Quarkchain

Scalability Each transaction is needed to be verified by a trusted central node [30], where the bottleneck would occur from the increasing transactions that are occurring every day [46]. This is especially prominent in multichain Blockchains [37]. Multichain Blockchains are private Blockchains that are used for financial applications, where it would require the use of full hashes of the transactions. Multichain Blockchain's design is to ensure total security and control for the transactions, hence the need for using fully hashed transactions for communication. Using this full hashed transaction results in need for increased storage for communication in the network stream, where bottlenecks would heavily affect it.

All of the bottleneck issues stems from the scalability issue with blocksizes being limited to 7 transactions per second. However, this scalability issue is repairable through implementing relevant technologies like graph-chain where parallel mining can be done to overcome the bottleneck [59] and the implementation of edge computing and fog computing to further reduce the issue. The Chu-ko-nu Mining, is a system that can bypass the scalability issue of limited transaction [60]. Chu-ko-nu Mining introduced "Asynchronous Consensus Zones" where it uses multiple parallels and independent single-chain nodes to reduce communication and partition the workload of the transactions. Implementing this system would ensure mining across single-chain nodes be the same and deliver over a thousand times of throughput, and two thousand times of capacity compared to Bitcoin and Ethereum.

Performance The performance with the current generation of Blockchains is plagued with several issues that are making it slow and unscalable for large transactions. Smart Contracts has an issue of inefficient transmission between nodes, and not being able to fully utilize arbitrary software programs that are restricted by the immutability of specific blocks [37]. The second issue is Forking, which is a divergence called "fork" formed from a Blockchain that has its block mined simultaneously by multiple nodes [61]. Forking causes a network delay of more than 1000 s [62]. Forking can also be exploited into a forking attack where back doors can be inserted into the new chain that was created from the divergent [63]. However, a customized PvScheme system has been proposed to counter Forking [64], where Forking can be mitigated. This PVScheme introduces the theory of probabilistic verification scheme to reduce the occurrence of forks. This theory with is accomplished by not requiring verification of new blocks from each node in the Blockchain. The third issue involves the performance bottleneck in Blockchain. This performance bottleneck is caused by long verification time from the blocksize's limited seven transactions [37, 46]. To resolve this issue of a performance bottleneck, there would be a need to have an increased blocksize to house more

storage. This blocksize increase can be expanded with the proposed "Layer 2" system protocol with Lightning Network. An alternate solution is to harness Forking to allow more transactions.

Privacy Although Blockchain's innate security provides anonymity for the user by hashing the public key and private key, there have been findings by [56] where both keys can be compromised. Both embedded keys can be extracted to show user's private information [46]. The keys can be further exploited into erasing stored information data in the nodes [65]. It is also possible to trace the user's address to the identities of users that execute transactions. This identity tracing is caused by the nodes using the same false address continuously, as the Blockchain does not refresh a new false address for the node [46].

Mining issue Selfish mining is a major issue within the Blockchain, as selfish miners would store their mined blocks. These mined blocks are released only after the selfish miner's requirements are met. Selfish mining would cause wastage of resources by the normal miners for mining blocks, as selfish miners would have a private branch that may have shorter chains than the public branch of the chain [46]. Personalization mining is another issue in the Blockchain, where it is formed from being unable to specify Blockchains to interact with Internet services. These mining issues can be solved by making parts of the Blockchain smarter with artificial intelligence to reduce the likelihood of personalized mining [37].

4 Investigating the consensus algorithm in blockchain for decentralization

A good decentralized Blockchain depends on a good consensus algorithm [66]. A reliable decentralized consensus algorithm should not rely on trusted third-party services [66], leading to the dismissal of permissionless Blockchain as a choice. Permissioned Blockchains is the favoring choice, due to it being able to provide both dependability and trust in a decentralized way [36]. There is also the matter of fog computing and edge architecture to account for, as it has relevance to IoT and Internet infrastructure in terms of providing performance without latency issues for nodes connected at the "edge" of the Blockchain network. All of these variables give us the reasoning for needing to explore the available consensus algorithms.

There is a variety of consensus algorithms in the current market to select from, with new ones being developed. Suggestions can only be made for consensus algorithms due to the uncertainty of these algorithms. The following subsections would cover the selected consensus protocol and review how compatible it would be for the Internet. A

Table 3 Comparison of proof-based consensus algorithm (*IoT Suitability* Level of compatibility with IoT, *Efficiency for DI* Level of efficiency in achieving decentralization)

Consensus algorithm	Blockchain type	Permission type	Decentralization	IoT suitability	Efficiency for DI	Remarks
PoW (Work)	Public & private	Permissioned	Medium	Yes	High	High Computing Power Wastage
PoET	Consortium & private	Permissioned & permissionless	Medium	Yes	Medium	Dependent on Intel's SGX
PoS (Search)	Private	Permissioned	Low	Plausible	High	Dependent on resource provision
PoAh	Public	Permissioned & permissionless	High	Yes	High	Low computation need when implemented with fog and edge computing
PoP	Public	Permissionless	High	Plausible	High	Requires further research
PoS (Stake), LPoS, dPos	Private	Permissioned	Low	Medium to High	Plausible	Requires further research
PoI	Public	Permissionless	High	Plausible	Medium	Requires further improvements
PoB	Public	Permissionless	High	No	Low	Requires monetary value
PoC	Private	Permissioned	Medium	No	Medium	Uses Storage as mining rights
PoA (Activity)	Public	Permissionless	High	No	Low	Can experience high levels of Delay
PoW (Weight)	Consortium & public	Permissioned & permissionless	Medium	Plausible	Low	Requires monetary values
Casper	Consortium & public	Permissioned & permissionless	High	No	Medium	Unable to meet IoT requirements
PoL	Public	Permissionless	High	No	Medium	Efficiency not high enough for IoT

Table 4 Comparison of BFT and crash-based consensus algorithm (*IoT Suitability* Level of compatibility with IoT, *Efficiency for DI* Level of efficiency in achieving decentralization)

Consensus algorithm	Blockchain type	Permission type	Decentralization	IoT suitability	Efficiency for DI	Remarks
PBFT	Private	Permissioned	Medium	Yes	High	Limited scalability
dBFT	Private	Permissioned	Medium	Plausible	Low	Suffers with low network speed
SCP & ripple	Public	Permissionless	High	Plausible	Medium	Suffers with latency issues
Hyperledger & variants	Private	Permissioned	Low	Mostly no	Low to Medium	Requires further improvements for a lot of the variants
PoA (Authority)	Private	Permissionless	Low	No	Medium	Conflicting design methodology
Paxos	Private	Permissioned	Low	No	High	Needs to be adapted
Raft	Private	Permissioned	Medium	Plausible	High	Requires further improvements

table consisting of the consensus algorithms that have been reviewed is done in Tables 3 and 4.

4.1 Proof based consensus algorithm

Proof based consensus revolves around nodes competing with each other to calculate and solve a cryptographic problem. Whoever solves the problem will earn the right to append the Blockchain. After appending the Blockchain, the cycle restarts. This type of consensus is widely seen in permissionless Blockchains [67].

4.1.1 Proof-of-work (PoW)

Widely used in a lot of Blockchain [54], PoW has its foundation from cryptocurrencies like Bitcoin and Ethereum. PoW uses computational power competition between nodes in solving a mathematical puzzle [67]. For each round of consensus, the winner is given both rewards and power to create the next block in the Blockchain [55, 68, 69]. A new round would start, increasing the size of the Blockchain indefinitely. PoW has a major flaw where it causes huge wastage of power for the calculation [46].

This wastage of power extends to IoT devices being unable to compete with high computing power [70]. The complexity of the calculation is determined by the overall computational power of the Blockchain [69], and the length of the chain is proportional to the amount of workload [68]. All of these flaws of power wastage and high computational power requirement makes PoW not optimized enough to be chosen for reaching consensus in a Blockchain.

4.1.2 Proof-of-elapsed time (PoET)

PoET is a consensus algorithm that functions similarly to PoW, where it requires computation power to solve a calculation to create the next block. PoET differs from PoW, where there is no competition between stakeholders in solving the calculation. A winner is chosen based on whoever expires first from a random waiting time. PoET also has a considerably lower need for power consumption and sports a low latency and high throughput, making it a potential protocol for the decentralized Internet and particularly for IoT devices with limited resources [71]. Although an issue arises, as PoET's verification process is dependent on Intel's Software Guard Extension (SGX) [72], thus making the consensus protocol having a centralized point, hence defeating the purpose of being a decentralized network.

4.1.3 Proof-of-search (PoS)

PoS uses the wasted power formed from PoW to calculate and give optimization solution for the Blockchain [73]. The PoS is designed to offer computational service within a grid computing infrastructure, which is suited for large networks like data centers. However, the PoS process requires each node to check large amounts of plausible optimized solutions. This presents a problem with large computation requirements, where it would hinder the performance and compatibility with IoT.

4.1.4 Proof-of-authentication (PoAh)

PoAh is a consensus algorithm that targets IoT [74]. PoAh removes the reverse hashing function in favor of utilizing an energy-efficient lightweight block verification method. The verification process of PoAh would authenticate the block and the source of the block. A node gains a trust value after completed a verified transaction. The trust value is a core part of the PoAh consensus protocol. PoAh is also scalable enough to integrate fog computing and edge infrastructure, due to its efficient verification. For PoAH to be able to benefit from future technologies while maintaining a lightweight consensus method, makes PoAh to be a viable consensus protocol.

4.1.5 Proof-of-property (PoP)

PoP is a lightweight and scalable consensus protocol that provides "proof" for properties within the data structures of Blockchain [75]. This "proof" is tied to the unique addresses of the node. The "proof" stores the state of the Blockchain in every newly created block, which is a concept from Ethereum's design. PoP is energy-efficient due to the "proof" design that allows the nodes to lessen the amount of information needed for every transaction. PoP would be a possible candidate for usage in IoT due to its reduced storage and processing power needed to join the Blockchain. However, PoP has not yet been successfully applied in the industry and requires more time to be developed. Thus, making PoP not a choice due to its infancy phase.

