The Future of Blockchain and Its Implications

Xueming (Caroline) Cai

cax@seas.upenn.edu

University of Pennsylvania

EAS 499 | Senior Thesis

May 2019

Abstract

This paper explores the future of blockchain by first analyzing the technical details of the technology, and then delving into its implications in different industries. There is little doubt that blockchain will reform the banking industry with its secure transaction technology (e.g. cryptocurrency) or even replace it. However, the future of blockchain doesn't stop there. Many more industries such as music, pharmaceuticals, social media, real estate, and charity will also be impacted by blockchain applications. [1] The impact of blockchain, just like many other great technology advances in the past, is two folds. On one hand, it will replace work that is currently done manually, increasing the efficiency of the economy. On the other hand, it will be a disruptive change to many industries in the future, potentially resulting in unemployment and economic distress.

Table of Contents

Introduction

Up until this point in the human history, trust has been among the most important contributors to building a civilization. A society without trust could never survive and thrive. Arguably, it is within human nature to cheat for one's benefit when there is no enforcement of honesty; the outcome of such scenario makes itself apparent in the well-known prisoner's dilemma case.[2] In the prison's dilemma, a lack of trust between participants results in an overall sub-optimal outcome and inefficiency. Therefore, it is crucial to have some third-party enforcement agency to establish and instill trust in a society, in trades, transactions, property records, and many other relevant areas. Up until now, people mainly relied on banks and notaries to be the "middleman" or "judge" in a transaction to ensure fair-trading. We relied on somewhat siloed legal documents and government records to decide which land belongs to what family.

Today, the birth of blockchain not only made the abovementioned human efforts replaceable, but also presented us more efficient and equitable ways to accomplish these tasks. Now with the establishment of cryptocurrencies such as Bitcoin and the wide applications of blockchain, banks are no longer needed for safe transactions. Transactions are not going to be reversed or tempered with under blockchain technology. Information will not be lost.

The impact of blockchain doesn't just stop at the cryptocurrency level.[3] For example, startups such as *Steem*[4] grow communities and focus on social impact. Social media content producers could get paid for their work through microtransactions.[5] The ubiquity of information under the blockchain means no one will be treated unfairly due to inaccessibility of data. We are never closer to establishing universal trust than we are now – blockchain ensures that what happened has indeed happened and clearly documented in the record, and can never be erased or modified.

This paper will explore the technical, industrial, financial, and social implications of the rise of blockchain and where the future for blockchain holds.

History of Blockchain

Blockchain was first invented in 2008 by Satoshi Nakamoto, who released the whitepaper *Bitcoin: A Peer to Peer Electronic Cash System.*[6] While the true identity of Satoshi Nakamoto remains unknown to the public, the impact of Nakamoto's work is groundbreaking. The said whitepaper described Bitcoin as a "purely peer-to-peer version of electronic cash," introducing the concept of blockchain for the first time.

Bitcoin presents solution to an electronic currency for which transactions do not need to go through a trusted third-party financial institution to be validated. Its built-in blockchain technology legitimizes valid Bitcoin transactions and voids illegitimate activities such as double-spending (i.e. the scenario in which a user tries to spend the same money in two separate transactions). It eliminates the need for a mediator with its non-reversibility nature and fraud prevention.

Blockchain originated from Bitcoin. Blockchain provides the infrastructure for Bitcoin and other cryptocurrencies that came after. Blockchain to Bitcoin is just like interstate highway to cars or reception to cellphones – it paves the way for the latter to be used to its full potential. It is the underlying framework technology that enables Bitcoin transactions, timestamp, and proof of work, which this paper will explore in later sections.

After the introduction of Bitcoin, the concept of blockchain has been studied since 2014 by an elite group of scientists and engineers[7], with an emerging conclusion that the blockchain framework could be separated from Bitcoin and used in all sorts of organizations that involve transactions or networks.

The next notable invention after Bitcoin was smart contracts embodied in the Ethereum cryptocurrency[8], enabling blockchain transactions of other financial instruments such as loans or bonds, in addition to cash-like cryptocurrencies like the Bitcoin. Since then, blockchain has been explored in many different industries other than finance. Banking, healthcare, real estate, social media, and charity industries are all affected by blockchain, just to name a few.

What is Blockchain

Blockchain is a distributed, decentralized public ledger[9] that allows information to be shared and assessed but not copied. It is a digital ledger that stores transactions and prevents fraud. The name "blockchain" originated from the structure of the technology: it is composed of individual blocks, chained together with cryptography in the chronological order that they were created. It follows a linked-list architecture.

The blocks store useful information about transactions, such as date and time, amount of cryptocurrency in exchange, participants, and a self-identifying hash. Every block keeps track of an immutable record, and the information is decentralized and accessible to anyone in the network.

