Futuristic Trends in Blockchain Applications

Mr. K.A. Mohamed Riyazudeen
Assistant Professor,
Department of Computer Science, Sadakathullah Appa College, Tirunelveli.

Dr. M. Sheik Muhideen Badhusha
Dean, Research and Development & Assistant Professor,
Department of Chemistry, Sadakathullah Appa College, Tirunelveli.

ABSTRACT

In today's cutthroat market, cutting-edge innovations in technology appear daily. Blockchain software was developed as a result of recent technological progress. It's useful in numerous settings, including cryptocurrency exchanges, banks, financial services, the IoT, risk management, and more. Although several studies have been undertaken on the topic at hand, none have focused on how this technology may be put to practical use or provided a comprehensive overview of where the field is headed. In this post, we'll look at how blockchain technology may be used in many contexts and how it can open up new possibilities in the future.
Blockchain, as its name suggests, is composed of two parts: a "block" and a "chain." Here, "block" refers to the discrete units of individual bitcoin transactions carried out across multiple computers worldwide. Chain, on the other hand, is the interconnected system of computers in a network that verifies and records each transaction. From this, we learn that blockchain is a distributed ledger that keeps track of all the individual purchases and sales made with a cryptocurrency like Bitcoin across a network of computers. Like artificial intelligence, blockchain technology is a very new field (AI). Like artificial intelligence (AI), blockchain is having a significant influence on the world as it is now and is causing many industries to reevaluate their practices. This chapter does not cover every possible scenario or industry where blockchain is having an effect. Instead, blockchain's revolutionary effects on the IT industry are the primary emphasis. This article thus addresses the subsequent IT reevaluation brought forth by blockchain technology.

INTRODUCTION

Using a logbook method with distinct important aspects including order, growth, security, and digitalization, blockchain technology records information and data digitally. In addition to these qualities, the blockchain also has others that are not intrinsic to the technology but are instead the result of the implementation of other technologies, such as sharing and distribution mechanisms or communication and agreement protocols. Blockchain technology is a distributed ledger consisting of many data chains that are cryptographically connected. Using cryptographic hashes, these blockchains are connected consecutively. Hash is a unique number that is calculated from an existing message or document and has a predetermined length. Each block consisted of three main parts: (1) Block-Data, which is a collection of messages or transactions; (2) Chaining-Hash, which is a duplicate of the hash value of the previous block; and (3) Block-Hash, which is the hash value of the data block or messages plus the chaining hash value (Norton, 2016; Gupta, 2017; Nakamoto, 2008). In 2008, the idea of blockchain technology was suggested, and by 2009, it was being used. Essentially, it is a public ledger whereby a series of blocks are committed to protecting the integrity of the transactions recorded in them. These chained bricks keep becoming bigger as more and more are added to them. Decentralization, persistence, privacy, and audibility are just a few of the features that blockchain technology offers. Integrating several foundational technologies, such as a cryptographic hash, digital signature, and dispersed consensus process, blockchain technology may also function in a decentralized setting. In a decentralized system, blockchain technology enables transactions. If the blockchain system is implemented, productivity gains are possible. It will also aid in cost savings (Norton, 2016).

Cryptocurrency has recently garnered the interest of both academics and businesspeople. It was the very first cryptocurrency, Bitcoin, that helped the global capital market reach $10 billion in value in 2016. While Bitcoin is where most people will be familiar with blockchain technology, there are many more potential uses for the platform. Since it allows for bank payments to be made without the need for a middleman, blockchain technology has several potential applications in the financial sector, including the management of digital assets, settlement, and electronic payments (Foroglou, 2015; Peters, 2015). Furthermore, blockchain technology is receiving attention as a future-leading technology in the field of internet communication systems like advance agreements (Kosba, 2016), community services (Akins, 2013), the Internet of Things (IoT) (Zhang, 2015), status systems (Sharples, 2015), and safety facilities (Kosba, 2016; Akins, 2013; Zhang, 2015). (Noyes, 2016). Although blockchain technology is quickly becoming one of the most promising candidates for the infrastructure of the future internet, it is also facing several technical challenges (Foroglou and Tsilidou, 2016).

Scalability is the primary area of concern. At the moment, 1 MB is the maximum size of a bitcoin, and new 1 MB squares are mined at regular intervals. As a result, the Bitcoin network cannot support high-frequency trading due to its low transaction throughput of just 7 per second. Yet, it is believed that the blocks occupy more space and cause the network to spread more slowly. The gradual move toward consolidation is because every blockchain user is keen on preserving the distributed ledger. Hence, it's becoming difficult to keep the balance between the block size and the level of security. In addition, it is plain to see that the miners make a lot more money than their fair share by using the self-centered excavation strategy (Eyal, 2014). These blocks are also kept secret by miners so that they may be mined at a later date for a profit (Carboni, 2014).