4.1.6 Other proof-based consensus

Despite many consensus algorithms to pick from, there is also a list of consensus algorithms that fall in the latter categories of not applicable. Such categories of consensus algorithm have gimmicks such as depending on specific data like cryptocurrency to function or depending on a node that has the most active hour in the Blockchain. This need for features within the consensus algorithm is seen as not desirable in the Internet architecture, as it only creates more complex transactions that will have no benefits. Consensus algorithms like Proof-Of-Stake (PoS), and its variants of Leased Proof-Of-Stake (LPoS) and Delegated Proof-Of-Stake (DPoS) are dependent on the usage of monetary values like cryptocurrencies as a stake. These three protocols require further development before it can be used practically in the Blockchain [71, 76]. There are also other consensus protocols that revolve around the need for utilizing monetary concept as well, Proof-Of-Importance (PoI) where it prioritizes nodes with more activity in the network which can potentially be adapted but needs more research [68, 71], Proof-Of-Burn (PoB) where it uses the concept of burning monetary values, Proof-Of-Capacity (PoC) where it requires a large volume of storage [71, 76], Proof-Of-Activity (PoA) whereby it can experience a higher level of delay which is not suitable for delay-sensitive computers [76, 77], Proof-Of-Weight (PoW) where it depends on the amount of crypto coins a stakeholder possesses [76], Casper which is an adaptation of PoS but is incapable of handling challenges that are present in IoT [71], and lastly Proof-Of-Luck where despite its system being fully randomized and energy-efficient, its

computation efficiency is not high enough to accommodate for IoT [72].

4.2 Voting (Byzantine-based) consensus

The concept of the Byzantine based consensus revolves around tackling the concept of the Byzantine General Problem, whereby in Blockchain's scenario, a node may fail and return leading false messages for the system and user [76]. This concept is usually referred to as the Byzantine Fault Tolerance (BFT) when used as an algorithm. The Byzantine-based Consensus takes into account of false leads or voting in the voting process when reaching consensus.

4.2.1 Practical Byzantine fault tolerance (PBFT)

PBFT was the first system from 1999 proposed to solve a transmission error with its efficient algorithm [68] where it provides high throughput, low latency, and lowered power usage as compared to PoW [78]. This results in PBFT being favorable for IoT networks [71]. PBFT requires all the nodes to take part in the consensus process, and only need 2/3rd of all node's agreement to reach consensus. However, it lacks scalability to work in a permissionless Blockchain due to its limited scalability caused by high network overhead and a low tolerance for exploits [71].

4.2.2 Delegated Byzantine fault tolerance (dBFT)

The dBFT applies similar techniques from PBFT with the addition of not requiring the participation of all nodes, rendering it more scalable than its predecessor. A quirk with dBFT is that certain nodes are chosen to represent others or a group of nodes. Despite the scalability improvement, the network performance is not within an acceptable range due to its 15 s of average latency for creating new blocks in the Blockchain [71]. Thus, making dBFT not suitable as a candidate for reaching consensus in the Blockchain due to its slow performance.

4.2.3 Stellar consensus protocol (SCP)

SCP uses a variant of PBFT called Federated Byzantine Fault Tolerance (FBFT) and is a publicly opened decentralized protocol [71]. SCP allows complete "freedom" for the nodes to trust one another. This "freedom" of trust is used for assisting the process of reaching consensus. SCP calls a set of nodes a quorum, and a quorum is made up of multiple quorum slices. A quorum slice represents the trust between nodes. This binding of quorum slice forms a web-like structure in a P2P fashion [67]. SCP can offer both high throughput and low power usage but suffers from

latency issues caused by significant network overhead. There is also a lack of security for the specific scenario of selecting an incorrect quorum slice to connect. Both of these issues cause SCP to be not suitable for reaching consensus.

An alternate to SCP is Ripple, which is capable of reducing the latency for the Blockchain. Ripple can tolerate up to 20% of faulty nodes. Despite the focus on solving the latency issue, Ripple is aimed for monetary purposes and is not fast enough for IoT [71].

4.2.4 Hyperledgers

Hyperledger is a series of open-source Blockchain projects [79] that has huge backing from big technology providers such as Linux and Intel. Certain projects within Hyperledger does have interesting options to consider. These Hyperledger projects are aimed directly at permissioned Blockchains. Hyperledger Fabric is a distributed ledger protocol that is run by peers within the Blockchain [67]. However, the design of Hyperledger Fabric, even as of now in version 2.0, operates in a distributed manner with certain aspects needing certifications created by a centralized point with a Smart Contract called Chaincode [80]. This makes Hyperledger Fabric not ideal for decentralization due to its dependence on a singular service. Hyperledger Sawtooth is still in its infancy stage, as it requires more development before it can be taken into consideration. Hyperledger Indy has a lack of notable features to be used as a use case. Hyperledger Burrow has an issue where networks may halt due to the lack of specific roles within the Blockchain [71] as the Hyperledgers needs a "leader" within the permissioned Blockchain to reach a consensus [67], making it not suitable for reaching consensus in the Blockchain with its reliance of a leader. Hyperledger Iroha might instill some promises with its mobile design, making it compatible with IoT.

4.2.5 Proof-of-authority (PoA)

Despite it being part of the Proof based consensus protocols, its design is based on BFT. PoA is a solution for solving PoW's issue of high latency, low transaction rate, and power wastage. PoA is designed to restrict the creation of new blocks to a fixed set of nodes that are selected with the Byzantine method [81]. This restriction of creating new blocks makes PoA designed for an enclosed network system with an administrator. The need for an enclosed network and an administrator in PoA, makes it not a suitable choice for reaching consensus in the Blockchain, considering everybody should have access to the Internet.

4.3 Voting (crash-based) consensus

The crash-based consensus algorithm is a sub-category of Byzantine-based consensus that tackles "crash failure". This "crash failure" refers to a crashed node not being able to recover by itself. But these crashed nodes are taken into account when reaching consensus. Unlike the Byzantine-based, this type of consensus is not capable of sustaining a full 100% crash tolerance for the Blockchain system.

4.3.1 Paxos

Paxos is a highly theoretical consensus algorithm that was one of the first few consensus protocols that were proposed [78]. Due to its theoretical nature, Paxos is challenging to understand and implement as a system [76]. Paxos has a crash tolerance level of up to 50% [71], hence why it is a crash-based consensus algorithm. Paxos was designed for smaller enclosed networks, which makes it not suitable for Internet implementation. However Paxos's safety feature in its balloting and anchoring system would be useful for the Internet and IoT [82]. Paxos's design comprises of two main roles, the leader and the follower. Depending on different documentations, there are as many as five roles in Paxos. The leader is chosen by the follower's ballot and makes progress within the protocol. The follower acknowledges the leader and provides its vote to the leader. A major issue lies in the leader role dominating the follower role. This issue makes Paxos run in a centralized-like way despite the possibility of being implemented in a distributed way.

4.3.2 Raft

The Raft algorithm is an attempt on trying to make Paxos more accessible and easier to understand and implement [71, 78]. Raft achieves the same effect and efficiency of Paxos, but with a lower crash tolerance level of 40% [67]. Since Raft follows a similar architecture of Paxos, this results in the same issue of a dominating centralized leader role.

4.4 Usability of consensus algorithm

Three algorithms stood out as potential candidates and are suitable for an ideal decentralized Internet architecture, they are PoP, Paxos, and PoAh. PoP has a reduced need for storage and processing power. It is a strong contender due to its association with semantic technology for providing identities to properties of data structures. However, PoP suffers from a lack of practical testing, requiring further development. Paxos is the second choice due to its

potential for applicability. It has a history of being adapted to a wide array of systems, making it highly reputable for repurposing. Nevertheless, Paxos suffers from the difficulty of understanding its protocol and implementability. Making Paxos a plausible solution, but requiring a development team to modify Paxos for Blockchain. Finally, PoAh fits the criteria of being robust, scalable, and secure enough to handle the Internet, IoT, fog computing, and edge infrastructure. PoAh's trust system is an effective tool for establishing trustworthy nodes to interact on the Internet while maintaining equal voting power between all nodes. All these factors make PoAh a suitable candidate for decentralizing the Internet. The identification of the consensus algorithm for the decentralization of the Internet architecture would provide the needed protocol for ensuring decentralization between roles. What is left to consider is Blockchain with its limitation from Sect. 3.5 and how it can be resolved by incorporating other emerging technologies.

5 Blockchain and future internet technologies

Internet technology is constantly evolving and it is important to explore the opportunities for integration of the Blockchain with these future technologies. This evolution of internet includes the implementation of different systems and protocols to work together. Blockchain can also adopt a similar strategy by bringing together other internet technologies to improve the overall Blockchain system model. IoT is increasing in presence within the industry, making it a relevant technology that would impact the hardware requirement for the participating nodes of the Blockchain system. Since its conception, Cloud Computing has been an effective network and resource sharing technology. This makes it an ideal technology for connecting Blockchain to IoT through appropriate resource allocation. Graphchain is a developing technology that improves Blockchain, and opens up the possible alternate solution of a Graphchain-based Internet. Edge Computing and Fog Computing are technologies that enhance Cloud Computing by providing equal performance for nodes connected at the "edge" of the Internet. P2P technology is associated with the early days of file-sharing, making it vital to understand the sharing of resources between peers in a Blockchain. Lastly, Data Networking covers possible architectures that can replace the current TCP/IP architecture and change how information data would be connected. All of these topics as illustrated in the Fig. 5 will be covered in this section.
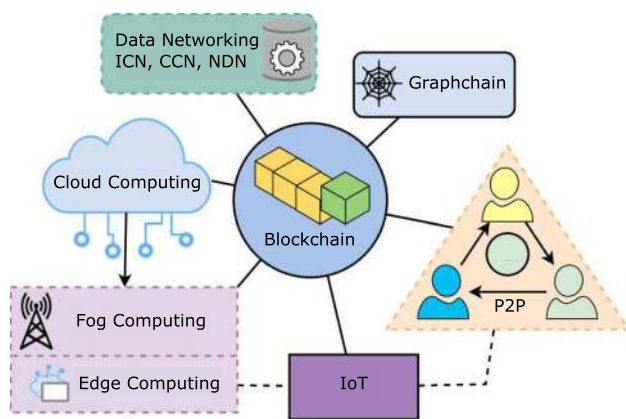
Fig. 5 The relationship between Blockchain and other Internet Technologies

5.1 Internet of things (IoT)

IoT has established a new standard for current internet technology by pushing the connectivity of the Internet to smart devices. This new standard of connectivity enabled smart devices results in a centralized massive architecture [83] . However, implementing IoT into Blockchain would expand how a node can take part in the Blockchain. This expansion is achievable with smart devices replacing traditional desktop computers as Blockchain nodes. This expansion also provides an increase in scalability for Blockchain. IoT has a major challenge that multiple different devices need to act as different main-in-the-middle for operations within the network [84]. There are no existing communication standards for IoT between different types of smart devices. This could lead to limitations in storage and computation power. Thus introducing the need for dedicated servers and infrastructure catered for IoT devices. But this challenge can be overcome with the implementation of resource provisioning through cloud computing.