Each individual block in the blockchain is identified via two ways:

1) The main way of identification is the block header hash, which is unique to the content of the block. For example, Bitcoin uses SHA-256 (Secure Hash Algorithm, 256) and Ethereum uses Ethash to create block header hashes.[10]
2) A secondary way to identify a block is to use its *height*. The height of a block refers to its "number in line." The first ever block, the so-called **Genesis Block**, has a height of zero, and each block after it will have an incremental number. However, the height of the block is *not* a unique identifier, as multiple blocks could be competing for the

same height simultaneously.[11]

Perhaps the most remarkable aspect about blockchain is that it allows information and value to be passed on in a trusted manner, but without a third trusted party. The unique structure of the blockchain allows it to accomplish just that.

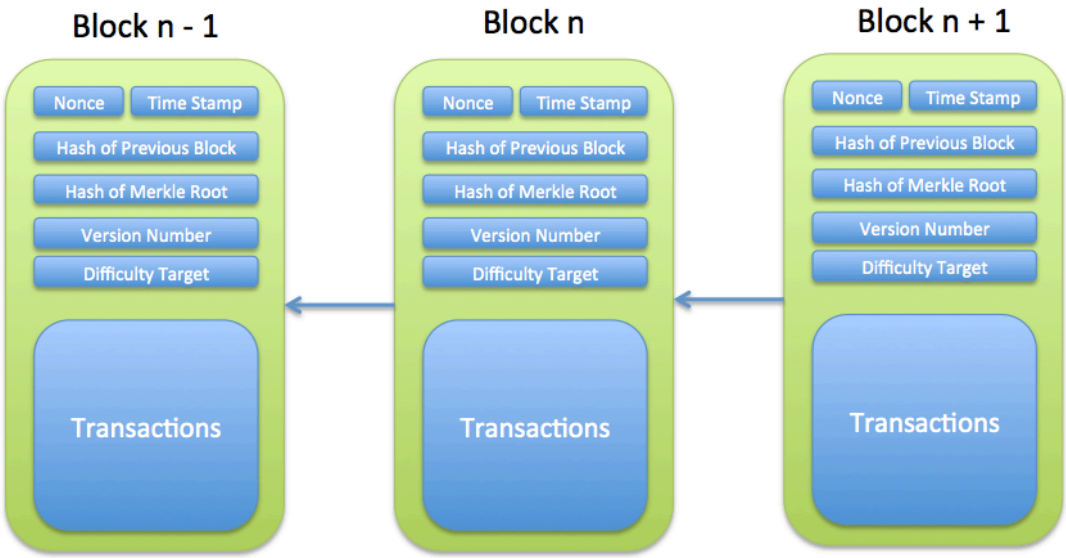
Let's take the Bitcoin block as an example. Each block contains a **header** followed by **transactions**.

The block header contains the following information[12]:

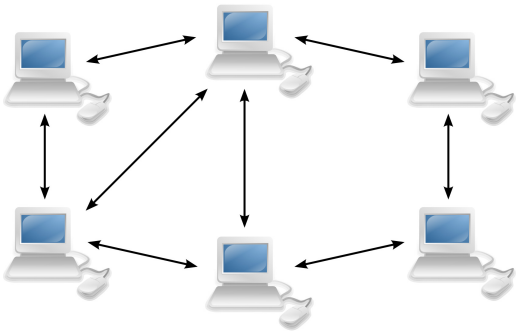
1) **Version number** to track the version of software used.
2) **Hash of the previous block**, effectively linking the current block to its predecessor, creating a linked-list structure. Note that the previous block's hash is used to calculate the current block's hash.
3) **Hash of the Merkle root** that records the transactions of this block. Note that this 256-bit hash is unique to the information and identity of the current block, and any change to the current block would cause the hash of the Merkle root to change. This acts as a "fingerprint" of the block and is generated using a cryptographic hash algorithm (e.g. SHA-256)[13].
4) **Timestamp** that records the time of the creation of this block.
5) **Difficulty target** of the proof-of-work algorithm, setting the number of zeros required at the beginning of the hash number.
6) **Nonce**, a 32-bit number calculated by miners for the proof-of-work algorithm to produce a hash that satisfies the difficulty target.

The transactions are the leaf nodes in a Merkle tree in each block. The Merkle tree architecture will be explained in detail later in this chapter.

A visualization of the structure of a blockchain is shown below. Each block contains the information listed above and is linked to the previous block.



The blockchain network is decentralized and authority-less[14]: it just requires a group of computers called **nodes** with high computing power owned by different people and organizations. The database is stored in those computers around the world, without a centralized "master copy." Decentralization helps prevent data corruption or attacks by hackers. The structure of the network is called "**peer-to-peer (P2P)**," demonstrated in the diagram[15] below:



When there's an update on the database (e.g. a new transaction occurred), this information gets spread in the manner of a *gossip protocol*[16]: the first node tells its neighbors, or other nodes in the

network that the first nodes has connection with (connections are illustrated by edges in the above diagram), and after receiving the news, the neighbors inform their respective neighbors, until all reachable nodes in the network are informed. The dissemination of information is extremely fast under the gossip protocol.