In a similar vein, disagreements among participants might slow the development of the blockchain. So, some kind of remedy to the situation must be proposed. However, it has been shown that privacy may be compromised even when using public and private keys for transactions (Biryukov, 2014). The user's true IP address may also be identified. Nevertheless, existing consensus algorithms have some significant challenges, such as verifying the work done or confirming the status. In the proof-of-work scenario, for instance, an excessive amount of energy is squandered, whereas, in the proof-of-stake consensus process, the affluent tend to grow wealthier. As a result, if blockchain technology advances, it is essential to tackle these issues without delay.

There is a wealth of material accessible on the topic of blockchain, including academic journal papers, conference proceedings, online discussion threads, code repositories, wikis, and dictionaries. As part of his technical examination of decentralized currencies, Tschorsch (2016) has included Bitcoin (Jaag et al., 2016). This chapter, in contrast to Tschorsch et al., will not deal with digital money per se but rather blockchain technology. The technical paper on blockchain was prepared by Nomura Research Institute (NRI, 2015). Our research, in contrast, has focused on the current state of blockchain studies, which incorporates both the most recent advances and anticipated directions in the field. To put it another way, blockchain technology contributes to the development of a trustworthy, secure, and transparent distributed ledger system. This technology, which may be better understood as the technology that is truly institutional and social, represents a revolution in its own right, being both novel and unconventional in its application to the upkeep of public databases. The public choice/institutional approach to the economics of blockchains suggests that this emerging technology may have far-reaching consequences for the economy. The argument is presented (Luther & White, 2016).

ARCHITECTURE OF BLOCKCHAIN

Similar to a traditional public ledger, a blockchain comprises blocks of data that are linked together sequentially to form a complete record of transactions. The blockchain scenario shown in Figure 14.1 above is illustrative. A block's parent is the block to which it was previously linked by reference via a hash value. Uncle block hashes, the offspring of the ancestral blocks, will be able to be stored on the Ethereum blockchain.

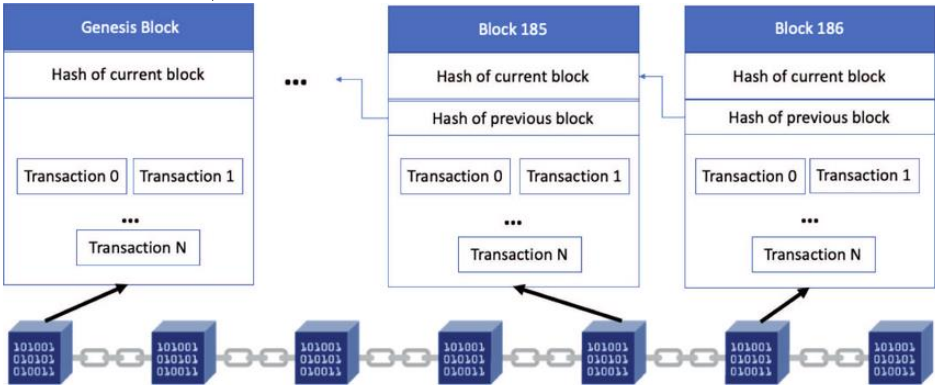

FIGURE 14.1 Blockchain design based on the sequential arrangement of blocks.

The first, or genesis, block in a blockchain's chronological order is the "parentless" block. Moreover, we have shown the blockchain's architecture and the digital signature process in another part of this chapter. In addition, we have covered the crucial features, and in later parts, we will go over a specific taxonomy of blockchain (Atzori, 2015).

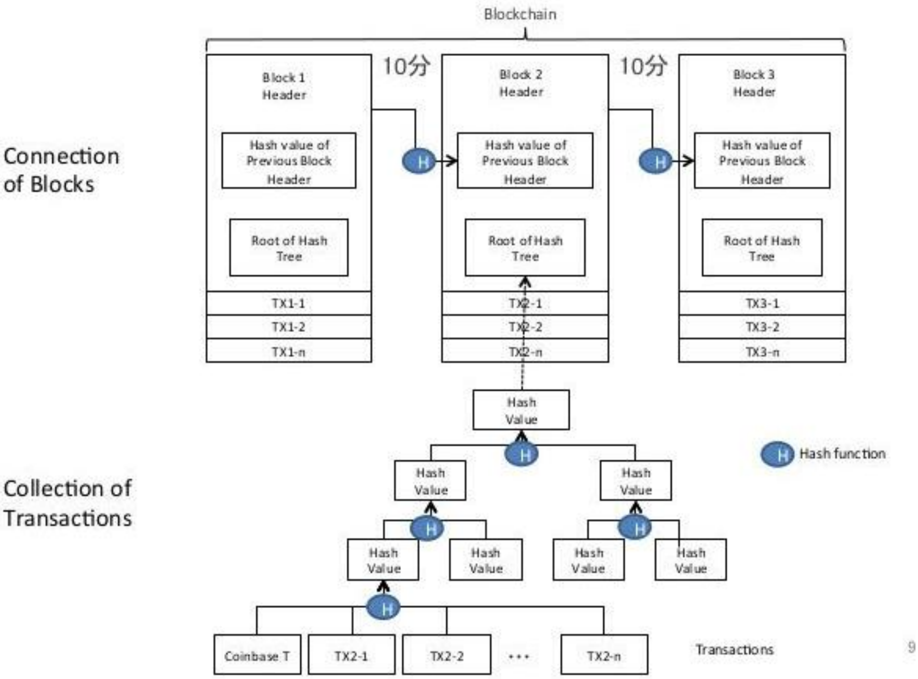

FIGURE 14.2 Structures of Blocks.

