11-2021

Blockchain Applications: SME Interviews and Financial & Banking Use Case

Van Tran
University of Northern Iowa, vtran@uni.edu

Matt Barton
Epic

See next page for additional authors

DECISION SCIENCES INSTITUTE

Blockchain Applications: SME Interviews and Financial & Banking Use Case

Van Tran
University of Northern Iowa
Email: vtran@uni.edu ; haivantran.29@gmail.com

Matt Barton
Epic
Email: bartomab@uni.edu ; mrb708058@gmail.com

Dan Bumblauskas, Ph.D.
University of Northern Iowa
Email: daniel.bumblauskas@uni.edu

Arti Mann, Ph.D.
University of Northern Iowa
Email: arti.mann@uni.edu

ABSTRACT

Blockchain is an emerging technology that is believed to be "the next internet." In this paper, we try to answer the questions- What is blockchain? How does blockchain work? and what are its uses across different industries? We also explore blockchain from a theoretical perspective and discusses its various applications. We analyze the drawbacks of this technology and also explore the uses of this technology in banking security and risk management.

KEYWORDS: Blockchain, Cybersecurity, Bitcoin, Digital Identity Management, Supply Chain

INTRODUCTION

Throughout human history, few technological advancements have so profoundly impacted the future that they are considered general-purpose technologies. Among the ranks of these advancements include the steam engine, electricity, and robotic automation (Muro & Andes, 2015). Blockchain, a driving force behind cryptocurrencies and simultaneous transactions, is predicted by many experts to emerge as the new general-purpose technology (Bullock, personal communication, 2021; [removed for blind peer review]). The adoption of blockchain was further pushed by the COVID-19 pandemic, as it revealed weaknesses in current supply chains and data management systems. Organizations, government agencies, and companies partnered to build blockchain-based solutions to effectively map and analyze the medical supply chain (van Hoek & Lacity, 2020). Blockchain was also used to build a faster and more secure data-sharing system amongst individuals, hospitals, governments, and other organizations (van Hoek & Lacity, 2020). The COVID crisis created the perfect storm for hackers around the world as they took advantage of the chaos and the expanding technology footprints and attack surface. The finance sector became one of the main targets as finance-related attacks accounted for 52% of all attacks seen across the VMware Carbon Black dataset, which was 'an unprecedented anomaly in [their] data tracking' (Upatham & Treinen, 2020). To combat the increasingly sophisticated frauds and cyberattacks, financial companies started looking into integrating

blockchain into their security systems. Blockchain's ability to foster data sharing without affecting data privacy and security can help improve data-driven decision-making processes while maintaining democratic values.

This brings us to the questions: What is blockchain?, How does blockchain work?, and What is blockchain used for? Through a careful analysis of publications, expert opinions, and informed research, this article defines blockchain, explore its theories, and examine its uses. We will also explore the concepts of the so-called double-spending problem, as well as the immutability and distributed ledger properties that solve this problem and so clearly define blockchain. We further provide a discussion on the uses of blockchain and focus on specific fields where blockchain may prove especially useful, such as in trade between new partners, agriculture and food, finance, healthcare, and security. Drawbacks of blockchain are also explored, including environmental impact and a lack of regulation so notable that it is even referred to as the "wild west" by experts (Bullock, personal communication, 2021; [removed for blind peer review]), will also be investigated. Finally, an anticipated future of blockchain applications will be provided.

Through this paper, a thorough analysis of blockchain technology has been researched. This technology is often regarded as the "next internet" in the business world: while the uses are at times not very apparent, businesses believe the impact of blockchain on the world will be revolutionary. As such, this paper will explain how blockchain works from a theoretical perspective, exploring the concepts and foundations that enable its functionalities as well as the current uses and applications of blockchain with a focus on banking security and risk management. This paper also serves to explain the drawbacks of this technology, as well as possible threats to its future. Finally, using this information, this work will answer the question: what applications will blockchain likely support in the future?

LITERATURE REVIEW

In its simplest form, a blockchain is a continuous ledger of business transactions that can never be deleted; the ledger can only be altered by adding additional transactions (Mougayar, 2016). It removes 'middlemen' entirely or requires them to add new information in blockchain processes because "trust" can be found by simply following the blockchain trails (Mougayar, 2016). In other words, middlemen, such as brokers who find trustworthy trade partners, will no longer be needed to determine how trustworthy another party is because their history is documented in the blockchain. Furthermore, while traditional databases are administered and only create the "illusion" of reliability, blockchain technology is cataloged such that the data is "irrefutable" (Mougayar, 2016). On a similar note, blockchains can be used to confirm a transaction, and this confirmation means that it is less likely that a transaction will be canceled (Ricci et al., 2019). Blocks are reconfirmed each time a block is added to the blockchain, meaning that all prior transactions become less likely to be reverted whenever a new block is added (Ricci et al., 2019). Blockchain can create an efficient and trustless environment through smart contracts, which are unbiased, digitized agreements that automatically execute if and only when all requirements of a transaction are met. Thus, one can safely conclude that, with blockchain, there are benefits to businesses that conduct business in a trustworthy manner, lest they have a long, permanent history of reverted transactions or, even worse, an undeniable history of disreputable behavior documented in the blockchain.