There has been several research studies for implementation of Blockchain [85, 86]. However, some of these research has the drawback that the test cases use cryptocurrency reliant blockchains and consensus algorithms. Since IoT will be a key technology that is already in the process of becoming the new norm, it would be crucial to implement IoT into Blockchain. Nevertheless, current implementation methodologies would need further research for proper integration.

5.2 Cloud computing

Cloud computing with its power of resource pooling and virtualization is a new generation of network technology. IoT has many similarities with Cloud computing since both principals center around increasing efficiency for network operation. Cloud computing would also solve some of the challenges with IoT [87, 88]. The efficiency and performance of verification processing for the nodes in the Blockchain can be increased by implementing IoT and Cloud computing. The integration of Cloud computing by itself would also increase security, scalability, and the lowering of data storage for transactions in the Blockchain. Much of these efficiency increases could allow the integration of more types of consensus algorithms with lowered requirements of data storage and network overhead. Currently, cloud computing is used in a distributed state that is composed of multiple components within the network, where it is used to maintain fail-safe protocols [89]. Blockchain technology can inversely help security for cloud computing by making the information and data in the cloud storage to be immutable, persistent, and decentralized [90, 91].

There has been studies combining the inevitability of Blockchain, cloud computing, and IoT converging into Blockchain-of-Things (BCoT) as part of the evolution of the internet and a future infrastructure [92]. Cloud computing has the potential to be adapted as a service for the future Internet [93]. However, there is an issue with the communication protocol between cloud computing, IoT, and Blockchain. There are no standardized communication protocols for all three technologies to communicate with each other [94]. This makes the development of the protocol a priority before it can be integrated with Blockchain or IoT.

5.3 Graphchain

Graphchain is a technology that replaces the network structure of Blockchain with a graph data structure [59]. Graphchain is considered an improved version of Blockchain. Graphchain uses the same components of Blockchain but implements a decentralized graph rather than a linear chain resulting in a self-scaling and self-regulated cross-verifying transaction framework [58]. Graphchain disseminates the transaction data in "data shards" between multiple nodes in the graph. Thus, rendering it effectively scalable resulting in high-performance. Graphchain also has the benefit of using parallel mining [59] for increased performance and transaction processing. Graphchain is capable of being implemented with semantic technology of providing relations and "meaning" for the data structure to enhance the distributed ledger component [45]. But, there is an issue with Graphchain. Despite the necessity of assuring a decentralized system, centralization could result within a Graphchain due to a common descendant being shared between all newly created transactions [58]. This centralization issue could be overlooked in comparison to

the benefits Graphchain would provide for the decentralized Internet.

5.4 Edge computing

Edge computing is a system designed by Cisco in 2014 to expand cloud computing by distributing cloud resources to the "edge" of the cloud network, forming an "edge" cloud [92]. Edge computing centers around the concept of reaching the "edge" of the network. Edge computing operates similarly to Fog computing, as both technologies give benefits of scalability, security, and performance. The interaction between the two is demonstrated in Fig. 6 [92, 95]. Edge computing can be implemented into Blockchain to tap into the edge processing capabilities of the public architecture. Edge processing would be able to offer nodes connected at the "edge" of the network to have the same computation speed as nodes closer to the core network. This integration has so far been only tested in permissioned Blockchain types [96]. There is a need to investigate the same for permissionless Blockchains.

The ability to pool resources from public architectures would enable edge computing to work effectively with technologies centered around the network and architecture.
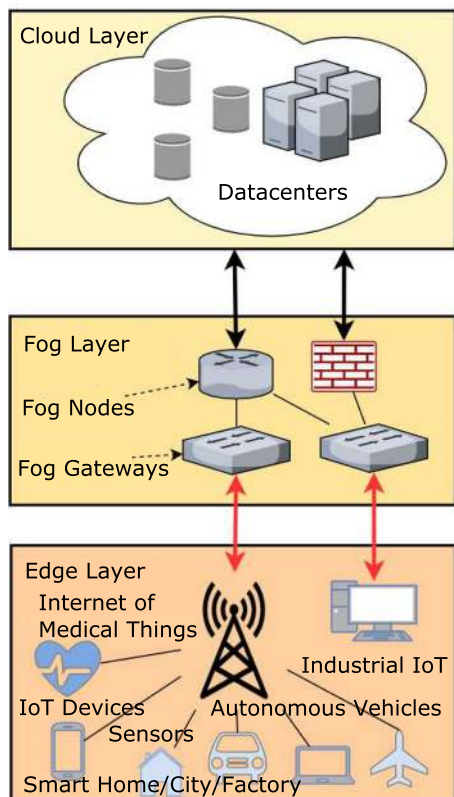
Fig. 6 The relation between fog computing and edge computing

This brings Software Defined Network (SDN) and Network Function Virtualization (NFV) [95] as relevant future technologies to be considered in this study.

5.5 Fog computing

Fog Computing is described as a system-level architecture distributing services and resources of computing, control, storage and networking anywhere with the continuum from Cloud to Edge [97]. The communication devices like switches and routers in this architecture are able to provide various communication and computation features with their extended computational and storage resources. The control, computing, data, security, and networking levels will allow for a robust standardization, unification, and convergence under this computing paradigm. This could give efficiency when implemented into Blockchain cutting the necessary storage for network communication and transaction for both IoT and Blockchain. The design of fog computing is based on removing the distance and performance needed for network traffic. But its intentions are driven by marketing, mainly leveraging user interaction via advertising, entertainment, and Big Data analytical applications [95, 98]. A notable flaw with fog computing is that its fault tolerance level has not been extensively studied. The only results available on fault tolerance for fog computing in the current literature are for node failures [99]. This flaw could be resolved by implementing fog computing into Blockchain, by partitioning fog node clusters using fog nodes within a Blockchain [100]. This forms a Blockchain-based fog node cluster that uses a consensus algorithm to work with any computers in the network. This implementation also provides an increased level of machine-to-human communication, which is beneficial for IoT [101]. There is also network storage cost to consider, as fog computing would need to account for Big Data. Big Data could result in performance bottleneck problems for the network affecting both fog computing and cloud computing.

There are two possible solutions for this performance bottleneck problem. The first solution is to have a federated learning Blockchain to assist fog computing [102]. This solution provides increased security and efficiency for the Blockchain suitable for decentralized privacy protection. The alternate proposal is fog computing being implemented with a novel "Plasma" framework Blockchain [103]. This "Plasma" framework enables fog nodes in the Blockchain to allow IoT to connect into the Blockchain. This solution solves the bottleneck by removing the need for large overhead storage or computation power for network transmission.

5.6 Peer-to-peer (P2P)

P2P technology is prevalent with Blockchain due to its association in the distributed network. P2P was popular in the age of privacy when it was used for file sharing between users. P2P provided a platform of anonymity which symbolized complete freedom on the Internet. This opened up entirely new issues of digital piracy and DMCA. P2P is described as a peer being able to share resources with other peers in the network while maintaining equal roles and privileges within the network. P2P has an association with IoT for enabling both anonymity and decentralization at the cost of storage issues [15]. But, there is a clear decline of pure P2P applications and software within the past years [36]. Blockchain with permissioned consensus may have the key to revitalize the decentralization of P2P and provide increased trust and dependability [36].

5.7 Data networking

Despite the focus on having decentralization where every user is equal and not adhere to a central figure, network configuration plays an important role in standardization. Without this standardization, a multitude of issues may arise from performance hindrance due to conflicting protocols, increased cost to accommodate different configurations, reduced scalability and reliability due to conflicting configurations. This brings in a difficult position of requiring authoritative management to ensure both management and standardization of the network. The network configurations are maintained with network management applications. Network management applications have many approaches for handling networks. Each approach provides a different set of administrative and performance advantages. In a traditional network scheme, the Internet would operate similarly to a core network and allow computers to participate via the network infrastructure of ISPs and data centers. But this scheme is avoided in the industry due to the need for expensive new equipment, accounting clunky inherent configurations, and maintenance of the infrastructure. Therefore, a dynamic, scalable, and cheaper alternative is required for maintaining the network.