Since information is so transparent and easily accessible to the public, a common concern is security and fraud prevention. Blockchain accomplishes this by its **proof-of-work**[17] (or proof-of-stake, to be discussed later). The proof-of-work (PoW) adds value to the blockchain network by doing the following:

1) **Validate the transaction** by finding a nonce that makes the block header hash smaller than the difficulty target number. The nonce, which sits inside the block header, is a random whole number generated by the miner machine. A different nonce would cause the block header hash to change entirely. A miner tests many different values for the nonce until a nonce is found such that the new block header hash created has a lesser value than the difficulty target, or in other words, has *more zeros at the start* than the difficulty target. There is no known "shortcuts" to finding a satisfactory nonce: miners will have to find it via brute force, incrementing the value of nonce at each iteration until a good one is found. Because the nonce is 32-bit with additional extraNonce space allocated when the number overflows, there are more than 4 billion (2^32 = 4,294,967,296) possible nonces to test. Although miners with their high efficiency machines can test millions of nonces every second[18], finding a good nonce is still not a trivial task, which is why the process is called "proof-of-work": it would be extremely difficult to temper with a block, cause its hash and the hashes of all blocks after it to change, and find new nonces for it and every block after it! Once a nonce is found and the PoW problem is solved, the block is considered valid and added to the chain.

2) **Create more coins** as a reward for the miner who first successfully validates the block. This creates a competitive environment for miners around the world to race to be the first one who solves the PoW problem. To maintain a steady pace (~10 minutes for Bitcoin) of new blocks added to the chain and to control inflation caused by new reward created, the blockchain network determines a difficulty target such that the difficulty level of the PoW is directly proportional to the number of miners there are. In other words, the more miners working on validating the block, the harder the PoW problem.[19] Being the first to find a satisfactory nonce, therefore, is quite similar to winning the lottery!

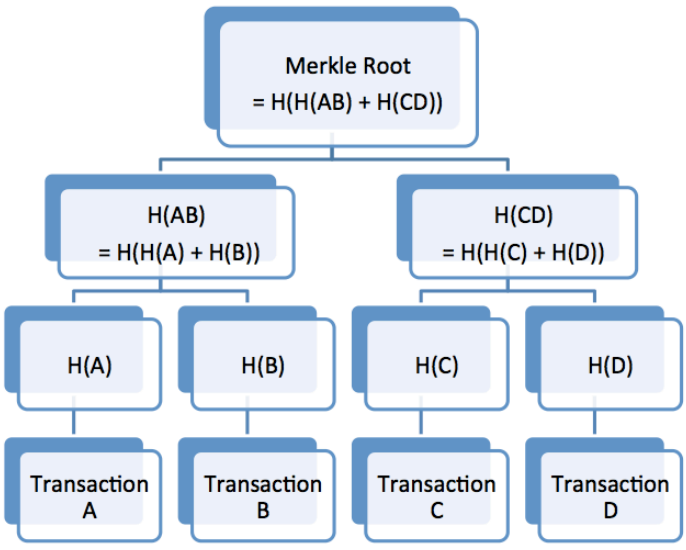
Because of its competitive nature, proof-of-work requires many miners to solve the same problem at the same time, creating redundant use of electricity and energy. To address the concern of energy and resource waste, the **proof-of-stake (PoS)** method is widely used by the world's second-largest cryptocurrency: Ethereum.

Different from proof-of-work, proof-of-stake assigns a block to *only one* node (called validator or forger) to validate, either randomly or based on the node's current wealth. For example, if a node currently owns 1% of the total coins on the market, then it'll be distributed 1% of the new blocks to validate.[20] This means that PoS validators have to own the cryptocurrency they are validating, in contrast to PoW miners who could potentially own none of the coins they are mining. Another difference between PoS and PoW is that PoS validators don't get awarded new coins, but instead they get paid a transaction fee from the original pool of coins.[21]

Once a transaction is logged into the ledger, how do we access it for later use? There are so many transactions happening every day, and the naïve way of verifying if a transaction actually happened would require each node to keep a copy of the entire database. Not only would this space requirement be

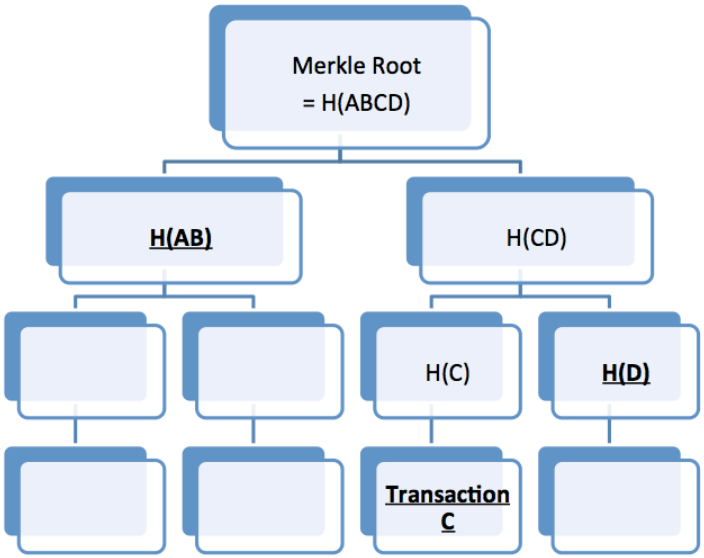
tremendously expensive and inefficient, the time required to verify a past transaction would be too long and non-scalable.