BLOCK

Figure 14.2 depicts the components of a blockchain block, which are the block header and the block content.

About the block's header, its primary parts are as follows:

(i) For the I Block version, this shows the sequence of blocks that the validation criteria apply to.
(ii) Parent block hash: This block's value is a 256-bit hash that references the one before it.
(iii) For calculating the Merkle tree root hash, the total hash value of the transactions in the block is taken into account.

(iv) The current time, in seconds since 1970-01-01T00:00 UTC (iv).
(v) The current hashing goal, expressed in nBits.
(vi) A 4-byte field that typically begins at 0 and increments with each hash computation; sometimes known as a "nonce.".

The block's meat is the transaction counter and the transactions themselves. The amount of transactions a given block may continue is based on two factors: the block size and the transaction size. By using an asymmetric cryptographic technique, blockchain technology ensures the authenticity of all transactions. Digital signatures based on uneven cryptography are useful in an environment where confidence is hard to come by. Let's look at a simple digital sign example now (Biryukov et al., 2014).

SIGNING IN DIGITAL FORM:

Each participant in a blockchain network has their own unique set of keys, both public and private. The private keys are used to sign the transactions. This signature is generated with the help of the private key. These digital signatures are dispersed over the network and accessible via public keys. Figure 14.3 is an example of a digital signature being used in a blockchain application. This kind of electronic authentication may be broken down into two subcategories: the signature phase and the authenticating phase. Referring back to Figure 14.3 is a useful exercise. In this case, Alice has already created the hash value used to sign the transaction before she signs it. Then, the original data, together with its encrypted hash, was delivered to a different operator named Bob using the secret keys. Once Bob receives a transaction, he decrypts the associated funds and uses the resulting hash value to confirm the authenticity of the information he has received. Elliptic Curve Digital Signature Algorithm (ECDSA) uses the tried-and-true method of digitally signing documents using a computer (Atzori et al., 2010).

FIGURE 14.3 Implementation of Digital Signatures on the Blockchain.

KEY COMPONENTS OF BLOCKCHAIN

The following categories may be used to group the properties of the blockchain:

1. Decentralization: In the typical centralized transaction system, each transaction is validated by the central trusted agency (such as the central bank), which undoubtedly causes budget and act bottlenecks at the main servers.

TABLE 14.1 Comparisons between Public Blockchain, Consortium Blockchain, and PrivateBlockchain

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	One organization
Read permission	Public	Could be public or restricted	Could be public or restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

This is in contrast to the blockchain network, where any two peers may conduct any transaction without the need for approval from the central authority. Using this strategy, the cost of the server may be decreased (including the cost of process improvements) and performance bottlenecks at the primary server can be moderated (Foro- glow and Tsilidou, 2015).

- Persistence: Since the blockchain is distributed across the network and every transaction must be verified and recorded in the blocks distributed throughout the system, it becomes extremely difficult to tamper with the data. Also, each transaction will be examined, and other nodes will be confirming the block that was widely broadcast. As a result, it is simple to spot the deception.
- Anonymity: Using blockchain technology, users may communicate by creating addresses. In addition, users may create several addresses to avoid revealing their identities.

- The user's private information is not being maintained by the principal individual in this. As a result, this method enables the blockchain to retain transaction anonymity to some degree. It should be mentioned that owing to inherent constraints and other limitations, blockchain technology cannot perfectly guarantee anonymity.
- Auditability: Since each transaction in blockchain technology is timestamped and documented, it is simple for users to verify and follow previous events by accessing any transaction in the system that has been circulated (Noyes, 2016).
- You can find every transaction that was ever made using the Bitcoin blockchain technology. As a result, the accessibility and openness of any transactions recorded in the blockchain are improved.

TAXONOMY OF BLOCKCHAIN SYSTEMS

- Private blockchains, public blockchains, and consortium blockchains are the three main types of blockchain systems. Table 14.1 compares and contrasts the several blockchain architectures now in use.
- As every block in a blockchain can be seen by the public, it may be utilized in the process of reaching a consensus. In contrast, in the consortium blockchain, just a subset of the blocks is responsible for the validation of the block. If a private chain is led by a single organization in the final consensus, that organization will be that organization (Peters and Panayi, 2015).
- Permission to read: Unrestricted blockchain transactions are public and transparent, whereas private blockchains or consortiums of blockchains determine who may view which blocks. The consortium or organization may decide whether or not the stored data will be accessible to the public.
- Immutability: As the ledger's transactions are spread out over several blocks, tampering with the public ledger is a tedious and time-consuming process. The private blockchain may be edited or rewritten if the change is made at the group or central level.