There are two types of blockchains – permissioned (private) and permissionless (public). A public blockchain is open to everyone, and an example of a public blockchain is the platform

that runs Bitcoin. Public blockchain platforms employ a crypto-economic model that rewards users' tokens as a way to incentivize them to contribute to the networks (Kadiyala, 2018). The more decentralized and distributed the network is, or the longer the transaction history, the harder it is to hack into. On the other hand, a permissioned blockchain is only accessible to a certain number of nodes who have permission to enter. It is usually built for an organization or a consortium to exchange information. A private blockchain is not completely decentralized as the identities of all nodes are managed. The consensus mechanisms of these blockchains are relatively inexpensive when compared to the public blockchain. They are also much more scalable and efficient than permissionless platforms (Kadiyala, 2018). As they do not follow the same crypto-economic model, many permissioned blockchains do not have their currency.

The value of blockchain, as well as its applications, are founded on five basic principles: “truth and trust,” “transparency,” “security,” “quality and certainty,” and “efficiency” (Welfare, 2019, p. 10-11). Welfare explained that one major use of blockchain is the utilization of cryptocurrency, which are essentially virtual currencies that demonstrate the same characteristics as other blockchain technologies (permanent transaction records, distribution of these records, and all other characteristics). Welfare goes on to explain applications in “identity management”, “loyalty” programs, “warranty management and refund management”, along with numerous supply chain applications such as the handling of inventory, logistics and transportation, and even counterfeit prevention. Bumblauskas et al. (2020) explores the applications utilized by Bytable Inc. for the distribution of eggs. Specifically, this study uses blockchain to determine the routes eggs take as they travel “from farm to consumer.” Blockchain enables a variety of benefits to the egg industry. First, it allows for compliance with FDA regulations. Second, when utilized with other technologies, relevant information can be easily maintained. In the egg use case, temperature sensors are used to add temperature information to the blocks in the blockchain so that Bytable, Inc. knows the eggs were stored at a safe temperature. In the event of recalls, Bytable Inc. will know which sources required a recall and will know exactly which egg cartons came from which sources because it is all stored in the blockchain. Finally, “food fraud and ethics” are accounted for because Bytable, Inc. can ensure their suppliers uphold the ethical standards their consumers are willing to pay extra for (e.g., fair treatment of the chickens that lay the eggs) (Bumblauskas et al., 2020). Ultimately, Bumblauskas et al. (2020) determined blockchain is a viable means of food tracing.

Regarding future research, Ante (2020) identifies further avenues for research to be conducted in the field of blockchain. Ante (2020) considers the original theories for blockchain presented by Satoshi Nakamoto in 2008 and seeks additional room for research in his article. In addition to applications of blockchain, the area of research this study will explore, Ante (2020) finds a need to conduct further research into the anonymity of transactions. Blockchain allows for anonymous transactions if the information linking the transaction to one specific person is withheld, as explained by Nakamoto (2008) in the original white paper explaining the concept of Bitcoin.

METHODOLOGIES

The first aspect of the methodology for this study involves the analysis of scholarly articles and other publications on the subject matter. Through analysis and synthesis of these publications, strong background details and a preliminary summary of the applications of blockchain, both current and future, will be produced.

The next aspect of the methodology behind this study is a small set of interviews with experts on the subject matter. The first person interviewed is Bert Bullock, a long-time expert in computer technology with a rich history of introducing and utilizing cutting-edge technology in various businesses including Alcare Computers, EDS, AtlasVac, and other businesses in the technology sector. Bert regularly studies the latest innovations in regards to information systems, and blockchain is one such technology he studies. The second person interviewed [has been removed for blind peer review].

Finally, concepts and current applications of blockchain are synthesized into a projection of the future of blockchain and the businesses that will be most impacted by these innovations. This synthesis incorporates ideas proposed by the aforementioned experts, as well as utilizes a working knowledge established through a review of literature and publications on blockchain technology. These projections are not merely wishful thinking and personal predictions, but rather a well-defined and highly plausible image of the future of blockchain.