Merkle trees present a solution to the time and space efficiency problem. Merkle trees are binary trees with transactions as the leaf nodes. See the diagram below for a visual representation of the data structure. In this simplified example, there are four transactions stored in the block, Transactions A, B, C and D. A hash for each of the transactions is then created, with H() denoting the hash function. Then a new hash is created for each pair of the sibling hashes, which becomes their parent node. Repeat this process until the root is reached and the entire tree is built. An even number of transactions is preferred and required by the binary tree data structure, but in the case of an odd number of transactions, the latest transaction will be duplicated to create an even number of leaf nodes.[22]



Merkle trees provide a space-efficient way to verify the existence of a transaction in the current block. They enable **Simplified Payment Verification (SPV)**, a method that allows verification of transactions without downloading the entire block.[23] The following diagram illustrates the SPV process using the same example described previously. If a node needs to verify the

existence of Transaction C on this block, it only needs to download information for the siblings of the branch from the Merkle root to Transaction C. When the information required is obtained, we can compute H(C), H(CD), and eventually H(ABCD) using the specified hashing algorithm. The final step is to compare the computed H(ABCD) to the Merkle root hash stored in the block header. If they match, then Transaction C indeed exists on this block and is therefore verified. Together, the verification algorithm only needs to be given three elements, namely the transaction waiting to be verified, H(AB) and H(D), as highlighted in the diagram. This space efficiency of the algorithm enables light-clients[24], or nodes that don't need to store the entire chain.



*Underscored values are given. Rest are computed during the verification process.

Another benefit of Merkle trees is time efficiency. Because only one branch needs to be traversed, the transaction verification process takes *O(lg(n))*, with n referring to the number of nodes in the tree. This low computational complexity does not need a lot of memory and can save a lot of time and resources.

Last but not the least, despite the transparency of shared information on the blockchain network, each individual

participating node does not need to disclose its true identity. In fact, we know that each blockchain address is linked to a real participant, but we don't get to know who this participant is in real life.[25] This anonymity is designed to protect participants' privacy.

Banking

The banking industry is largely based on payments. Banks act as the intermediary, or agency, between two parties that don't necessarily trust each other entirely but are doing business with each other. As of the time this paper is written, bank transactions usually take days to process. This is because for a transaction to be processed, the bank needs to check for fraud, wire the sender's money to a clearinghouse, and then the clearinghouse sends the money to the receiving bank. Some suggest that banks have further slowed down their transaction process not only to avoid fraud, but also to use the extra time to invest your money for the bank's own benefit.[26]

Moving to blockchain from traditional banking could hugely speed up the transaction process, make it safer, and make our economy more efficient. With blockchain, banks can save on their fraud prevention expenses, and losses due to friction in the transferring process to the clearinghouse and then the receiving bank. Indeed, the need for clearinghouses and similar intermediaries will become obsolete as blockchain adoption becomes more prevalent. Santander, a Spanish bank, has estimated the cost saved by the blockchain technology to be 20 billion annually.[27]

Cryptocurrency, such as Bitcoin and Ethereum, presents a transparent, digital, and efficient solution to enable and ensure trust between two parties in a payment transaction. The definition of crytocurrency, according to Investopedia, is "a digital or virtual currency that uses cryptography for security."[28] Furthermore, cryptocurrency is "organic": "it is not issued by any

central authority, rendering it theoretically immune to government interference or manipulation."[29] Its organic feature makes central banks (i.e. the banks that make monetary policies including interest rates and money supply) unnecessary in a society that fully adopts cryptocurrency.

Cryptocurrency could be a threat to the traditional banking industry. It offers what banks offer nowadays, but with higher security and less manual work. With its secure blockchain infrastructure and fraud prevention features, Cryptocurrency could replace banks completely.

Another industry-transformative usage of blockchain is the **smart contract**. Smart contract, in its core, is a simple "if A then B" logic built into the blockchain code. With smart contracts, event B will be triggered after event A happens. This gives a chain of events coherent conditionals, which creates a lot of potential for payments. Banks can leverage smart contracts on loans and automatic payments. Ethereum is currently the biggest influencer that leverages smart contracts.[30]

To further illustrate how smart contracts work, let's take KYC as an example. KYC, or Know-Your-Customer, is a due diligence process that banks conduct to verify the identity of their customers, making sure they are not involved in illegal trades or criminal activities. KYC is currently an expensive, lengthy process in onboarding new clients involving lots of manual work, which results in high customer acquisition costs (CAC) and delay in opening new accounts. With smart contracts, banks can do customer background check more easily with the verified database in the blockchain network, and conditional logic could be coded such that bank accounts automatically open once the background check is approved. This reduces a lot of manual work and significantly shortens the processing time.[31]