  Efficiency: The public blockchain network has many nodes, which means that broadcasting a transaction takes a long time.
- Further restrictions will be placed on the public blockchain to ensure the safety of the network. Hence, transaction throughput will be low and latency will be significant. Reducing the number of

validators in a consortium or private blockchain may improve its efficiency.

- In terms of centralization, the primary distinction between the three types of blockchains is that the first, the open blockchain, is decentralized, while the second, the consortium blockchain, is partially integrated, and the third, the private blockchain, is fully brought together because it is constrained by a single gathering. Reference: (Wanget al., 2015).
- Consensus procedure: Everyone in the world with access to the public blockchain may participate in the Consensus process. Both types of blockchain are allowed, although the latter is restricted. Authenticating nodes that participate in a consortium or public blockchain's consensus process is crucial. With the blockchain's unrestricted version out in the open, it has the potential to attract a large user base. Over time, unfettered blockchain has evolved as a viable technology, according to studies. Blockchain has the potential to be useful in many different parts of the business, especially if it is used in a collaborative setting. The business consortium's frameworks are currently being developed by Hyperledger. Ethereum has furthermore supplied a variety of instruments for the establishment of consortium blockchains. Several businesses are using blockchain technology, particularly private blockchains, to improve audibility and operational efficiency. As reported by (Zhang and Wen, 2015).

NEW DEVELOPMENTS AND FUTURE OBSTACLES IN BLOCKCHAIN

Being a relatively new technology, blockchain is still vulnerable to a wide range of potential risks and challenges. For your convenience, we have summed up the three most common dangers:

1. Scalability
2. Disclosure of Confidential Information
3. Selfish mining

The blockchain is becoming heavier as the number of transactions increases daily. Too far, bitcoin's blockchain has amassed more than 100 GB of data.

- All of these interactions are documented to verify their legitimacy. Furthermore, Bitcoin transactions will only be able to process seven transactions before a new block is generated, which is insufficient to meet the need of processing millions of transactions in real-time. This restriction was present in the original block size and time gap for the generation of a new block. However, the block's limited capacity might cause a backlog of transactions since miners prioritize those with the highest transaction fees (Sharples and Domingue, 2015). Yet, the vast size of the blockchain and the traffic directed to blockchain nodes will impede propagation speed. Thus, scalability is a demanding and complex problem to solve. There are several suggested methods for overcoming the scalability issue, and they may be roughly classified into two categories:
- To solve the problem of blockchain congestion, a novel bitcoin storage system was presented, which included optimizing the blockchain's storage capacity. With the new system, networks often purge old transactions and use a tree-like database to track the cumulative funds of all active account holders. Similarly, nodes don't need to keep copies of all transactions to ensure their legitimacy. A client's lack of heft might help them solve the issues as well. As an alternative, a revolutionary approach known as VerSum has shown the existence of lightweight clients. VerSum has made it possible to outsource the intensive calculation of big inputs by using lightweight clients. Several servers are used to compare the data and compute the final figures.
- One potential evolution of blockchain technology, Bitcoin-NG, has been suggested, which would need a redesign of the blockchain itself. Bitcoin-central NG's tenet is that there should be two distinct kinds of conservational blocks, one for voting on leaders (the "kep block") and another for recording transactions (the "macroblock"). The miners are all vying for the position of foreman. It has been calculated that only when macroblock creation occurs would the new leader emerge (Namecoin, 2014).

FUTURE TRENDS

Several industries, especially those that have relied on third parties to vouch for one another in the past, stand to benefit from blockchain technology.

trust. According to Atzori (2015), the blockchain has the potential to restructure not just the government but the whole society. Several societal functions may become obsolete if people start using decentralized platforms for social organization and security. Moreover, he concludes that citizens' power over government services via authorized blockchains is welcomed and desired since it has the potential to significantly enhance the efficiency of public administration. Permissioned blockchains make the decentralization of publicly funded organizations a real possibility and appealing prospect since they have the potential to greatly increase the utility of open institutions. The most pressing need for developing countries is social reconstruction. The people's money is safer in the hands of those who use the blockchain. Especially in the developing world, landlords have the challenge of establishing ownership when the government encourages citizens to own property. Putting land titles on the blockchain might reduce or eliminate these problems. According to Glaser (2017), the porous borders between the virtual and physical worlds might undermine trust in the decentralized ledger system (blockchain). The Federal Bureau of Investigation said in 2012 that there was a debate between controllers and investigators as to whether or not blockchain-based cryptocurrencies might serve the same functions as fiat cash. According to Mishkin (2004), money is anything that is generally accepted as payment for products and services or as part of the settlement of debts owed to creditors. The "something generally recognized as an installment payment for items or services or in the discharge of debts." Luther and White (2014) claim that virtual currencies are seldom utilized as a means of exchange in the present day. In his 2014 article, Glaser offers realistic predictions that Bitcoin will continue to serve primarily as a fictitious asset. As a result of the innovative techniques created by business owners, the widespread use of cryptocurrencies as a substitute for the traditional currency may facilitate simpler transactions and wider acceptance of the new currency. When it comes to how individuals make purchases, the blockchain might be a game-changer. Huge transaction fees are incurred by landowners throughout the acquisition process. According to Goldman Sachs (2016), if blockchain were implemented to reduce errors and manual labor, insurance premiums would drop by $2 billion to $4 billion in the United States alone. By eliminating inaccuracies and saving time, "Blockchain might cut title insurance rates and produce $2-4 billion in cost savings in the US." Computer scientists, on the one hand, tend to concentrate on the purely technical and cryptographic challenges of this area, while researchers with a background in business and information systems engineering are allowed to place special emphasis on purely business and organizational issues.