THEORIES BEHIND BLOCKCHAIN

The greatest aspects of the blockchain theory lie in the original Bitcoin white paper, written by the enigmatic Satoshi Nakamoto, which presents the first recommended solution to an issue known as the double-spending problem. As Entertainment Newsweekly (2020) describes, “in blockchain networks, due to reproducibility of data, a digital asset could be reused. For example, multiple parallel blockchain transactions can be performed on the same (sic) digital asset (referred to as double-spending).” This, of course, presents a very clear counterfeiting problem, as digital assets such as digital currencies would only hold value if the assets cannot be replicated freely. Nakamoto (2008) produces “a solution to the double-spending problem using a peer-to-peer network” in Bitcoin. Bitcoin, being confirmed in this peer-to-peer system, prevents double-spending; it uses hashing to prove the order in which transactions occur, and it utilizes cryptography to prevent attackers from modifying this chronological data. By proving the chronological order of transactions, the blockchain would not accept multiple transactions to occur on one asset.

This system, of course, depends on a peer-to-peer network, as Nakamoto (2008) describes. Because many transactions take place in blockchain, a large number of computers are needed to constantly confirm the order of transactions. The computers not only prove the transactions but encrypt the data in the blocks so that an attacker cannot later alter the data to enable double-spending, according to Nakamoto (2008). The encryptions used in Bitcoin, as Bullock (personal communication, 2021) describes, are incredibly difficult to break, taking unfathomably long amounts of time for a classical computer to solve. For this reason, blockchain takes on its immutability: if the blocks could be modified, the double-spending problem would remain unsolved, as attackers could change the data and double-spend the digital assets.

Chronology, however, is not enough to completely prevent the double-spending problem. Nakamoto (2008) recognizes that there must also be a system to identify which assets are legitimate and which are simply replicas. Therefore, a repository documenting which assets are real and which assets are fraudulent proves necessary, but Nakamoto (2008) did not want to use a central “mint”, as he called it, that users would simply have to trust. Thus, the distributed ledger emerges: if all computers engaged in the network could agree on which assets and transactions are legitimate, then any outside fraudulent assets used by attackers attempting to

double-spend could be recognized as fakes (Nakamoto, 2008). The distributed ledger quite literally distributes the ledger across every computer in the network, meaning all computers engaged in the blockchain processes must store the entire blockchain. To be clear, as Nakamoto (2008) described blockchain, there is no location where any data should be stored or accessed beyond blockchain participants' computers. This adds an additional layer of security: no attacker can simply access a central data repository and change information, as there is no repository to attack. Therefore, even if one node was altered, the chain would be protected. One obvious concern, of course, relates to the storage of all this data, but Nakamoto (2008) dispels these concerns. The storage space required to hold every single block generated in a given year, assuming new blocks are generated every ten minutes, will on average require "4.2 MB (megabytes) per year (Nakamoto, 2008)." For perspective, some of the smallest hard drives one could reasonably expect to find in a modern computer hold over 30,000 times as much data.

The entire theory enabling blockchain solutions that do not double-spend are summarized in a set of steps, also described by Nakamoto (2008) in his white paper. To summarize, somebody attempts to complete a transaction, and all computers in the network are notified. Then, one "node" of the network "collects new transactions into a block (Nakamoto, 2008)." Cryptography is applied to secure the data in the transaction, then the original node informs all the other nodes within the network. All other computers in the network then verify with each other that "all transactions in (the block) are valid and not already spent (Nakamoto, 2008)." Finally, the transaction is solidified by locking it in place when a new block is added to the chain. Through these steps, Nakamoto's theoretical blockchain that solves the double-spending problem can be expressed in all practical applications of blockchain.

APPLICATIONS OF BLOCKCHAIN

On its most foundational level, blockchain creates trustworthiness in transactions. As Bert Bullock (personal communication, 2021) explains, blockchain allows for "simultaneous" transactions in which ownership titles and currency are exchanged at precisely the same moment in time. As a result, the transaction is added to the blockchain, all items in the transaction immediately change hands, and there is no need to trust the other parties in the transaction. As Bullock (personal communication, 2021) explains, "blockchain builds trust where trust is in dispute."

An area of blockchain application that has been gaining a lot of interest in recent years is fintech. Despite blockchain being a fairly new technology, the benefits that it brings are being widely recognized by business leaders in the finance sector. According to a survey conducted by Cognizant - a technology company that specializes in business consulting, information technology and outsourcing services - firms in the financial sector believe improved data management, improved risk management, heightened security, reduced fraud, and improved auditing are among the top benefits of blockchain (Varghese et al., 2017, p. 8). A study by Taylor et al. (2020) shows that the majority of blockchain research on cybersecurity focuses on the Internet of things (IoT) (45%) and Data storage and Sharing (16%) (p. 150). Leaders in the industry are starting to look into blockchain to create a secured environment that can protect them against cyber-attacks and frauds.