5.7.1 Software-defined networking (SDN)

These days, SDN has been loosely used by the networking industry for defining any network architecture that is operated by software. The original definition of SDN involves four components [104, 105]:
1. The ability to remove the control functionality for network devices.
2. Usage of OpenFlow protocol, for its flow-based forwarding decision. This protocol is used to direct and manage network traffic between routers, switches, and vendors.
3. An external controller which is a software platform that facilitates the control functionality while acting as a virtualization and resource vendor
4. The ability of programming software application to operate on top of the controller and interact with underlying data plane devices

The main attraction with SDN is its programmable feature to allow customizability to configure the network. SDN provides a dynamic configuration that operates from a central controller to be more efficient and customizable from the traditional network infrastructure. When fog computing is implemented with an SDN-enabled Blockchain by deploying fog services, studies have shown that there is an increase of performance and security for offloading data to the cloud while being cost-efficient [106]. This implementation would result in a distributed Blockchain. This architecture uses controllers within SDN to enable fog computing to offer low cost, secure, and on-demand access to edge nodes in the Blockchain. This proposed system would be scalable and secure enough to accommodate the expansion of IoT and the volume of data on the Internet and enable on-demand for low latency IoT devices. SDN's Architecture and routing can be seen in Figs. 7 and 8.

5.7.2 Information-centric networking (ICN)

Information-Centric Network (ICN) is an alternate approach that centers around content data that is suited to the interest of the network [107]. ICN provides a cost-efficient and scalable method of handling the global expansion of IP traffic with its secure design of persistence and unique naming scheme for the data information. ICN consists of three components.

The first component is the Named Data Object (NDO). This is a self-certifying name method applied to metadata of an information data to give a unique identity. NDO consists of a unique identifier, the data, and the metadata [108]. NDO adopts two types of naming schemes. Both of these offer unique names and security for the NDO. The first naming scheme is a hierarchical scheme that provides an aggregated approach for prefixes of the NDO. The second naming scheme is a self-certifying scheme which is implemented by embedding a hash containing the prefixes into the data [109].

The second component is the Naming and Security of the information data, which encompasses the concept of establishing the identity of independent information data
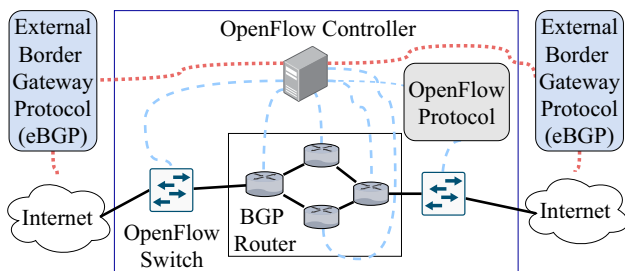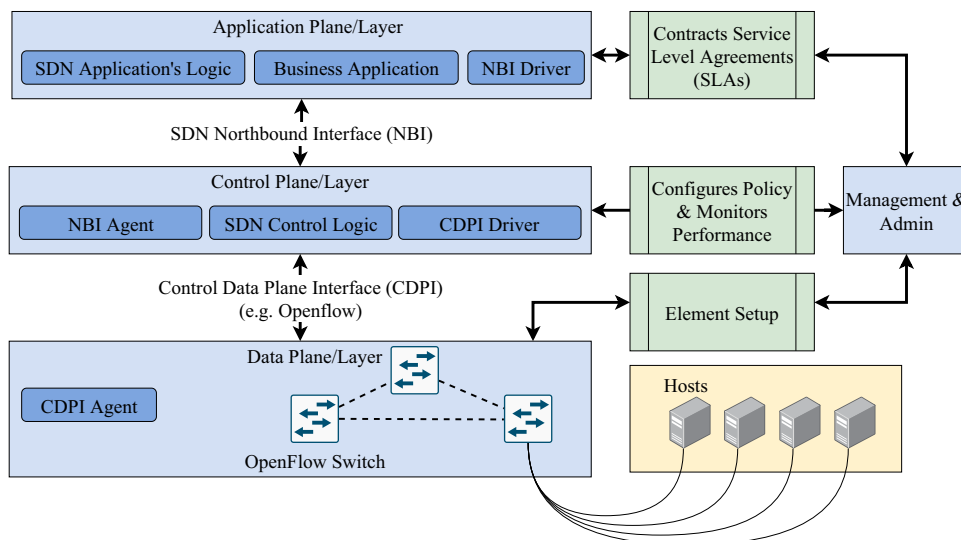
Fig. 7 SDN architecture

Fig. 8 SDN routing

that is outside the network [109]. This component consists of two schemes as well. The first scheme being Name Resolution Service (NRS) where it uses an external entity to interpret the name of the NDO after mapping the named data. But NRS suffers from a single point of failure due to the funneling of information data to an external entity for interpretation. The second scheme revolves around direct routing from the data requester to the data source of the network. This is heavily dependent on algorithms to find the properties needed to identify the namespace for both the requester and the data source.

The third component is the Application Programming Interface (API), which is used to request and deliver NDO around the network [109]. The node that provisions the NDO is called a source/producer and controls the publishing of the NDO in the network. NDO is requested by client/consumer calling its name, through a request, finding, subscribing, or setting one of NDO's metadata as an interest. There are many approaches for managing how NDO is requested, from PSIRP where it is built on a subscription-based approach or CURLING where it supports location parameters.

The fourth component is caching, which is used to satisfy NDO requests by allowing nodes to hold a copy of the

NDO in its cache. This application of caching allows ICN to apply edge computing and P2P for an in-network edge of "transparent web cache". Although the caching is simple by design, this can be improved with edge caching. As simulations have shown that current caching can be improved with edge caching to accommodate IoT for increased efficiency of data distribution for the ICN [108].

5.7.3 Content-centric-networking (CCN) & named-data networking (NDN)

The CCN is an architecture that is part of the ICN that centers around making content nameable and routable within the network. CCN communicates in the network through named data, as opposed to TCP/IP's approach of using IP addresses [110]. CCN is able to improve the existing method of routing and forwarding from TCP/IP due to the named data. This improvement is achieved by computers fetching data with appropriately labeled names. This is later improved with Named Data Networking (NDN).

NDN is an evolution of CCN where it uses the same approach of communication as CCN with named data [111]. NDN is designed to take advantage of rising new technology to meet the onset of demands such as Big Data that would make TCP/IP obsolete [111]. The vision of NDN is to reshape the hourglass structure in TCP/IP by replacing IP with Content Chunks that are named data [112] as shown in Fig. 9. NDN can combine the networking aspect, storage expansion for the onset of Big Data, and the process of fetching data into a unified system. This helps to match and even exceed TCP/IP in meeting challenges of IoT on the network layer [113]. NDN would give IoT a scalable, secure, energy-efficient, and heterogeneous system due to its functionalities. This benefit for

Fig. 9 The IP and NDN architecture hourglass
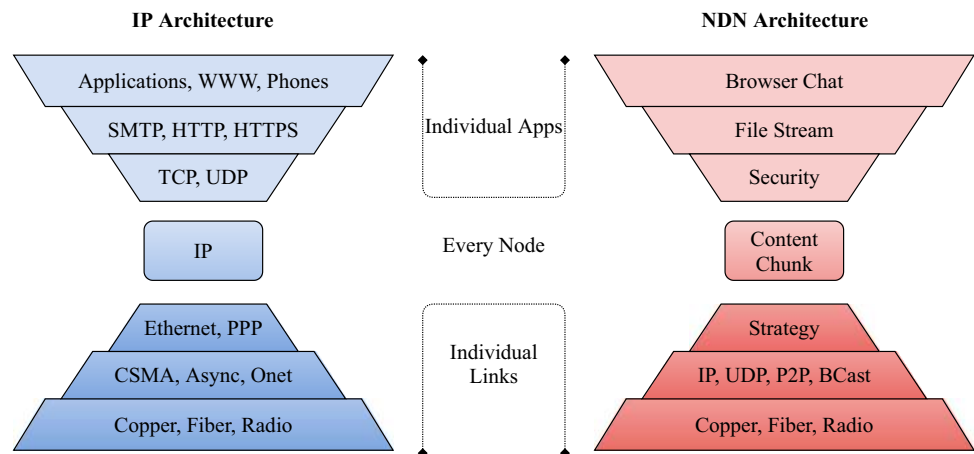
IoT is also further reinstated with the proposal of introducing Fog Computing with NDN [114]. This results in a smarter and more efficient approach in storage and resource provisioning to increase the performance of data transmission, caching, and improved security on the NDN.

It seems that NDN draws parallel to how Semantic technology is applied to the TCP/IP architecture in its concept of naming data. This parallel makes NDN capable of accomplishing the melding between Semantic technology and TCP/IP architecture with naming data chunks on the Internet by providing links, relevancy, and meaning to the data chunks.

6 Discussion

New ideas and iterations of systems being discussed for development evolve constantly in the current tech industry. This could lead to decisions being made for dictating the directions of how Blockchain technology is utilized in the tech industry. This section initially discusses the trade-offs between technology. The trade-offs can be considered as an ongoing discussions for adopting new technologies to replace and improve legacy systems. These trade-offs could lead to new standardization of the future industries, and the decisions to adopt Blockchain technology as a new norm. This section further discusses the relationship between the Internet and the impact of decentralization. The details include importance of decentralization and why the monopolization from ISP should not be allowed. Next, the development trends that are seen currently within the tech industry are discussed. This is an important topic as centralization from IoT and development of quantum computing poses a unique situation for the future development of the Internet. The next topic revolves around re-centralization from the Internet, where the possibility of centralizing from the decentralization within Web 3.0 is

discussed in detail. The next topic discussed is the battlefield implementation with IoT. Gathering and utilization of battlefield information through current and future technology such as Graphchain and NDN would enable the next step of cyber warfare. The last topic in this section is the Merkle Tree which is used for the encryption of information to be stored in a ledger. As the Merkle tree is the only hash-based data structure used in Blockchain, would there be other alternatives to replace Merkle Tree like the proposed Verkle Tree [115]?

6.1 Trade-off between technologies

Trade-offs are always a concern when implementing new technologies to replace a new architecture, that is why there are different proposals for achieving Web 3.0. In our case, Blockchain has trade-offs occurring with the future technologies that we have proposed in Sect. 5. There are two notable trade-offs that need to be decided from this paper.