marketplace architecture, trust and privacy concerns, and the decision to employ cutting-edge technologies. In addition, this revolutionary development may alter existing business models and inspire new, ground-breaking ones, potentially having a far-reaching impact across all relevant sectors. Hence, research at the intersection of markets, technologies, and business models is crucial.

Major developments in blockchain technology during the last four years:

The blockchain industry is seeing several different developments at once. Here, we break out the several subtypes of blockchain developments that have recently emerged. The writers have organized the trends into several parts, with the first focusing on financial developments and the next on those associated with the Internet of Things. Other topics covered include security and privacy, followed by public and social services, and then the reputation system.

Let's start delving into the many parts.

Funding

1. Firstly, the development of blockchain systems like Bitcoin has a significant impact on conventional business and financial services (Nakamoto, 2008). Peters (2015) said that blockchain technology has the potential to disrupt the financial sector. Many applications exist for blockchain technology, including the elucidation and settlement of financial assets. Moreover, Morini (2016) mentioned some of the real business situations where the use of blockchain may reduce the costs and dangers, such as the collateralization of financial derivatives. There has been a lot of interest in blockchain technology recently, therefore several software businesses including Microsoft Azure (2016) and IBM (2016) are intending to deliver blockchain as a service.
2. Second, Blockchain makes it simpler for traditional businesses to modernize their operations and keep up with the times in terms of both business and financial services. Let's use postal operators (POs) as an example; their traditional function is to act as a go-between for consumers and businesses, but blockchain and cryptocurrencies are helping them expand into new areas of service, both financially and otherwise. Postcoin, a colored Bitcoin found by Jaag and Bach in 2016, may be issued independently by each postal operator, representing a promising opportunity for postal operators to progress via blockchain technology. Postal service providers' extensive retail infrastructure,

3. Users have easy access to Postcoin since postal operators are widely regarded as the public's most reliable authority. Moreover, Jaag and Bach (2016) examine how blockchain technology offers various commercial options to postal operators, including service identification, device management, and supply chain administration.
4. Third, the peer-to-peer (P2P) financial sector is made more secure and reliable by blockchain technology. Noyes discovers several approaches for integrating P2P tools with multiparty calculation protocols to create a new market for peer-to-peer financial multiparty computation (Noyes, 2016). The MPC demonstration based on blockchain technology enables the transfer of computing tasks to an untraceable network of peer processors.
5. Fourth, the structure of risk management plays a crucial role in financial technology (also known as FinTech), and when combined with blockchain technology, its performance may be improved. In a novel approach to risk management, Pilkington (2016) makes use of blockchain technology to assess the dangers associated with a financial venture in Luxembourg. In today's market, investors who acquire shares through such connections have a significant danger of losing money on all of their holdings. Blockchain technology allows for more expedited decision-making when it comes to investments and securities. Michele (2016) demonstrates how using a new system in tandem with blockchain technology may reduce custodial risk while keeping transactions at the same degree of security. Also, blockchain enables autonomous organizations to take part in business-related cooperation. To protect the business-semantics prompted consistency criteria, Norta (2015) proposes a highly reliable DAO-GaaS conflict architecture.

Internet of Things

The Internet of Things (IoT) is one of the most talked-about innovations, and for good reason: it's poised to become the next big thing in terms of both data collection and transmission (ICT). The Internet of Things (IoT) aims to connect everyday items (sometimes called "smart devices") to the internet to provide customers with a variety of new services (Atzori, 2010; Miorandi, 2012). Managing logistics using Radio Frequency Identification (RFID) technology (ISO/IEC, 2013), smart homes (Dixon, 2012), e-health (Habib, 2015), smart grids (Fan, 2013), the marine industry (Wang, 2015), and so on are only some of the fundamental but essential uses of the Internet of Things. In theory, blockchain technology has the potential to significantly advance the Internet of Things.