Firstly, the implementation of blockchain can help banks control risks much more effectively. All transactions being encrypted, tamperproof, time-stamped, and tracked in real-time discourage fraudulent activities. As a result, communications among peers are protected, and the integrity

of data is ensured. In addition, audits can be conducted more effectively. Blockchain technology and its transparency element also allow banks to verify the identity of their customers, which saves banks time and money on their Know Your Customer (KYC) process.

Secondly, blockchain can enhance data privacy and security as all data is encrypted and stored across all nodes in the network instead of just one centralized server, which eliminates a single point of failure. An article by Deloitte discusses the applications of blockchain on the Internet of Things (IoT) security and Distributed Denial of Services (DDoS) attack prevention. A DDoS attack overloads a targeted server by recruiting multiple computers (botnets) connected to the Internet to send traffic simultaneously and repeatedly. Hackers either remotely access devices using easily guessable login credentials to install malware, or they launch DDoS attacks with a Command and Control server, which is a master server that gives instructions for the bots to read and act on (Sallaba et al., 2017, p. 2). Instead of the default login credential, blockchain requires devices to use a public key and private key cryptography that would only be known to the user, making the system more difficult to hack (Sallaba et al., 2017, p. 2). As a decentralized, peer-to-peer network, the attacker's Command and Control server will not be able to gain access to control other nodes to launch a DDoS attack. Sallaba et al. also notes that blockchain can eliminate the use of Domain Name System (DNS) server, which is a centralized server that maps IP addresses to domain names (2017, p. 2-3). As the name and address pair will be stored on blockchain and copied across all nodes, there is no longer a need for a DNS server and therefore, no one single point of failure. Lastly, the distributed and shared nature of the blockchain could facilitate the recovery of both data and processes in the case of an attack (assuming that not all the nodes are corrupted simultaneously). This could reduce the need for costly recovery plans (Dzhaparov, 2020, p. 47).

As smart contracts are unbiased, digitized agreements that only execute when all requirements are met, less trust is needed between partners. This, along with other benefits of blockchain discussed above, provides a safe environment that encourages the sharing of information between partners, with or without trust being established in advance.

As mentioned above, the use of blockchain in digital identity management is one of the areas that are gaining interest. Since the COVID-19 pandemic moved many different financial services online, banks need to rethink their identity verification and credential sharing processes as physical contacts need to be kept to a minimum. Sensitive data is stored in centralized databases by third parties opens up many vulnerabilities for hackers to exploit. Furthermore, customers having to manage multiple accounts and passwords over many different websites also put their data at risk. They can forget their log-in credentials, which in return might force them to provide third parties with even more personal data to regain their passwords. Similar, easier-to-remember passwords can also be used over multiple websites as a result, leaving many of their online accounts vulnerable. Lastly, the KYC policies have always been considered overly costly and complex.

Blockchain introduces a new identity management system with the concept of self-sovereign identity, which allows an individual (a person or an organization) to be in full control and ownership of their own data. Figure 1 is a blockchain's identity management framework proposed by Aydar, Ayvaz, and Cetin (2020, p. 7-17).

Figure 1 *Overall workflow of the proposed identity system*

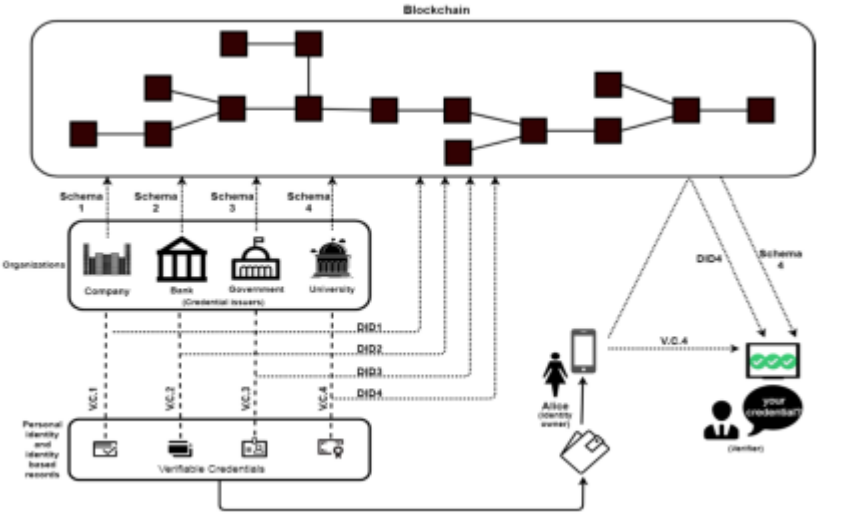

Figure 1 Note. From "Towards a Blockchain based digital identity verification, record attestation and record sharing system," by M. Aydar, S. Ayvaz and S. Cemil, 2020, p. 8 (https://arxiv.org/abs/1906.09791). arXiv.org perpetual, non-exclusive license.