Graphchain is considered as an upgrade version of Blockchain in terms of optimization. However, there is a trade-off with Graphchain, where the optimized routes will eventually be centralized due to the route taken with common descendants. This makes the decision to decide how centralizability should a Blockchain have for Internet architecture. There is also the case of cloud computing's standardization, where there is a risk of reduced performance and scalability if we use middlewares for communication standardization. Deciding which technology to implement would be a challenge on itself, as balancing the trade-offs between technologies would be a hurdle in the advancement of developing the internet architecture.

6.2 Relationship between the internet and decentralized infrastructure

The push for a decentralized architecture has resided within the Internet community, only to be reinforced with the incident from Net Neutrality. ISPs have complete control over the user's Internet with its monopolization of network flow for users connecting through the Internet, which was further discussed in Sect. 2.2. This monopolization from the ISP allows exploitation and abuse from large corporation. With how much personal information being linked due to social media's influence, it's no surprise that it is easy to trace a user's personal information based on techniques like social engineering. A decentralized architecture is the proposed solution, where its anonymity is used to prevent misuse of personal information. This leads to the outcry of having a decentralized architecture to distinguish users away from needing a centralized node, despite the drawbacks came from the initial first generation of Blockchain.

6.3 Development trends

The current trend of the Internet is driven by the impending arrival of IoT. As the days of bulky computers are gone, comes the influx of new smart devices that would interact with the Internet architecture. Now the question lies on how the IoT interacts with the proposed Blockchain Internet architecture. One trend that is consistently shown in news outlets is smart devices being linked with each other in a network to form a high-tech lifestyle where smart devices connected in the network can be operable with a single smart device. Another future trend is quantum computing, as it brings optimization features for the future decentralized Internet with its quantum communication. Quantum communication would be able to outperform the limits of traditional sender-receiver communications. This communication is done by entangling quantum nodes to multiple levels of entanglement, which results in a heterogeneous multi-level entanglement network structure [116]. This network structure would result in an efficient decentralized routing, which would be beneficial with the onset of exponential growth in information in the future Internet.

6.4 Re-centralization

Although the goal of this paper is to achieve decentralization for a future internet architecture, it brings up the question of how the Internet developed into its current centralized state. Web 1.0 was designed to be decentralized, only to be centralized in Web 2.0. This migration to

Web 2.0 brought new centralized services that allowed the Web to have more functions and be more optimized than Web 1.0. The real challenge comes during the implementation of the decentralized Web 3.0 or dWeb. Would it be possible to offer the same optimization and efficiency of the centralized services, but in a decentralized manner? A major aspect to consider is the personal data of a user, where a centralized architecture would provide a higher quality of life in personalization of applications and advertisements based on personalized information and profiling of users. But in the event of removing this feature to allow complete decentralization of the architecture to be an acceptable loss? This trade-off of quality of service would occur during the migration towards decentralization. Unless a new design of architecture that can preserve the services while maintaining a decentralized Internet is proposed, this would remain a huge issue. This is a huge conundrum in itself with personal data, as a decentralized architecture would present a situation where nobody could be held accountable for events that occurs. This brings the discussion of the practicality of data centers, with current investors steering towards the idea of investing in bigger data centers to account for the exponential growth of information on the Internet. However, with a Blockchain-enabled decentralized architecture, it would be possible to implement the services of data centres into individual nodes of the Internet, ensuring a probable solution that is cheaper, scalable, and efficient. But diving into a purely decentralized Internet would not be an ideal setting in the current world's reliance on a centralized governing figure such as the government and financial banks. This is caused by the concerns disruption of balance in their respective industry due to no governing forces as any updates are done via majority voting without a supervision forces. A balance is needed to provide for both centralized and decentralized in this aspect, as a purely decentralized network without a governing figure would ensure possible chaos without supervision.

6.5 Battlefield implementation with IoT

In the onset of a decentralized infrastructure, a unique situation comes from the attempted implementation of IoT into future battlefield situation with relevant network technology such as Graphchain and NDN [117, 118]. By incorporating information data about battlefield information such as ammunition, troops, and enemy intelligence, this would change how current warfare is engaged. Information plays a vital role in the battlefield, as it provides benefits on how a commander would able to make quick and decisive tactical decisions based on on-site real-time information. Incorporating military aspects into a decentralized network infrastructure with Blockchain

implementation seems to be a possible future. Integration of cyber warfare is already in the present, so it would be the next step of information warfare.

6.6 Merkle tree

The Merkle tree is an important hash-based data structure used for optimized distribution and verification of the hashed ledger in Blockchain. This data structure allows each node to optimize the storage of multiple ledgers. This Merkle Tree is also used in the projects that are mentioned in Sect. 2.3 for encoding files to be distributed around the decentralized network.

The Merkle tree is used to encrypt multiple information many times to reach an eventual Merkle root, which houses multiple information of a single ledger. This Merkle root is then used to verify the integrity of the ledger for every decryption that has been executed on the ledger, to verify the hash's information. This brings the question of Merkle Tree being the only option for encryption in Blockchain, and if there are any other alternatives or optimized encryptions that can be considered. Although the Merkle tree can be re-purposed into a file system [119] where it is a decentralized network of P2P and is capable of being expanded, this would result on relying Merkle Tree as the only solution. Alternative encryption has been proposed with Verkle Tree [115], where it can optimize and reduce the bandwidth needed for consensus protocols to communicate in the network. However, Merkle Tree is still in its testing phases with limited resources and results shown, therefore leading us back to the Merkle Tree. This brings us back the question of would there be an alternative in encryption of the ledger that is better than the Merkle Tree.

7 Related work

Throughout the years on Blockchain technology, the technology itself has been surveyed and constantly monitored thoroughly. Blockchain has amassed to a technology that is capable of being integrated into numerous technology since its initial conceptualization and inception from Satoshi Nakamato's paper [120]. It has continued to be expanded for more usage in tandem with other technologies. Current literature encompasses reviews of Blockchain technology for different purposes, applications, research areas, and research problems [46, 121, 122]. Several works have explored and investigated capabilities of Blockchain for Internet of Vehicles (IoV) [123], Internet of Things and the edge networks [124–126]. However, to the best of authors knowledge, very limited research has been performed to study Blockchain's capabilities and potentials to enable decentralization for the Internet and core networks.

Hassan et al. [127] aimed to provide a guiding reference manual in a generic form on the subject and presented a survey of blockchain-based network applications discussing their applicability, sustainability and scalability challenges. Chowdhury et al. [128] provided a generic short review on blockchain technology for decentralisation of Internet without discussing details of Internet challenges/issues and Blockchain capabilities to address those issues while ignoring the impact of other emerging technologies on both Internet and Blockchain.

8 Conclusion

This paper delved into the recommendation of Blockchain and how it is an effective enabler in achieving a decentralized Internet. Although there are other methods of achieving decentralization, we are confident with the choice of using Blockchain as an enabler to decentralize the Internet. From this paper, we understood that the current Internet architecture suffers from a myriad of issues as discussed in Sect. 2.2, and proposed that using Blockchain would solve those issues. It is also discovered that the consensus algorithm would play a vital role in determining the level of power a node holds within the network, and how the network should communicate. From the list of consensus algorithms that have been discussed in Sect. 4, three algorithms which are Proof-Of-Property, Paxos, and Proof-Of-Authority, stood out as options for handling the nodes in the Blockchain. With upcoming technologies being constantly introduced into the industry, there would be better and more optimized technologies that can replace the proposed technologies that have been proposed in this paper.

From this study, we have identified and investigated two important Blockchain research aspects that provide key roles in feasibility of achieving a decentralized Internet using Blockchain. First, being the consensus algorithms that provide the needed decentralization but in factors of different optimization and achieving consensus. Second, the relevant technology which would reduce the flaws of Blockchain and help Blockchain to succeed in decentralizing the Internet. The survey that this paper has provided on Blockchain will help in providing coordination in achieving decentralization for the Internet.

Data availability The authors declare that all data supporting the findings of this study are available within the article.

References

1. Alazab, M., Alhyari, S., Awajan, A., Abdallah, A.B.: Blockchain technology in supply chain management: an empirical study of the factors affecting user adoption/acceptance. Clust. Comput. **24**(1), 83–101 (2021)
2. Pavithran, D., Shaalan, K., Al-Karaki, J.N., Gawanmeh, A.: Towards building a blockchain framework for iot. Clust. Comput. **23**(3), 2089–2103 (2020)
3. Li, H., Pei, L., Liao, D., Wang, X., Xu, D., Sun, J.: BDDT: use blockchain to facilitate IoT data transactions. Clust. Comput. 1–15 (2020)
4. Khalid, U., Asim, M., Baker, T., Hung, P.C., Tariq, M.A., Rafferty, L.: A decentralized lightweight blockchain-based authentication mechanism for IoT systems. Clust. Comput. 1–21 (2020)
5. Attaran, M., Gunasekaran, A.: Blockchain-enabled technology: the emerging technology set to reshape and decentralise many industries. Int. J. Appl. Decis. Sci. **12**(4), 424–444 (2019)
6. Abbasi, M.A., Memon, Z.A., Durrani, N.M., Haider, W., Laeeq, K., Mallah, G.A.: A multi-layer trust-based middleware framework for handling interoperability issues in heterogeneous IoTs. Clust. Comput. 1–28 (2021)
7. Elkhalil, A., Zhang, J., Elhabob, R.: An efficient heterogeneous blockchain-based online/offline signcryption systems for internet of vehicles. Clust. Comput. 1–18 (2021)
8. Balakrishnan, H., Banerjee, S., Cidon, I., Culler, D., Estrin, D., Katz-Bassett, E., Zegura, E., et al.: Revitalizing the public internet by making it extensible. ACM SIGCOMM Comput. Commun. Rev. **51**(2) (2021)
9. Hendler, J.: Web 3.0: the dawn of semantic search. Computer **43**(1), 77–80 (2010)
10. Alabdulwahhab, F.A.: Web 3.0: the decentralized web blockchain networks and protocol innovation. In: 2018 1st International Conference on Computer Applications Information Security (ICCAIS), pp. 1–4 (2018)
11. Raman, A., Joglekar, S., Cristofaro, E.D., Sastry, N., Tyson, G.: Challenges in the decentralised web: the mastodon case. In: Proceedings of the Internet Measurement Conference, IMC'19, page 217–229, New York, NY, USA. Association for Computing Machinery. ISBN 9781-450369480. https://doi.org/10.1145/3355369.3355572 (2019)
12. Wang, X., Li, K., Li, H., Li, Y., Liang, Z.: Consortiumdns: a distributed domain name service based on consortium chain. In: 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pp. 617–620 (2017)
13. Ren, S., Liu, B., Yang, F., Wei, X., Yang, X., Wang, C.: Blockdns: enhancing domain name ownership and data