1. One example is the blockchain technology that Zhang (2015) proposed using the knowledge of business deals using smart property and savvy agreement to create a new kind of online business model. In this framework, Distributed Autonomous Companies operate as autonomous transaction entities (DAC). Users use DAC to buy currencies and trade sensor data directly, without the need for a middleman (Dixon et al., 2015).
2. Second, the IoT sector places a premium on safeguarding data privacy and security. The blockchain may be used to enhance the privacy of IoT applications. In particular, Hardjono (2016) proposed a privacy-security approach to cloud-based IoT device assignment. In particular, Hardjono (2016) proposed a novel structure to enable the gadget to prove its generating source without the verification of the middleman, and thus, it is authorized to list inadvertently. In addition, IBM (2015) revealed proof of concept for their Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT) system, which is based on blockchain technology and is used to build a distributed network of devices. Machines in the home will be able to detect operational problems and recover software upgrades using this paradigm.

Services for the Community and Its Members

Blockchain technology has found widespread use in community and public service (Carboni, 2016).

1. The most fundamental use of blockchain technology in government is in land registration (NRI, 2015). For example, the land's current state and the rights associated with it might be recorded and disseminated using blockchain technology. In addition, the efficiency of public services will rise if any changes are made to the land status, such as the transfer of land or the creation of any sort of mortgage, and these changes may be registered and recorded on the blockchains.
2. Second, blockchain technology may also be used for green energy. Increased use of sustainable energy sources was one goal of Gogerty's proposed solar coin in 2011.
3. Thirdly, solar energy manufacturers are content with solar coins, which are a kind of digital cash. These solar coins, in contrast to those obtained via mining, may be organized by the solar coin foundation for as long as you generate solar energy.
4. Blockchain was originally developed to facilitate monetary transactions in a trustless environment. Yet, if we continue to use the information and training process as money, the blockchain approach may also be valuable to the digital age of the Education business. According to Devine (2015), one should educate themselves about blockchain technology. It is reasonable to suppose

that the academics are responsible for packing and positioning the blocks into the blockchain and that the coins represent academic success in the study of blockchain technology (Hardjono and Smith, 2016).

5. Fifth, the blockchain can safeguard the infrastructure of the internet, including things like domain name systems and user profiles. Namecoin, released in 2014, is an example of a new open-source technology designed to improve the security, decentralization, censorship conflict, confidentiality, and speed of the Domain Name System (DNS) and digital identities (Namecoin, 2014). It protects the right to free expression on the internet by making the web more resistant to censorship. Akins (2013) suggests expanding the use of blockchain technology beyond its current applications in areas like marriage registration, patent management, and taxes administration. As blockchain becomes more integral to government operations, digitally signed mobile devices may replace traditional seals on official documents. The massive amount of paperwork will be greatly reduced as a result of this (Goldman Sachs, 2016).

Management of One's Reputation

One of the most important indicators of how much people trust, believe in and respect you is your reputation. A person's trustworthiness in the eyes of others is proportional to the quality of their reputation. Each person's reputation may be gauged by looking at their past dealings and interactions with the public. The instances of people exhibiting a false identity are on the rise. For example, many service providers in the e-commerce sector intentionally sign up a huge number of fake customers to boost their reputation. Blockchain technology is the key to fixing this problem.

1. To begin with, one's standing among peers is quite important in the academic world. Sharples (2015) argued that the distributed ledger technology used in blockchains should be used for academic and professional reputations as well. The first stage is to provide each establishment and expert employee with some kind of preliminary prize scholastic reputation currency. If a company wants to show its appreciation for a worker, it will share some of the credit for that worker's stellar reputation. As all transactions are publicly accessible on the blockchain, it is easy to detect any shift in standing.
2. To be able to evaluate the standing of any member of the online community is a crucial ability. Carboni (2015) proposed a reputation model based on a blockchain, in which satisfied customers would sign a voucher to attest to their satisfaction and offer positive feedback. When the consumer signs the voucher, the service provider is required to pay an extra 3% of the total cost to

the system as an optional charge to deter Sybil attacks. The sum of the voting fee may be used to estimate the service provider's standing. Dennis (2015) proposed a novel reputation setup that may be used across a wide variety of networks. As specified, they developed a novel blockchain that may log completed transactions with any one-dimensional values of reputation, such as 0 or 1. Here, A might transfer any file to B. B then sends a transaction with the score, hash of the file, and B's private key to verify the identity of the sender after receiving the file. When that is done, the miners will contact A and B to ensure the transaction is legitimate. As all reputation-related transactions are permanently recorded on the blockchain, it is impossible to falsify them (Akins et al., 2015).

SAFETY AND CONFIDENTIALITY

Safety Improvement: Since more people are using more kinds of mobile phones and services, many of them are more vulnerable to harmful nodes. There are a plethora of anti-malware strainers advised to locate malicious files by using the same pattern methods. The host computer where the bug may be stored and updated. Yet, these centralized defensive procedures are vulnerable to certain sneaky attackers. There is room for improvement in the security of large-scale networks, but this is where blockchain technology comes in. Noyes (2016) proposed BitAV, a novel anti-malware environment in which the user may assign the virus's pattern on the blockchain. This method allows BitAV to be more tolerant of errors. Noyes (2016) demonstrates that BitAV may be utilized to speed up scanning and enhance fault dependability, i.e., reduce susceptibility to directed ignorance of the service attacks. Blockchain technology may also be used to increase the trustworthiness of the security infrastructure. The reliability of conservative Public Key Infrastructure (PKIs) is sometimes called into question because of worries about bugs in the system's hardware or software, as well as malicious assaults. According to Axon (2015), blockchain technology may be used to improve the trustworthiness of traditional PKIs while simultaneously facilitating the creation of more privacy-friendly ones.