In the system above, a digital identity is assigned to each individual through blockchain. The blockchain itself does not store any actual private personal data, but rather the proof of verification (Aydar et al., 2020, p. 8). For example, if someone's driving license is being used to verify their identity, the actual license is not stored on the blockchain. What will be on the blockchain is just the fact that their document has been verified by, in this case, the local government and therefore is good to use (Aydar et al., 2020, p. 8). Users can store all of their verifiable credentials, which are machine readable, cryptographically secure digital credentials, in an identity wallet. Once again, identity owners fully control their data and can divide whom to share their data.

This identity management system allows banks to streamline their customer on-boarding processes. Banks no longer have to spend as much time, money and labor on verifying customers' information. Transparency as well as information accuracy and reliability are also significantly increased. Due to the secure nature of blockchain, the risk of ID theft and fraud is also reduced.

For customers, blockchain's identity management system provides a much more convenient user experience as all verifiable credentials are stored in one place, users no longer need to memorize multiple log-in credentials or reach out to third parties whenever they need to verify their identities. Customers are once again in full control of their own data, which provides full transparency between customers and financial institutions.

However, this framework is not without flaws. Since all identities are essentially created and only exist in the digital world, banks still need to figure out who is responsible to provide the trust mapping between real life physical identity and the digital identity ("Practical thoughts," n.d., p. 9). It will be crucial to ensure that a vulnerable identity provider doesn't open up opportunities for an identity takeover on the network. Furthermore, with blockchain still being a very new technology, businesses may face resistance from both partners and their own employees. In order to retain their customers, verifying organizations may refuse to share data or collaborate

("Practical thoughts," n.d., p. 10). Lastly, there has not been many clear regulations on the use of blockchain in the financial sector. As a result, all entities involved have to accept risk and uncertainty by agreeing to participate in an identity network.

Figure 2 shows an example use case of a loan application (Aydar et al., 2020, p. 11). In this use case, the customer Alice, who is a current customer of Bank A, wants to apply for a loan with Bank B. Bank A and Bank B are trusted partners. Alice also owns land, and that information is kept by the local government. Because Bank B has never worked with Alice before, they are required by KYC regulations to know her before accepting her application. Using the proposed framework, Allice authenticates herself with Bank B, who then reaches out to related organizations to collect the information needed for the loan application. Alice will need to give her consent to these organizations before they can share her information in the form of verifiable credentials. The whole process happens within minutes without physical interaction between any parties involved.

Figure 2 *Use Case: Loan Application*

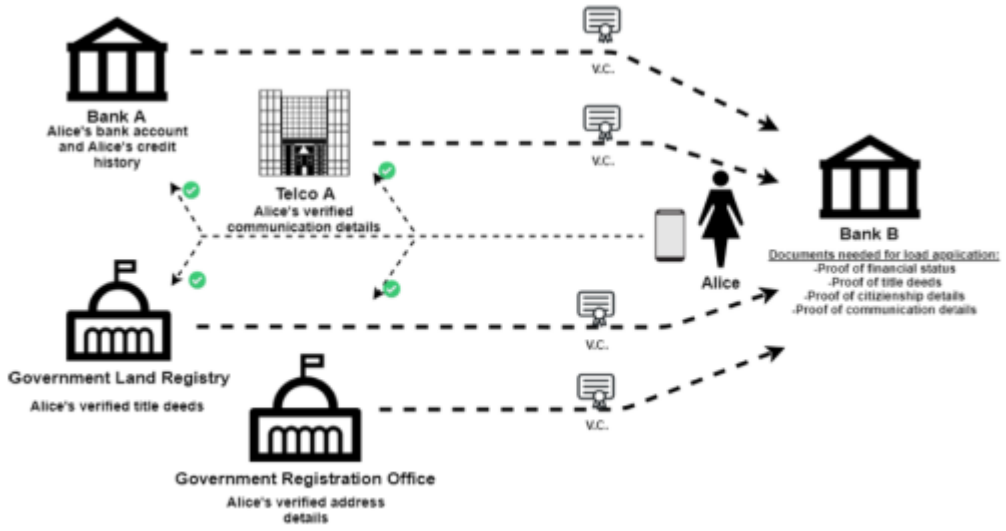

Figure 2 Note. From "Towards a Blockchain based digital identity verification, record attestation and record sharing system," by M. Aydar, S. Ayvaz and S. Cemil, 2020, p. 11 (https://arxiv.org/abs/1906.09791). arXiv.org perpetual, non-exclusive license.