As we can see, blockchain has the power of rendering some financial services such as clearinghouses obsolete. To avoid falling behind and having their jobs wiped eternally from the market, many incumbent banks have invested heavily in

blockchain startups and their own blockchain endeavors to stay up to date with the trend. Then as the time comes for a full transition to the blockchain, they will have a new business model fitted and more knowledge on the potential of the technology.[32]

Healthcare

Today, when we purchase a cabbage from the supermarket, we have no idea where it came from or the journey it took to get here, nor do we get information on how old it is. There's a risk associated with not knowing if it's from a clean source or transported by legit facilities; we have to put our health in others' hands by trusting the brand of the supermarket. Not only does this lack of traceability limit consumers' abilities to choose and indirectly affect their health, it also presents a risk for the seller unknowingly selling unqualified food and damaging their reputation. To address this concern, Walmart has started exploring blockchain solutions to trace its fresh produces.[33] Leveraging blockchain's immutability, records such as where a lettuce came from and each step in its transportation can be securely and permanently stored on the public digital ledger easily accessible by both the food providers and consumers.

The same traceability application of blockchain applied in the pharmaceutical industry can have an even larger impact on our health. A bad source of fresh produce may result in food poisoning and other minor diseases, but a bad source of drug would have imaginable consequences. The FDA has been fighting counterfeit drugs for a long time, and it is currently exploring the possibilities that the blockchain technology could bring to their effort.[34] Indeed, if drug retailers could have a trusted source of information on where the drugs came from, weeding out counterfeit drugs would be almost trivial. As a result, our society would better flourish with higher level of health and more importantly, higher level of trust and integrity.

The benefits that blockchain could bring to patients don't just stop at counterfeit drug elimination. In fact, in April 2018, five healthcare companies, namely Humana (NYSE: HUM), MultiPlan, Quest Diagnostics (NYSE: DGX) and UnitedHealth Group's (NYSE: UNH) Optum and UnitedHealthcare, have started looking into possibilities of building and maintaining a public healthcare provider directory backed by blockchain to ensure that the most up-to-date provider information is available for patients to view. As of today, different healthcare organizations and segments keep separate copies of provider information, and they are often out of date which causes differences to arise – it's like a distributed public ledger with no reliable way of synchronizing their copies of the same data! According to industry estimates, around $2.1 billion is spent on reconciling the differences and maintaining the public provider data. If this effort to move to blockchain technology indeed succeeds in the future, not only will patients benefit from more transparent, comprehensive, and up-to-date healthcare information to facilitate selection of providers, the $2.1 billion frictional cost could be saved because by definition, a public record backed by blockchain is synchronized, up-to-date, and shared by everyone in the network.[35]

On the other hand, blockchain could provide solution to integrating patient health records across different healthcare platforms. Having patient health records permanently stored and conveniently accessible reduces human error and contributes to a more comprehensive, friction-less healthcare system. It can also address the concern of patients forgetting about their medical history or any manipulation of it. One risk with handling sensitive, private data is malicious attacks to steal information. This risk is addressed by the blockchain's **privacy-by-design**[36], namely a trusted environment owned by no one, which allows users ultimate control over sharing their personal data.

Furthermore, the clinical trial process could largely benefit from blockchain. The privacy-by-design feature mentioned above can facilitate clinical trials and research by attracting more volunteers to participate. According to a recent poll, 80% of people are

willing to share their personal health information with researchers if the privacy of their data is ensured. Additionally, smart contracts can help chain a series of steps in the clinical trial and organize its workflow.[37]

According to a 2018 study, 60% of pharmaceutical companies are experimenting with blockchain. The industry sentiment on the future potential of blockchain lies 30% in medical supply chain, 25% in electronic medical records, 20% in clinical trials management, and 15% in scientific data sharing.[38]

Unlike the banking industry, the healthcare industry is not threatened by blockchain but rather tremendously benefited from it. There's a bright future ahead with lots of potentials to further integrate blockchain into the healthcare system. Moreover, the traceability of food and drug supply discussed in this section exemplifies blockchain's significant impact and future potential on **supply chain management (SCM)**, the management of flow in goods and services from raw material to final products.[39]

Charity

A large proportion of the population does not donate to charity not because they don't want to, but because they are not sure if the money will actually go to the places they wish. A 2015 poll finds that one third of Americans don't trust charities.[40] In addition, there is little to none emotional attachment to the money donated due to the lack of transparency in fund usage and little perception of impact.

Blockchain startup companies such as *Alice*[41] provide solutions to such gaps. Using blockchain, charity organizations can trace the entire journey of a fund from the moment it's donated to the moment it's used. The donor can clearly monitor where the money goes, which not only strengthens their trust on the charity organization but also cultivates their emotional attachment to their act of goodwill. The emotional attachment would likely

incentivize consistent, repeated donation behavior. Moreover, the value of impact is more easily calculated with blockchain as information is open and public. Blockchain can help charities build a feedback loop in this manner, and make their impact more transparent and tangible to the public. As a result, more people are incentivized to donate and regular donors are incentivized to donate more frequently.