14. Murugesan, S.: Understanding web 2.0. IT Profess. **9**(4), 34–41 (2007)
15. Conoscenti, M., Vetrò, A., Martin, J.C.D.: Peer to peer for privacy and decentralization in the internet of things. In: 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C), pp. 288–290 (2017)
16. Foley, M.J.: All about microsoft: microsoft azure customers reporting hitting virtual machine limits. https://www.zdnet.com/article/microsoft-azure-customers-reporting-hitting-virtual-machine-limits-in-u-s-east-regions/#ftag=RSSbaffb68 (2019)
17. Donnelly, C.: Coronavirus: Microsoft azure suffers datacentre capacity shortages in Europe (2020). https://www.computerweekly.com/news/252481265/Coronavirus-Microsoft-Azure-suffers-datacentre-capacity-shortages-in-Europe
18. Chowdhury, S.H.M., Jahan, F., Sara, S.M., Nandi, D.: Secured blockchain based decentralised internet: a proposed new internet. In: Proceedings of the International Conference on Computing Advancements, ICCA 2020, pages 1–7, New York, NY, USA. Association for Computing Machinery. ISBN 9781450377782. https://doi.org/10.1145/3377049.3377083 (2020)
19. St Juste, P., Wolinsky, D., Lee, K., Oscar Boykin, P., Figueiredo, R.J.: Socialdns: a decentralized naming service for collaborative p2p VPNS. In: 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2010), pp. 1–10 (2010)
20. Zave, P., Rexford, J.: The compositional architecture of the internet. Commun. ACM **62**(3), 78–87 (2019). https://doi.org/10.1145/3226588
21. Kohlweiss, M., Maurer, U., Onete, C., Tackmann, B., Venturi, D.: De-constructing TLS 1.3. In: Proceedings of the 16th International Conference on Progress in Cryptology—INDOCRYPT 2015—vol. 9462, pp. 85–102. Springer, Berlin. ISBN 9783-319266169. URL https://doi.org/10.1007/978-3-319-26617-6_5 (2015)
22. Li, Q., Qi, X., Liu, J., Han, H.: Design and implementation of traditional DNS protocol. In: 2017 International Conference on Computer Technology, Electronics and Communication (ICCTEC), pp. 1384–1390 (2017)
23. Zou, F., Zhang, S., Pei, B., Pan, L., Li, L., Li, J.: Survey on domain name system security. In: 2016 IEEE First International Conference on Data Science in Cyberspace (DSC), pp. 602–607 (2016)
24. Dong, Y., Kim, W., Boutaba, R.: Bitforest: a portable and efficient blockchain-based naming system. In: 2018 14th International Conference on Network and Service Management (CNSM), pp. 226–232 (2018)
25. Al-Jarrah, M., Tamimi, A.R.: A thin security layer protocol over IP protocol on TCP/IP suite for security enhancement. In: 2006 Innovations in Information Technology, pp. 1–5 (2006)
26. Gebraselase, B.G., Helvik, B.E., Jiang, Y.: Suitability of blockchains to enable and support networking functions: State of art. In: Proceedings of the 2019 4th International Conference on Cloud Computing and Internet of Things, CCIOT 2019, pp. 110–119, New York, NY, USA. Association for Computing Machinery. ISBN 9781450372411. https://doi.org/10.1145/3361821.3361838 (2019)
27. Chandra, D.G., Kathing, M., Kumar, D.P.: A comparative study on ipv4 and ipv6. In: 2013 International Conference on Communication Systems and Network Technologies, pp. 286–289 (2013)
28. Gu, K., Zhang, L., Wang, Z., Kong, Y.: Comparative studies of ipv6 tunnel security. In: 2017 13th International Conference on

Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), pp. 2799–2804 (2017)

29. Saraj, T., Hanan, A., Akbar, M.S. Yousaf, M., Qayyum, A., Tufail, M.: Ipv6 tunneling protocols: mathematical and testbed setup performance analysis. In: 2015 Conference on Information Assurance and Cyber Security (CIACS), pp. 62–68 (2015)

30. Macedo, D.F., Santos, A.L.D., Pujolle, G.: From TCP/IP to convergent networks: challenges and taxonomy. IEEE Commun. Surv. Tutor. **10**(4), 40–55 (2008)

31. LLC Google. Ipv6—google. https://www.google.com/intl/en/ipv6/statistics.html

32. Franklin, J., McCoy, D., Tabriz, P., Neagoe, V., Randwyk, J.V., Sicker, D.: Passive data link layer 802.11 wireless device driver fingerprinting. In: USENIX Security Symposium, vol. 3, pp. 16–89 (2006)

33. Stokes, A.: TCP/IP, chapter T, pp. 1745–1747. Wiley, GBR (2003)

34. Bidgoli, H.: The Internet Encyclopedia, vol. 2 (G-O). The Internet Encyclopedia. Wiley. ISBN 9780471689966. https://books.google.co.uk/books?id=gZ9srwU_9xMC (2004)

35. Brown, W.: Centralizing information technology in a distributed system (again?). In: Proceedings of the 30th Annual ACM SIGUCCS Conference on User Services, SIGUCCS '02, pp. 222–225, New York, NY, USA. Association for Computing Machinery. ISBN 1581-135645. https://doi.org/10.1145/588646.588700 (2002)

36. Lopez, P.G., Montresor, A., Datta, A.: Please, do not decentralize the internet with (permissionless) blockchains! In: 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), pp. 1901–1911. ISBN 1063-6927 (2019)

37. Yang, W., Aghasian, E., Garg, S., Herbert, D., Disiuta, L., Kang, B.: A survey on blockchain-based internet service architecture: requirements, challenges, trends, and future. IEEE Access **7**, 75845–75872 (2019)

38. Cho, S., Lee, S.: Survey on the application of blockchain to IoT. In: 2019 International Conference on Electronics, Information, and Communication (ICEIC), pp. 1–2 (2019)

39. Tiwari, T., Trachtenberg, A.: Alternative (ab)uses for http alternative services. In: 13th USENIX Workshop on Offensive Technologies (WOOT 19), pp. 1–12, Santa Clara, CA. USENIX Association. https://www.usenix.org/conference/woot19/presentation/tiwari (2019)

40. Ibáñez, L., Simperl, E., Gandon, F., Story, H.: Redecentralizing the web with distributed ledgers. IEEE Intell. Syst. **32**(1), 92–95 (2017)

41. Ali, A., Khan, M., Saddique, M., Pirzada, U., Zohaib, M., Ahmad, I., Debnath, N.: Tor vs i2p: a comparative study. In: 2016 IEEE International Conference on Industrial Technology (ICIT), pp. 1748–1751 (2016)

42. Ding, J., Guo, X., Chen, Z.: Big data analyses of zeronet sites for exploring the new generation darkweb. In: Proceedings of the 3rd International Conference on Software Engineering and Information Management, ICSIM '20, pp. 46–52, New York, NY, USA. Association for Computing Machinery. ISBN 9781450376907. 10.1145/3378936.3378981. URL https://doi.org/10.1145/3378936.3378981 (2020)

43. Hoang, N. P., Kintis, P., Antonakakis, M., Polychronakis, M.: An empirical study of the i2p anonymity network and its censorship resistance. In: Proceedings of the Internet Measurement Conference 2018, IMC '18, pp. 379–392, New York, NY, USA. Association for Computing Machinery. ISBN 9781450356190. https://doi.org/10.1145/3278532.3278565 (2018)

44. Pierro, M.D.: What is the blockchain? Comput. Sci. Eng. **19**(5), 92–95 (2017)

45. Sopek, M., Gradzki, P., Kosowski, W., Kuziski, D., Trojczak, R., Trypuz, R.: Graphchain: a distributed database with explicit semantics and chained RDF graphs. In: Companion Proceedings of the The Web Conference 2018, WWW'18, pp. 1171–1178, Republic and Canton of Geneva, CHE. International World Wide Web Conferences Steering Committee. ISBN 9781-450356404. https://doi.org/10.1145/3184558.3191554 (2018)

46. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557–564 (2017)

47. Halaburda, H.: Blockchain revolution without the blockchain? Commun. ACM **61**(7), 27–29 (2018). https://doi.org/10.1145/3225619

48. Elsden, C., Nissen, B., Jabbar, K., Talhouk, R., Lustig, C., Dunphy, P., Vines, J.. HCI for blockchain: studying, designing, critiquing and envisioning distributed ledger technologies. In: Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems, CHI EA '18, pp. 1–8, New York, NY, USA. Association for Computing Machinery. ISBN 9781-450356213. https://doi.org/10.1145/3170427.3170602 (2018)

49. Suciu, G., Nădrag, C., Istrate, C., Vulpe, A., Ditu, M., Subea, O.: Comparative analysis of distributed ledger technologies. In: 2018 Global Wireless Summit (GWS), pp. 370–373, (2018)

50. Chowdhury, M.J.M., Ferdous, M.S., Biswas, K., Chowdhury, N., Kayes, A.S.M., Alazab, M., Watters, P.: A comparative analysis of distributed ledger technology platforms. IEEE Access **7**, 167930–167943 (2019)

51. Burkhardt, D., Werling, M., Lasi, H.: Distributed ledger. In: 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), pp. 1–9 (2018)