DRAWBACKS AND LIMITATIONS OF BLOCKCHAIN

Blockchain, despite its many advantages, is not without its risks and downsides. Concerns are especially strong in regards to the tremendous environmental impact in processes that do not add value to the blockchain, which are derived from significant energy usage. Another major concern is the lack of regulation and possibilities for hacking, allowing so-called crypto-heists to occur. Numerous other issues, which have received less research attention, also exist and will be discussed as well. For blockchain to become a more viable solution, these concerns must be addressed.

Blockchain's dependence on peer-to-peer computer networks and cryptography presents a strong disadvantage for the environment. As Bullock (personal communication, 2021) explains, tremendous costs are necessary to add each block to a blockchain. Bullock is not alone, as Juričić et al. (2020) acknowledge that "blockchain is still strongly criticized for its lack of usefulness and resource-heavy consumption." These authors continue to explain that, in this blockchain system, computers must complete large amounts of calculations that add no direct value at all, but merely allow the system to function accurately. Juričić et al. (2020) describe using a graph that bitcoin mining, which is the process that validates blocks, uses approximately 75 trillion watt-hours of energy every year, and is estimated to soon consume nearly as much energy as the country of Ireland in these processes that add no direct value to any tangible goods or services. Juričić et al. (2020) further explain that most of this mining occurs in places that burn coal to produce power, generating a great deal of pollution in the process.

Another serious and concerning aspect of blockchain, in its current state, is its distinct lack of regulation. This lack of regulation serves as a double-edged sword, as Bullock (personal communication, 2021) explains: while there is much room for innovation to occur unhindered, there is also no authority to turn to when things go wrong. Botsman (2017) identifies one particular case where the Decentralized Autonomous Organization (DAO), which was based on a blockchain network known as Ethereum, was hacked and nearly lost over 60 million US dollars in cryptocurrency. Botsman (2017) further explains that rules were written into the Ethereum network's code to reverse the transaction using a "hard fork," which is "technical jargon for essentially rewriting history or changing the rules." Nonetheless, the DAO had no laws or governments to turn to and had to make this decision for themselves. Their decision to use a hard fork, Botsman (2017) documents, cost significant trust in the Ethereum network by performing what many considered a "blockchain sin," as it ran counter to numerous blockchain principles set forth by Nakamoto (2008) in his white paper, particularly in regards to the finality and immutability of transactions.

In addition to these major disadvantages of blockchain, Niranjanamurthy et al. (2019) and Bullock (personal communication, 2021) highlight other, less-researched drawbacks of this technology. Bullock expresses concerns about the amount of time required by a computer to validate blocks, and these concerns are echoed by Niranjanamurthy et al. (2019). This time is primarily derived from the time it takes to complete cryptographic processes, as well as time spent updating nodes in blockchain's peer-to-peer network. In his paper "The Quest of Scalable Blockchain Fabric," Marko Vukolic brings forth the tradeoff between scalability and performance amongst the two types of blockchain - Proof-of-Work (PoW) based and Byzantine fault-tolerant (BFT) based (2015, p. 4). PoW blockchain is the technology behind Bitcoin which requires nodes to "mine," or to add another block to the chain. A block is usually added every ten minutes, and mining takes up a lot of computing power (Vukolic, 2015, p. 2). However, PoW blockchain is a public blockchain and offers good scalability. On the other hand, BFT-based blockchain offers good performance for a small number of replicas or nodes (Vukolic, 2015, p. 3). This brings up the discussion of the Scalability Trilemma, a term coined by the founder of the public blockchain Ethereum, Vitalik Buterin (Viswanathan & Shah, 2018). The trilemma refers to the tradeoffs between security, scalability, and decentralization. Currently, there are no blockchain platforms that can optimize all three of these factors, and it is up to the business to decide which factors are best suited for their needs.

In addition, Niranjanamurthy et al. (2019) also acknowledge concerns in integrating blockchain systems, which inherently require the replacement of existing systems. As a result,

implementing a blockchain framework into a new company requires both time and money, and it requires “cultural adoption,” all of which can prove difficult to overcome. It is also worth noting that blockchain technology has only been around for ten years. Smart contracts, though more reliable, are expensive and difficult to program. Several studies selected analyzed proposals or concepts and have little quantitative data or practical applications.