Besides playing a role in tracking donations, blockchain can be utilized by charities for beneficiary registration and identification purposes. The United Nations World Food Programme (WTP), a philanthropic institution dedicated to providing food for the ones in need, is developing a biometrics-based blockchain technology that would register and identify Syrian refugees. The technology, if successfully developed, would allow refugees to purchase food with an iris scan of their eyes, an accurate and cutting-edge technology of biometric identity authentication, instead of with cash or card which can be easily lost or stolen. "Blockchain technology allows us to step up the fight against hunger," said WFP's Director of Innovation and Change Management, Robert Opp. Blockchain's ability to facilitate **digital identity management** has a huge future potential in philanthropy and beyond.[42]

Leveraging blockchain technology will help more charities and non-profit organizations gain trust from the public, and in turn help more people in need. An abundant future potential exists for the implementation of blockchain in the charity industry, and we are optimistic in the impact blockchain will have on making the world a better place.

Intellectual Property

Digitization of content and the Internet have made information sharing easier than ever. Though it brought many people convenience, it also violated others' copyrights when copies of

intellectual property are shared around illegally. Blockchain could protect copyrights with its support of value exchange.

Let's take music producers as an example. Right now, music producers are not getting a fair amount of pay for their music content because of pirate and torrent websites as well as intermediary streaming services such as Spotify and Apple Music that take a significant cut of the amount customers pay. The current music industry does not provide musicians with the channels or opportunities to acquire all the royalties they deserve.

Blockchain could play a role in protecting intellectual properties and facilitating **Digital Rights Management (DRM)**[43] in two aspects:

1) With its decentralized digital ledger infrastructure, blockchain can be used to record all information about the music content itself and its copyright. This information will be transparent and temper-proof to the public, making illegal infringement of copyrights virtually unfeasible. Blockchain can accomplish this task by its proof-of-existence44 service, which allows members in the network to anonymously upload information they own and receive a timestamped verification of their original work.[45]
2) Blockchain can eliminate intermediary music streaming services and allow music content producers to directly sell to consumers. The low transaction cost of blockchain will allow music producers to receive much more royalty payment than they currently do. Smart contracts can be used to facilitate licensing and recurring royalties by implementing a simple logic in the code such as: "if my music is played by party X, request payment of $Y from party X." Furthermore, the low transaction cost of cryptocurrencies enables micropayments typically to the eighth decimal place[46], making it possible for easy royalty payments.

Many other professionals such as online content producers can also benefit from blockchain the same way as musicians. Blog writers, for example, could get their content verified via proof-of-existence. They could leverage smart contracts to implement pay-per-view on their website via microtransactions. Further opportunities could be explored for other areas involving intellectual property.

Sharing Economy

Powered by the prevalent use of the Internet, our society is progressing into a sharing economy in which matchmaking platforms allow individuals to share their private assets and resources with each other for mutual value gain.

Uber in rideshare and AirBnB in home-share are two industry-leading examples of such matchmaking platforms. Uber allows a rider to put in requests for transportation services, and the platform automatically matches a driver to the rider. Likewise, Airbnb allows travelers to borrow rooms in private homes that homeowners are not using. Whether it's sharing a car or a house, matchmaking platforms allow idle resources to be utilized, creating value by expanding the resource pool and therefore increasing the efficiency of the economy. In exchange for providing and maintaining the matchmaking platforms, the middle agencies usually take a significant cut in each transaction: Uber takes 20-25% of the price for each ride[47], and Airbnb takes a cut of 3-15% of each overnight stay.[48]

The nature of a sharing economy requires peer-to-peer (P2P) interactions, when a match is made for individual A to lend something to individual B, in exchange for some value from B (usually in the form of monetary payment). This decentralized P2P activity model fits the model of the blockchain system perfectly, making it possible for blockchain to replace current matchmaking platforms.

As previously discussed, blockchain enables P2P value exchange in its network via secure cryptography. To accomplish the same rideshare service as Uber, for instance, drivers just need to put up their up-to-date information on the blockchain, and riders can select their rides based on the transparent information on the blockchain. The transaction will be made on the blockchain in its trusted environment directly from the rider to the driver, eliminating the need for a platform like Uber. This is extremely industry-disruptive as blockchain itself requires no transactional cost and only infrastructure cost, driving down the transaction fee drastically, making it much preferred than incumbent rideshare platforms that makes money from those transactions.

With its low transaction cost and high trust, blockchain will disrupt the current sharing platform industry by pushing sharing economy to a new height. Recently, a blockchain startup called Bee Token introduced *beenest*[49], a home-sharing platform that provides the same service as Airbnb *but does not charge any direct processing fee*. Instead, users could pay up to 2-3% of the transaction amount for insurance on the Ethereum blockchain—a huge decrease from the Airbnb commission. As the blockchain technology matures, a larger fraction of value transactions will be directly from peer to peer, and it will present a larger threat to incumbent platforms in the likes of Airbnb and Uber, reducing and eventually eliminating opportunities for those companies to take a cut in the middle of a transaction.