CONFIDENTIALITY Protection: More and more apps and websites on our phones and the internet are collecting our private information, which puts us in danger of having it stolen by malware. For instance, since its founding day, Facebook has amassed more than 300 petabytes of user data (Vagata, 2014). The obtained information is often stored at the primary servers of the service providers, which are often the origins of malicious attacks. Blockchain technology may be used to increase the security of sensitive private data. To provide a decentralized system for private data management that gives users control over their data while protecting its confidentiality (Gupta, 2014). The blockchain platform is used for this setup. The following are examples of privacy issues that may be mitigated by this system:

- Data ownership,
- Data audibility,
- Data transparency, and
- Data access control at granular levels

To similarly and autonomously distribute sensitive information, Ethos proposes a solution based on blockchain technology (2014).

REFERENCES

1. Akins, B. W.; Chapman, J. L.; Gordon, J. M.: A Whole New World: Income Tax considerationsof The Bitcoin Economy. 2013, https://ssrn.com/abstract=2394738.
2. Atzori, M (2015) Blockchain Technology and Decentralized Governance: Is the State Still Necessary? Work Pap Barber S, Boyen X, Shi E, Uzun E (2012) Bitter to Better—How to Make Bitcoin a Better Currency. International Conference on Financial Cryptography and Data Security. Springer, Heidelberg, pp 399–414.
3. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A Survey. (15), 2787–2805. Axon, L.. Privacy-Awareness in Blockchain-based PKI. CDT Technical Paper Series, 2015.
4. Biryukov, A.; Khovratovich, D.; Pustogarov, I. Deanonymisation of Clients in Bitcoin p2p Network. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. pp. 15–29. New York, NY, USA, 2014.
5. Carboni, D.(2015). Feedback-Based Reputation on Top of the Bitcoin Blockchain. arXiv preprint arXiv:1502.01504.
6. Devine, P. Blockchain Learning: Can Crypto-currency Methods be Appropriated to Enhance
7. Online Learning? In: ALT Online Winter Conference, 2015.
8. Dixon, C.; Mahajan, R.; Agarwal, S.; Brush, A.; Saroiu, B. L. S.; Bahl, P. An operating system for the home. In: NSDI. USENIX, 2012.
9. Ethos (2014), http://viral.media.mit.edu/projects/ethos/
10. Eyal, I.; Sirer, E. G. Majority is not enough: Bitcoin mining is vulnerable. In: Proceedings of International Conference on Financial Cryptography and Data Security. pp. 436–454. Berlin, Heidelberg, 2014.
11. Fan, Z.; Kulkarni, P.; Gormus, S.; Efthymiou, C.; Kalogridis, G.; Sooriyabandara, M.; Zhu, Z.; Lambotharan, S.; Chin, W. H. Smart Grid Communications: Overview Of Research Challenges, Solutions, And Standardization Activities. (1), 21–38.
12. Federal Bureau of Investigation (2012) Bitcoin Virtual Currency: Intelligence Unique Features Present Distinct Challenges for Deterring Illicit Activity. https://www.wired.com/ images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf. Accessed 30 Nov 2016.
13. Foroglou, G.; Tsilidou, A. L. Further Applications of the Blockchain, 2015.
14. Glaser, F. Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain-Enabled System and Use Case Analysis, 2017.
15. Glaser, F., Zimmermann, K.: Haferkorn, M.; Weber, M.; Siering, M. Bitcoin-asset or Currency? Revealing Users' Hidden Intentions. In: Proceedings of the 22nd European Conference on Information Systems (ECIS 2014); Tel Aviv, Israel, 2014.
16. Gogerty, N.; Zitoli, J. Deko: An Electricity-backed Currency Proposal. Social Science Research Network, 2011.