In addition, Niranjanamurthy et al. (2019) identify further hacking risks besides the aforementioned crypto-heists, including “user identity theft,” “injection of malicious code into a distributed ledger,” and “fictitious blockchain applications (that) will appear to steal transaction details/personal information/behavior from nodes/individuals,” among others (pp. 14754-14755). While blockchain’s decentralization has the power to transform governments and businesses, it introduces a different set of weaknesses. For industries that require a high level of confidentiality such as financial services, private data can be monitored and pierced together to become a serious data privacy breach as all data is being shared with all users on a network (Fitzpatrick, 2019).

THE FUTURE OF BLOCKCHAIN

Blockchain, being in its infancy, has only scratched the surface of its great potential thus far. Indeed, as Ante (2020) describes, room exists to further study the practical applications of blockchain. Based on the insight of experts in the field of blockchain, in addition to well-informed personal speculation, a glimpse into the future of blockchain can be found.

As Bullock (personal communication, 2021) explains, blockchain resolves issues where trust is questionable, which illustrates the strong potential for blockchain to facilitate contract negotiations. According to Bullock (personal communication, 2021), these applications are less developed than other existing applications, such as cryptocurrency. He explains that, because blockchain can allow simultaneous transactions when certain conditions are met, blockchain offers a contract solution by guaranteeing all parts of the transaction, such as funds and ownership titles, are traded at precisely the same time, removing the ability for one side to con the other during the trade. Furthermore, because of the immutable nature of blocks, blockchain may prove incredibly powerful at resolving contract-based conflicts, as the evidence cannot be tampered with. Simply put, Bullock (personal communication, 2021) envisions blockchain will serve as a “data repository to hold the contractual obligations between the parties.”

Both Bullock (personal communication, 2021) and [removed for blind peer review] (personal communication, 2021) expect blockchain to manifest itself especially prominently in procurement, namely regarding bills of materials. Bullock (personal communication, 2021) describes a system where blockchain facilitates just-in-time delivery utilizing the same simultaneous transaction mechanisms as in contracts. When certain criteria are met, such as inventory dipping below a certain threshold and a sufficient number of parts becoming available from a supplier, blockchain can facilitate automatic transactions to maintain an optimal supply of inventory. [removed for blind peer review] (personal communication, 2021) suggests that a different use for blockchain in bills of materials may also emerge. He suspects that a “blockchain button ([removed for blind peer review])” may be incorporated into applications so that users can see details about their product that are currently unavailable, such as where each part in the bill of materials was sourced and the steps the product took to ultimately arrive in the

hands of purchasers. Such an application would especially benefit socially conscious consumers and companies who may wish to know these smaller details, such as how environmentally friendly a product labeled as “organic” actually is or if products were manufactured in facilities with a positive track record for treatment of employees.

Another potential phase blockchain may face is centered around the idea of standardization. Because blockchain is still within early phases of development, there are multiple different blockchain systems in use at the same time, some of which are entirely incompatible with each other ([removed for blind peer review]). Considering the concerns about the energy consumption of blockchain, [removed for blind peer review] (personal communication, 2021) recognizes that “there are different ways to create (blockchain) ledgers that are less energy-intensive.” He believes that standardization of blockchain is a likely step in the near future to address some of the less-than-desirable outcomes created by the current systems.

CONCLUSION

Blockchain, although early in its life cycle, already demonstrates a powerful capacity to forever change the world of business. The COVID-19 pandemic forced companies in all industries to embrace major technological disruption and further accelerated the development and adoption of blockchain. Specifically, the banking industry - one of the main targets for hackers during the global crisis - gained more and more interest in using blockchain technology to develop a more proactive and advanced security system. Through careful analysis of articles, literature, and other written works, as well as interviews with experts, many foundational concepts of blockchain have been explained. Blockchain’s most essential aspects include a distributed ledger, transparency, and immutability, and the theories behind blockchain solutions that prevent double-spending help guarantee these qualities remain in effect. Blockchain demonstrates applications today as a trust-building tool that can provide a decentralized, trustless and transparent platform that can significantly improve security, data management and risk management in the finance sector as well as other industries. This paper introduces a blockchain-based digital identity framework that promises to foster collaboration and data sharing between businesses and their partners without the need for physical interactions between parties involved. Nonetheless, blockchain is not without its disadvantages, as it consumes tremendous amounts of power, proves to contain some vulnerabilities to malicious actors, requires a great deal of validation time for blocks, and presents organizational risks in implementation and adoption. Despite these disadvantages, blockchain has a bright future, with the most likely future applications appearing in contract negotiations and bills of materials. With these applications, and because blockchain is largely unregulated, future standardizations are also expected to come into existence. While blockchain is still early in its development, make no mistake: the next general-purpose technology has arrived.