Real Estate

Blockchain can disturb the real estate industry and replace jobs currently done by humans. Take buying a house as an example. Today, if you want to purchase a house, you would need to go check out the house to find out all the information you need with a broker, and after you decide to buy it, you would need to go to a lawyer to process legal documents. You also need to pay for the house via a bank transfer or a check, which can take days to be approved. Insurance is another thing you have to take care

of. If you are applying for a mortgage, the process could take even take longer as the bank need time to approve your loan. Eventually the lawyer will put your information on public records stating this house belongs to you, and only now can you move in, possibly after weeks or even months from your initial decision to buy the house. This whole process is extremely convoluted, tedious, and hard to navigate for first timers.

With smart contracts on the blockchain, however, buying a house could only need as short as a few minutes. The house seller puts all required information up on the blockchain, which is verified by the community to be authentic, and the buyer after reviewing the information can seamless pay via crytocurrency, which automatically updates the public ledger and everybody now knows the new owner of the house. As a result, blockchain can serve as a "proof of ownership." [50]

The process of buying a house on blockchain is intuitive and easy to navigate. Not only will blockchain technology make the moment of purchase in house buying more efficient, it will also reduce siloed datasets and aggregate all house information into one transparent and easy-to-access database, providing buyers with more comprehensive information to make more optimal decisions.

On the flipside, a full adoption of blockchain in the real estate industry would completely eliminate the need for intermediary parties, namely lawyers, brokers, and banks. This would cause the number of available jobs to decline, resulting in layoffs of incumbent industry professionals, who would have to go back to school or look for jobs elsewhere.

Conclusion

This paper first explains the background and technical details of the blockchain technology, and then delves into the potential impact of blockchain in different industries and fields, namely

banking, healthcare, intellectual property, charity, sharing economy, and real estate. Blockchain's secure, decentralized infrastructure builds trust in a network and allows friction-free peer-to-peer transactions. In its core, blockchain offers safety, transparency, efficiency, and cost reduction in its abundance of applications in various industries. While blockchain's traceability will empower better supply chain management to capture more value in healthcare and charity industries, its built-in trust protocol will reduce job availabilities in intermediary service providers such as banks, rideshare, and real estate brokerage. It is expected that blockchain will cause a certain level of unemployment, but blockchain also could create more jobs in areas such as music and social media by creating new stable revenue streams for these professions. The future for blockchain remains mysterious, but our hopes are high.

Additional Thoughts

As Don Tapscott suggests in his TedTalk in 2016[51], the Intenet so far has been an information platform, where people send copies of information to each other, while still retaining that information themselves. The introduction and adoption of blockchain has started and will completely change the Internet into a value platform, where value such as money can be transferred from one to another. Transferring value is significantly different from transferring information because it's zero-sum: if A transfers value to B, then it's important that A doesn't have that value anymore. This goal is precisely accomplished by the blockchain technology with its smart infrastructure.

In December 2017, a New York-based beverage maker company previously known as *Long Island Iced Tea* declared that it was going to pivot toward the use of blockchain and changed its name to *Long Blockchain Corp*. The mere name change, without any substantial effort to shift to blockchain, boosted the company's stock by nearly 300%.[52] This incident gives further

insight into the optimistic public sentiment of blockchain and its highly expected potential.

In the past, many technological innovations had the power of changing the way we live. The Global Positioning System (GPS) navigation technology, for example, completely transformed the way we travel. Barely anyone today still reads a map and memorizes all the turns and highway exits before hitting the road. Smartphones not only made the internet accessible at anytime, but also made it almost impossible to lose contact with someone no matter where they are. It made mobile telephones not just a means of communication but an embodiment of lifestyle in which we read news and scroll through pictures, making traditional newspapers and magazines obsolete. Online search engines such as Google made public information accessible at our fingertips, greatly speeding up the process of research and dissemination of new information. They made the old way of conducting research unimaginable: reading through thousands of books in the library to find the right information for a topic. Rideshare apps such as Uber and Lyft made traditional taxis undesirable for their inefficient way of hailing and payment. The point I want to make is that we take many of these technologies for granted, accepting them as the only way to do certain things or accomplish certain objectives once they were released and gained traction. Those technological innovations had the power to permeate the human society in the fastest and most perfused way, and we can only imagine how much blockchain will transform our society.

References

[1] Tapscott, Don TapscottAlex. "The Impact of the Blockchain Goes Beyond Financial Services." Harvard Business Review. February 17, 2017. Accessed April 30, 2019. https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services.

[2] Kuhn, Steven. "Prisoner's Dilemma." Stanford Encyclopedia of Philosophy. April 02, 2019. Accessed April 30, 2019. https://plato.stanford.edu/entries/prisoner-dilemma/.

[3] "Banking Is Only The Beginning: 42 Big Industries Blockchain Could Transform." CB Insights Research. December 19, 2018. Accessed April 30, 2019. https://www.cbinsights.com/research/industries-disrupted-blockchain/.

[4] "Powering Communities and Opportunities." Steem. Accessed April 30, 2019. https://steem.com/.