17. Goldman Sachs Profiles in Innovation – Blockchain. http://www.the-blockchain.com/docs/ Goldman-Sachs-report-Blockchain-Putting-Theory-into-Practice.pdf. Accessed 30 Nov 2016.
18. Gupta, M. Blockchain for Dummies, IBM Limited Edition, John Wiley and Sons, Hoboken, NJ, available at: https://public.dhe.ibm.com/common/ssi/ecm/xi/en/xim12354usen/ XIM12354USEN.PDF
19. Habib, K.; Torjusen, A.; Leister, W. Security Analysis of a Patient Monitoring System for the Internet of Things in eHealth. In: The Seventh International Conference on eHealth, Telemedicine, and Social Medicine (eTELEMED), 2015.
20. Hardjono, T.; Smith, N. Cloud-based Commissioning of Constrained Devices Using Permissioned Blockchains. In: Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security. pp. 29–36. ACM, 2016.
21. IBM Blockchain.http://www.ibm.com/blockchain/the blockchain. In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). pp. 131–138. IEEE,2015.
22. IBM: IBM ADEPT Practitioner Perspective - Pre-Publication Draft, 2015. ISO/IEC 18000 (2013), http://en.wikipedia.org/wiki/ISO/IEC_18000
23. Jaag, C.; Bach, C.; et al. (2016). Blockchain technology and cryptocurrencies: Opportunitiesfor postal financial services. Tech. rep.
24. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In: Proceedings of IEEE Symposium on Security and Privacy (SP). pp. 839–858. San Jose, CA, USA, 2016. Luther,
25. W. J.; White, L. H. Can Bitcoin Become a Major Currency? Working Paper. Miers, I, Garman, C, Green, M, Rubin, A. D. (2013) Zerocoin: Anonymous Distributed e-cash from Bitcoin. IEEE Symposium on Security and Privacy. IEEE. pp 397–411, 2014.
26. M. Nofer et al. Blockchain, Bus Inf Syst Eng 59(3):183–187 (2017) In Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS 2017), Waikoloa Village, Hawaii, 2017.
27. Michele, E.; von der Heyde, L. Holding, Clearing And Settling Securities Through Blockchain Technology Creating an Efficient System by Empowering Asset Owners. Social Science Research Network.
28. Microsoft Azure: Blockchain as a Service. (2016), https://azure.microsoft.com/en-us/ solutions/blockchain/
29. Miorandi, D.; Sicari, S.; Pellegrini, F. D.; Chlamtac, I. Internet of Things: Vision, Applications and Research Challenges. (7), 1497–1516.
30. Mishkin, F. S. The Economics of Money and Financial Markets, 7th Edn. Pearson: Boston, 2004.
31. Morini, M. From 'Blockchain Hype' to a Real Business Case for Financial Markets. Social Science Research Network, 2016.
32. Nakamoto, S. Bitcoin: A Peer-To-Peer Electronic Cash System (2008), https://bitcoin.org/ bitcoin.pdf
33. Namecoin (2014), https://www.namecoin.org/
34. Norta, A.; Othman, A. B.; Taveter, K. Conflict-resolution Lifecycles for Governed Decentralized Autonomous Organization Collaboration. In: Proceedings of 2015.
35. International Conference on Electronic Governance and Open Society: Challenges in Eurasia. pp. 244–257. ACM, 2015.
36. Norton, S. (2016), "CIO explainer: what is blockchain?", The Wall Street Journal Blog,
37. available at: https://blogs.wsj.com/cio/2016/02/02/cio-explainer-what-is-blockchain/ Noyes, C. (2016). Bitav: Fast Anti-Malware by Distributed Blockchain

Consensus and
38. Feedforward Scanning. arXiv preprint arXiv:1601.01405
39. Noyes, C.: Efficient Blockchain-Driven Multiparty Computation Markets at Scale. Tech. rep. (2016).https://www.overleaf.com/articles/blockchain-multiparty-computation-markets-at- scale/mwjgmsyybxvw/viewer.pdf
40. NRI: Survey on Blockchain Technologies and Related Services. Tech. rep., 2015.
41. Peters, G. W.; Panayi, E. Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing And Smart Contracts on the Internet of Money. Social Science Research Network, 2015.
42. Peters, G. W.; Panayi, E.; Chapelle, A. Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective (2015), http://dx.doi. org/10.2139/ssrn.2646618
43. Pilkington, M. Blockchain Technology: Principles and Applications. In , Olleros, F. X., Zhegu, M., Eds. Edward Elgar. Available at SSRN: http://ssrn.com/abstract=2662660
44. Richard Dennis, G. O. In, Proceedings of the 10th International Conference for Internet Technology and Secured Transactions, 2015, pp. 131–138.
45. Sharples, M.; Domingue, J. The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. In: Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015). pp. 490–496. Lyon, France, 2015.
46. Tschorsch, F., Scheuermann, B. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. 18(3), 2084–2123.
47. Vagata, P.; Wilfong, K. Scaling the Facebook Data Warehouse to 300 PB. Tech. rep. (2014), https://code.facebook.com/posts/229861827208629/ scaling-the-Facebook-data-warehouse-to-300-pb/
48. Wang, H.; Osen, O.; Li, G.; Li, W.; Dai, H. N.; Zeng, W. Big Data and Industrial Internet Of Things For The Maritime Industry In Northwestern Norway. In: IEEE Region 10 Conference (TENCON), 2015.
49. Zhang, Y.; Wen, J. An IoT Electric Business Model Based on the Protocol of Bitcoin. In: Proceedings of 18th International Conference on Intelligence in Next Generation Networks(ICIN). pp. 184–191. Paris, France, 2015.