52. Jannes, K., Lagaisse, B., Joosen, W.: You don't need a ledger: Lightweight decentralized consensus between mobile web clients. In: Proceedings of the 3rd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, SERIAL '19, pp. 3–8, New York, NY, USA. Association for Computing Machinery. ISBN 9781450370295. https://doi.org/10.1145/3366611.3368143 (2019)

53. Kim, H.S., Wang, K.: Immutability measure for different blockchain structures. In: 2018 IEEE 39th Sarnoff Symposium, pp. 1–6 (2018)

54. Labouseur, A.G., Johnson, M., Magnusson, T.: Demystifying blockchain by teaching it in computer science: adventures in essence, accidents, and data structures. J. Comput. Sci. Coll. **34**(6), 43–56 (2019)

55. Zhang, S., Lee, J.-H.: Analysis of the main consensus protocols of blockchain. ICT Express. http://www.sciencedirect.com/science/article/pii/S240595951930164X (2019)

56. Sayadi, S., Rejeb, S.B., Choukair, Z.: Blockchain challenges and security schemes: a survey. In: 2018 Seventh International Conference on Communications and Networking (ComNet), pp. 1–7 (2018). ISBN 2163-663X

57. Wüst , K., Gervais, A.: Do you need a blockchain? In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), pp. 45–54 (2018)

58. Boyen, X., Carr, C., Haines, T.: Graphchain: a blockchain-free scalable decentralised ledger. In: Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, BCC '18, pp. 21–33, New York, NY, USA. Association for Computing Machinery. ISBN 9781450357586. https://doi.org/10.1145/3205230.3205235 (2018)

59. Kan, J., Chen, S., Huang, X.: Networking. Improve blockchain performance using graph data structure and parallel mining. In: 2018 1st IEEE International Conference on Hot Information-Centric, pp. 173–178 (2018)

60. Wang, J., Wang, H.: Monoxide: Scale out blockchains with asynchronous consensus zones. In: 16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19), pp. 95–112, Boston, MA. USENIX Association. ISBN 9781-931971492. https://www.usenix.org/conference/nsdi19/presentation/wang-jiaping (2019)

61. da Silva, F.J.C., Damsgaard, S.B., Sorensen, M.A.M., Marty, F., Altariqi, B., Chatzigianni, E., Schwefel, H.P.: Analysis of blockchain forking on an Ethereum network (2019)

62. Mišić, V.B., Mišić, J., Chang, X.: On forks and fork characteristics in a bitcoin-like distribution network (2019)

63. Wang, S., Wang, C., Hu, Q.: Corking by forking: Vulnerability analysis of blockchain. In: IEEE INFOCOM 2019—IEEE Conference on Computer Communications, pp. 829–837. ISBN 2641-9874 (2019)

64. Liu, B., Qin, Y., Chu, X.: Reducing forks in the blockchain via probabilistic verification (2019)

65. Florian, M., Henningsen, S., Beaucamp, S., Scheuermann, B.: Erasing data from blockchain nodes. In: 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), pp. 367–376 (2019)

66. Kwon, Y., Liu, J., Kim, M., Song, D., Kim, Y.: Impossibility of full decentralization in permissionless blockchains. In: Proceedings of the 1st ACM Conference on Advances in Financial Technologies, AFT '19, pp. 110–123, New York, NY, USA. Association for Computing Machinery. ISBN 9781-450367325. https://doi.org/10.1145/3318041.3355463 (2019)

67. Pahlajani, S., Kshirsagar, A., Pachghare, V.: Survey on private blockchain consensus algorithms. In: 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), pp. 1–6 (2019)

68. Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., Qijun, C.: A review on consensus algorithm of blockchain. In: 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 2567–2572 (2017)

69. Chaudhry, N., Yousaf, M.M.: Consensus algorithms in blockchain: comparative analysis, challenges and opportunities. In: 2018 12th International Conference on Open Source and Technologies, pp. 54–63 (2018)

70. Salimitari, M., Chatterjee, M.: An overview of blockchain and consensus protocols for IoT networks. CoRR, abs/1809.05613 (2018). arXiv: 1809.05613

71. Salimitari, M., Chatterjee, M.: A survey on consensus protocols in blockchain for iot networks. arXiv e-prints, p. ar:1809.05613, (2018). https://ui.adsabs.harvard.edu/abs/2018arXiv180905613S. 1809.05613; Provided by the SAO/NASA Astrophysics Data System

72. Milutinovic, M., He, W., Wu, H., Kanwal, M.: Proof of luck: an efficient blockchain consensus protocol. arXiv e-prints, p. ar:1703.05435, (2017). https://ui.adsabs.harvard.edu/abs/2017arXiv170305435M. 1703.05435; Provided by the SAO/NASA Astrophysics Data System

73. Shibata, N.: Proof-of-search: combining blockchain consensus formation with solving optimization problems. IEEE Access 7, 172994–173006 (2019)

74. Puthal, D., Mohanty, S.P.: Proof of authentication: Iot-friendly blockchains. IEEE Potentials 38(1), 26–29 (2019)

75. Ehmke, C., Wessling, F., Friedrich, C.M.: Proof-of-property—a lightweight and scalable blockchain protocol. In: 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), pp. 48–51 (2018)

76. Andrey, A., Petr, C.: Review of existing consensus algorithms blockchain. In: 2019 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), pp. 124–127 (2019)

77. Bentov, I., Lee, C., Mizrahi, A., Rosenfeld, M.: Proof of activity: extending bitcoin's proof of work via proof of stake. SIGMETRICS Perform. Eval. Rev. 42(3), 34–37 (2014). https://doi.org/10.1145/2695533.2695545

78. Panda, S.S., Mohanta, B.K., Satapathy, U., Jena, D., Gountia, D., Patra, T.K.: Study of blockchain based decentralized consensus algorithms. In: TENCON 2019—2019 IEEE Region 10 Conference (TENCON), pp. 908–913 (2019)

79. Tasatanattakool, P., Techapanupreeda, C.: Blockchain: challenges and applications. In: 2018 International Conference on Information Networking (ICOIN), pp. 473–475 (2018)

80. Ali Syed, T., Alzahrani, A., Jan, S., Siddiqui, M.S., Nadeem, A., Alghamdi, T.: A comparative analysis of blockchain architecture and its applications: problems and recommendations (2019)

81. Liu, X., Zhao, G., Wang, X., Lin, Y., Zhou, Z., Tang, H., Chen, B.: MDP-based quantitative analysis framework for proof of authority. In: 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 227–236 (2019)

82. Charapko, A., Ailijiang, A., Demirbas, M.: Bridging paxos and blockchain consensus. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1545–1552 (2018)

83. Gomathi, R.M., Krishna, G.H.S., Brumancia, E., Dhas, Y.M.: A survey on IoT technologies, evolution and architecture. In: 2018 International Conference on Computer, Communication, and Signal Processing (ICCCSP), pp. 1–5 (2018)

84. Dixit, M., Kumar, J., Kumar, R.: Internet of things and its challenges. In: 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), pp. 810–814 (2015)

85. Reyna, A., Martin, C., Chen, J., Soler, E., Diaz, M.: On blockchain and its integration with IoT. Challenges and opportunities. Future Gener. Comput. Syst. 88, 173 (2018)

86. Conoscenti, M., Vetrò, A., Martin, J.C.D.: Blockchain for the internet of things: a systematic literature review. In: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1–6. ISBN 2161-5330 (2016)

87. Qiu, C., Yao, H., Jiang, C., Guo, S., Xu, F.: Cloud computing assisted blockchain-enabled internet of things (2019)

88. Sanghi, N., Bhatnagar, R., Kaur, G., Jain, V.: Blockcloud: blockchain with cloud computing (2018)

89. Mouradian, C., Naboulsi, D., Yangui, S., Glitho, R.H., Morrow, M. J., Polakos, P.A.: A comprehensive survey on fog computing: state-of-the-art and research challenges (2018)

90. Harshavardhan, A., Vijayakumar, T., Mugunthan, S.R.: Blockchain technology in cloud computing to overcome security vulnerabilities (2018)

91. Tosh, D.K., Shetty, S., Liang, X., Kamhoua, C.A., Kwiat, K.A., Njilla, L.: Security implications of blockchain cloud with analysis of block withholding attack (2017)

92. Yang, R., Yu, F.R., Si, P., Yang, Z., Zhang, Y.: Integrated blockchain and edge computing systems: a survey, some research issues and challenges. IEEE Commun. Surv. Tutor. 21(2), 1508–1532 (2019)

93. Moreno-Vozmediano, R., Montero, R.S., Llorente, I.M.: Key challenges in cloud computing: enabling the future internet of services (2013)

94. Botta, A., de Donato, W., Persico, V., Pescapé, A.:. On the integration of cloud computing and internet of things (2014)

95. Pan, J., McElhannon, J.: Future edge cloud and edge computing for internet of things applications. IEEE Internet Things J. 5(1), 439–449 (2018)

96. Mendki, P.: Blockchain enabled IoT edge computing. In: Proceedings of the 2019 International Conference on Blockchain

Technology, ICBCT 2019, pp. 66–69, New York, NY, USA. Association for Computing Machinery. ISBN 9781-450362689. https://doi.org/10.1145/3320154.3320166 (2019)

97. Bonomi, F., Milito, R., Zhu, J., Addepalli, S.: Fog computing and its role in the internet of things. In: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, pp. 13–16. ACM (2012)

98. Khan, A.Z., Qazi, I.A.: Mutual authentication scheme of IoT devices in fog computing environment. Clust. Comput. (2020). https://doi.org/10.1007/s10586-020-03211-1

99. Bakhshi, Z., Rodriguez-Navas, G., Hansson, H.: Dependable fog computing: a systematic literature review (2019)

100. Wu, D., Ansari, N.: A cooperative computing strategy for blockchain-secured fog computing (2020)

101. Seitz, A., Henze, D., Miehle, D., Bruegge, B., Nickles,J., Sauer, M.:. Fog computing as enabler for blockchain-based IoT app marketplaces—a case study. In: 2018 Fifth International Conference on Internet of Things: Systems, Management and Security, pp. 182–188 (2018)