REFERENCES

Ante, L. (2020). A place next to Satoshi: foundations of blockchain and cryptocurrency research in business and economics. *Scientometrics*, *124*(2), 1305–1333. https://doi.org/10.1007/s11192-020-03492-8.

Aydar, M., Ayvaz, S., & Cemil Cetin, S. (2020, June 23). Towards a blockchain based digital identity verification, record attestation and record sharing system. *arXiv e-prints, arXiv-1906.*

Botsman, R. (2017). The Great Crypto Heist. The Australian Financial Review, pp. The Australian financial review, 2017-10-13.

Bullock, B. (2021, March 9). Personal communication [Personal interview].

Bumblauskas, D., Mann, A., Dugan, B., & Rittmer, J. (2020). A blockchain use case in food distribution: Do you know where your food has been? *International Journal of Information Management*, *52*.

Dzhaparov, P. (2020). Application of blockchain and artificial intelligence in bank risk management. *И*кономика и управление, 17(1), 43-57.

Entertainment Newsweekly (2020). "Method And Device For Avoiding Double-Spending Problem In Read-Write Set-Model-Based Blockchain Technology" in Patent Application Approval Process (USPTO 20200349568). (2020, November 27). Entertainment Newsweekly, 626. https://link.gale.com/apps/doc/A642477304/ITOF?u=uni_rodit&sid=ITOF&xid=0fef0cee

Fitzpatrick, L. (2019, February 2). *A hacker's take on blockchain security.* Forbes. https://www.forbes.com/sites/lukefitzpatrick/2019/02/04/a-hackers-take-on-blockchain-security/.

Juričić, Vedran, Radošević, Matea, & Fuzul, Ena. (2020). Optimizing the Resource Consumption of Blockchain Technology in Business Systems. *Business Systems Research, 11*(3), 78-92.

Kadiyala, A. (2018, February 17). *Nuances between permissionless and permissioned blockchains*. Medium. https://medium.com/@akadiyala/nuances-between-permissionless-and-permissioned-blockchains-f5b566f5d483.

Mougayar, W. (2016). *The business blockchain: promise, practice, and application of the next Internet technology*. John Wiley & Sons, Inc.

Muro, M., & Andes, S. (2015, June 16). Robots Seem to Be Improving Productivity, Not Costing Jobs. *Harvard Business Review*.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. bitcoin.pdf. https://bitcoin.org/bitcoin.pdf.

Niranjanamurthy, M, Nithya, B N, & Jagannatha, S. (2019). Analysis of Blockchain technology: Pros, cons and SWOT. Cluster Computing, 22(S6), 14743-14757.

Practical thoughts on blockchain and identity. Okta. (n.d.). https://www.okta.com/resources/whitepaper/practical-thoughts-on-blockchain-and-identity/.

Ricci, S., Ferreira, E., Menasche, D. S., Ziviani, A., Souza, J. E., & Vieira, A. B. (2019). Learning Blockchain Delays. *ACM SIGMETRICS Performance Evaluation Review*, *46*(3), 122–125. https://doi.org/10.1145/3308897.3308952.

Sallaba, M., Kumar, S., & Paulsen, J. H. (2018, December 03). *Prevention of DDoS attacks with blockchain technology*. Deloitte. https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/cyber-security-prevention-of-ddos-attacks-with-blockchain-technology.html.

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks, 6*(2), 147-156.

Upatham, P., & Treinen, J. (2020, April 15). *Amid COVID-19, global orgs see a 148% spike in ransomware attacks; finance industry heavily targeted*. Carbon Black. https://www.carbonblack.com/blog/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/.

van Hoek , R., & Lacity, M. (2020, April 27). *How the pandemic is pushing blockchain forward*. Harvard Business Review. https://hbr.org/2020/04/how-the-pandemic-is-pushing-blockchain-forward.

Varghese, L., Tomer, M., & McCraw, F. (2017, June). *Financial services: Building blockchain one block at a time*. Cognizant. https://www.cognizant.com/whitepapers/financial-services-building-blockchain-one-block-at-a-time-codex2742.pdf.

Viswanathan, S., & Shah, A. (2018, October 19). *The scalability trilemma in blockchain*. Medium. https://medium.com/@aakash_13214/the-scalability-trilemma-in-blockchain-75fb57f646df.

Vukolić, M. (2015, October). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *International workshop on open problems in network security* (pp. 112-125). Springer, Cham.

Welfare, A. (2019). *Commercializing blockchain: strategic applications in the real world*. Wiley.