102. Qu, Y., Gao, L., Luan, T.H., Xiang, Y., Yu, S., Li, B., Zheng, G.: Decentralized privacy using blockchain-enabled federated learning in fog computing (2020)

103. Ziegler, M. H., Großmann, M., Krieger, U.R.:. Integration of fog computing and blockchain technology using the plasma framework. In: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 120–123 (2019)

104. Kreutz, D., Ramos, F.M.V., Veríssimo, P.E., Rothenberg, C.E., Azodolmolky, S., Uhlig, S.: Software-defined networking: a comprehensive survey. Proc. IEEE 103(1), 14–76 (2015)

105. Khan, A.Z., Qazi, I.A.: Recflow: SDN-based receiver-driven flow scheduling in datacenters. Clust. Comput. 23, 289–306 (2020). https://doi.org/10.1007/s10586-019-02922-4

106. Sharma, P.K., Chen, M., Park, J.H.: A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access 6, 115–124 (2018)

107. Jiang, X., Bi, J., Nan, G., Li, Z.: A survey on information-centric networking: rationales, designs and debates. China Commun. 12(7), 1–12 (2015)

108. Awais,M., Shah, M.A.: Information-centric networking: a review on futuristic networks. In: 2017 23rd International Conference on Automation and Computing (ICAC), pp. 1–5 (2017)

109. Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., Ohlman, B.: A survey of information-centric networking. IEEE Commun. Mag. 50(7), 26–36 (2012)

110. Waltari, O., Kangasharju, J.: Content-centric networking in the internet of things. In: 2016 13th IEEE Annual Consumer Communications Networking Conference (CCNC), pp. 73–78 (2016)

111. Afanasyev, A., Burke, J., Refaei, T., Wang, L., Zhang, B., Zhang, L.: A brief introduction to named data networking. In: MILCOM 2018—2018 IEEE Military Communications Conference (MILCOM), pp. 1–6 (2018)

112. Aboodi, A., Wan, T., Sodhy, G.: Survey on the incorporation of NDN/CCN in IoT. IEEE Access 7, 71827–71858 (2019)

113. Amadeo, M., Campolo, C., Iera, A., Molinaro, A.: Named data networking for IoT: an architectural perspective. In: 2014 European Conference on Networks and Communications (EuCNC), pp. 1–5 (2014)

114. Wu, J., Dong, M., Ota, K., Li, J., Yang, W., Wang, M.: Fog-computing-enabled cognitive network function virtualization for an information-centric future internet. IEEE Commun. Mag. 57(7), 48–54 (2019)

115. Kuszmaul, J.: Verkle trees. In: Verkle Trees, pp. 1–12 (2019). https://math.mit.edu/research/highschool/primes/materials/2018/Kuszmaul.pdf

116. Gyongyosi, L., Imre, S.: Decentralized base-graph routing for the quantum internet. Phys. Rev. A 98(2), 022310 (2018). https://doi.org/10.1103/PhysRevA.98.022310

117. Tripathi, G., Sharma, B., Rajvanshi, S.: A combination of internet of things (IoT) and graph database for future battlefield systems. In: 2017 International Conference on Computing, Communication and Automation (ICCCA), pp. 1252–1257 (2017)

118. Doku, R., Rawat, D.B., Garuba, M., Njilla, L.: Fusion of named data networking and blockchain for resilient internet-of-battle-field-things. In: 2020 IEEE 17th Annual Consumer Communications Networking Conference (CCNC), pp. 1–6 (2020)

119. Jia, K., Soo., K.K.: Mtfs: Merkle-tree-based file system. arXiv e-prints, p. ar:1902.09100, (2019). https://ui.adsabs.harvard.edu/abs/2019arXiv190209100K. 1902.09100; Provided by the SAO/NASA Astrophysics Data System

120. Nakamoto, S., Bitcoin, A.: A peer-to-peer electronic cash system. Bitcoin. https://bitcoin.org/bitcoin.pdf (2008)

121. Vujičić, D., Jagodić, D., Randić, S.: Blockchain technology, bitcoin, and ethereum: a brief overview. In: 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH), pp. 1–6 (2018)

122. Niranjanamurthy, M., Nithya, B.N., Jagannatha, S.: Analysis of blockchain technology: PROS, CONS and SWOT. Clust. Comput. 22(6), 14743–14757 (2019)

123. Cinque, M., Esposito, C., Russo, S., Tamburis, O.: Blockchain-empowered decentralised trust management for the internet of vehicles security. Comput. Electr. Eng. 86, 106722 (2020)

124. Alfandi, O., Khanji, S., Ahmad, L., Khattak, A.: A survey on boosting IoT security and privacy through blockchain. Clust. Comput. 1–19 (2020)

125. Liang, W., Ji, N.: Privacy challenges of IoT-based blockchain: a systematic review. Clust. Comput. 1–19 (2021)

126. Khan, M.A., Quasim, M.T., Algarni, F., Alharthi, A.: Decentralised Internet of Things: a blockchain perspective, vol. 71. Springer (2020)

127. Ali, A., Rahouti, M., Latif, S., Kanhere, S., Singh, J., Janjua, U., Crowcroft, J.. Blockchain and the future of the internet: a comprehensive review. CoRR, abs/1904.00733, (2019). http://arxiv.org/abs/1904.00733

128. Chowdhury, S.H.M., Jahan, F., Sara, S.M., Nandi, D.: Secured blockchain based decentralised internet: a proposed new internet. In: Proceedings of the International Conference on Computing Advancements, pp. 1–7 (2020)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Javad Zarrin received his Ph.D. in ComputerScience from Universidade de Aveiro, Portugal in2016. He also received his M.Sc. in TelecommunicationNetworks Engineering from UniversityPutra Malaysia and a B.Sc. in Physics from UrmiaUniversity. Currently, Javad is a lecturer at theSchool of Computing and Information Science,in Anglia Ruskin University (ARU-Cambridge).Before joining ARU, he was a postdoctoral researchassociate at the Department of ComputerScience and Technology at the

University of Cambridge, where he waspart of Systems Research Group (SRG). Since 2010, Javad worked as aresearcher at City University of London, University of Aveiro, and Institutode Teleco-municações (IT-Aveiro). His research interests are in the broadarea of distributed systems and his recent interests include Decentral-izedSystems, Machine Learning, Data Analytics, Optimization, Blockchain,Stream Processing, Scheduling, Simulation, HPC, Cloud, IoT, Fog andLarge-Scale Computing. He is an IEEE member and served as PC, TPC,keynote speaker, and reviewer for various events and venues such as ACMEurosys, IEEE Transactions on Cloud Computing, IEEE Transactions onVehicular Technology, Springer High-Performance Computing, and MDPIjournals. He has also spent several years in industry working as a seniorsoftware engineer and project leader.

Hao Wen Phang received his BIT InformationTechnology (Hons) from HELP Univer-sity,Malaysia in 2018, and M.Sc. Computer Sciencein Anglia Ruskin University (ARU-Cambridge) in2020. He was once a part of Malaysian MENSASociety, MENSA International back in 2011. Hisresearch interests lies in Blockchain, IoT, InternetArchi-tecture and Web Development.
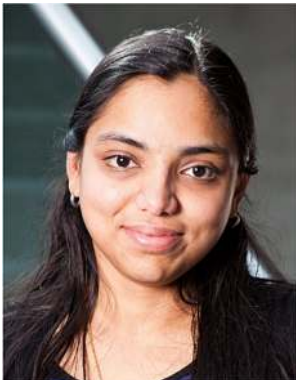
Lakshmi Babu Saheer received her Ph.D.degree from Ecole Polytechnique Federale de Lau-sanne(EPFL), Switzerland in 2012 after completingher Mas-ters by Research (M.S.) degreein Computer Science from the Indian Institute ofTechnology Madras (IITM), India in 2006. Shehas consider-able industrial experience workingwith international com-panies like Siemens Informa-tionSystems Ltd. (India), VEnable Technologies(U.S.A.) and Sony Ericsson Mobile Communications(Sweden), AudioAnalytic

(UK) and her own start-up initiative(Geneemo, Switzerland). She also has good academic experience workingas a research associate at IITM, research student, post-doc and scientificcollaborator at Idiap research institute, Switzerland. Currently, she is a seniorlecturer at the Anglia Ruskin University in Cambridge, UK. Her researchinterests include Artificial Intelligence, Machine Learning, Speech/AudioPro-cessing, Climate Change, Sustainability, IoT and Healthcare. She is amember of IEEE and an official reviewer for different IEEE journals likeIEEE Access, Journal of Selected Topics in Signal Processing, Transactionson Audio, Speech and Language Processing and Eurasip Journal.

Bahram Zarrin received his Ph.D. in ComputerScience from Technical University of Den-mark(DTU) in 2016. He also received his M.Sc.and B.Sc. in Software Engineering from UniversityPutraMalaysia and Bu-Ali Sina University in Iran.Currently, Bahram is a postdoctoral researcher atthe Department of Computer Sci-ence (DTU Compute)at DTU, where he is a member of Sec-tionfor Embedded Systems Engineering. He is thedirector of an European Training Network (ETN)project called FORA, which trains 15 PhD candidates in the area of FogComputing, during the period 2017–2021. His research interests are in thebroad area of software engineering and distributed embedded systems. Hisrecent interests include Fog Computing, Edge Computing, Industrial IoT,-modeling & simulation, optimization, programming languages, and formalmethods. He has served as PC, TPC, panelist, and reviewer for variousevents and venues such as Fog-IoT workshops, SummerSim/ SpringSimAnnual conferences sponsored by the Society for Modeling and SimulationInternational (SCS), the International Journal of Embedded and Real-TimeCommunication Systems (IJERTCS), the International Journal of Informationand Software Technology (INFSOF), the International Journal of Time-Critical Computing Systems (Real-Time Systems), ACM Transactions onModeling and Performance Evaluation of Computing Systems (ToMPECS).He also has more than ten years of experience in software industries.