[5]Music On The Blockchain - Middlesex University. (n.d.). Retrieved from https://www.mdx.ac.uk/__data/assets/pdf_file/0026/230696/Music-On-The-Blockchain.pdf

[6] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." https://bitcoin.org/bitcoin.pdf.

[7] Gupta, Vinay. "A Brief History of Blockchain." Harvard Business Review. April 05, 2017. Accessed April 30, 2019. https://hbr.org/2017/02/a-brief-history-of-blockchain.

[8] Marr, Bernard. "A Very Brief History Of Blockchain Technology Everyone Should Read." Forbes. March 20, 2018. Accessed April 30, 2019. https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#86f6e697bc47.

[9] Fortney, Luke. "Blockchain, Explained." Investopedia. March 12, 2019. Accessed April 30, 2019. https://www.investopedia.com/terms/b/blockchain.asp.

[10] Ethereum. "Ethereum/wiki." GitHub. Accessed April 30, 2019. https://github.com/ethereum/wiki/wiki/Ethash.

[11] Cosset, Damien. "Blockchain: What Is in a Block?" The Practical Dev. Accessed April 30, 2019. https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo.

[12] "What Is the Blockchain Data Structure?" CryptoTicker. November 25, 2018. Accessed April 30, 2019. https://cryptoticker.io/en/blockchain-data-structure/.

[13] https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture

[14] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." https://bitcoin.org/bitcoin.pdf.

[15] Cyberagents. "Peer-to-Peer Networks." Cyber Agents, Inc. September 14, 2018. Accessed April 30, 2019. http://www.cyberagentsinc.com/2018/09/14/peer-to-peer-networks/.

[16] Birman, Ken. "The Promise, and Limitations, of Gossip Protocols." http://www.cs.cornell.edu/Projects/Quicksilver/public_pdfs/2007PromiseAndLimitations.pdf.

[17] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress)*. doi:10.1109/bigdatacongress.2017.85

[18] "What Is a Nonce? A No-Nonsense Dive into Proof of Work." CoinCentral. December 18, 2018. Accessed April 30, 2019. https://coincentral.com/what-is-a-nonce-proof-of-work/.

[19] Mining?, What Is Bitcoin. "What Is Proof of Work." Everything You Need to Know about Bitcoin Mining. Accessed April 30, 2019. https://www.bitcoinmining.com/what-is-proof-of-work/.

[20] "Guide to PoS Mining: Everything You Need to Know About Staking." Coin Bureau. June 21, 2018. Accessed April 30, 2019. https://www.coinbureau.com/education/comprehensive-guide-pos-mining/.

[21] "Proof of Work vs Proof of Stake: Basic Mining Guide." Blockgeeks. Accessed April 30, 2019. https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/.

[22] Ray, Shaan, and Shaan Ray. "Merkle Trees." Hacker Noon. December 15, 2017. Accessed April 30, 2019. https://hackernoon.com/merkle-trees-181cb4bc30b4.

[23] Ibid.

[24] Andrew. "Blockchain Fundamentals #1: What Is a Merkle Tree?" Medium. February 26, 2018. Accessed April 30, 2019. https://medium.com/byzantine-studio/blockchain-fundamentals-what-is-a-merkle-tree-d44c529391d7.

[25] Sharma, Toshendra Kumar. "How Is Blockchain Verifiable by Public and Yet Anonymous?" Blockchain Council Blockchaincouncilorg. Accessed April 30, 2019. https://www.blockchain-council.org/blockchain/how-is-blockchain-verifiable-by-public-and-yet-anonymous/.

[26] "Why Do Bank Transfers And Deposits Take So Long?" Bible Money Matters. February 20, 2019. Accessed April 30, 2019.

https://www.biblemoneymatters.com/why-do-bank-transfers-and-deposits-take-so-long/.

[27] Perez, Yessi Bello, and Yessi Bello Perez. "Santander: Blockchain Tech Can Save Banks $20 Billion a Year." CoinDesk. July 05, 2015. Accessed April 30, 2019. https://www.coindesk.com/santander-blockchain-tech-can-save-banks-20-billion-a-year.

[28] Frankenfield, Jake. "Cryptocurrency." Investopedia. March 12, 2019. Accessed April 30, 2019. https://www.investopedia.com/terms/c/cryptocurrency.asp.

[29] Ibid.

[30] "What Are Smart Contracts? A Beginner's Guide to Smart Contracts." Blockgeeks. Accessed April 30, 2019. https://blockgeeks.com/guides/smart-contracts/.

[31] "Smart Contracts – From Ethereum to Potential Banking Use Cases." https://blockchainapac.fintecnet.com/uploads/2/4/3/8/24384857/smart_contracts.pdf.

[32] Holotiuk, Friedrich, et al. "Radicalness of Blockchain: an Assessment Based on Its Impact on the Payments Industry." *Technology Analysis & Strategic Management*, 2019, pp. 1–14., doi:10.1080/09537325.2019.1574341.

[33] Fingas, Jon. "Walmart Will Use Blockchain to Ensure the Safety of Leafy Greens." Engadget. September 25, 2018. Accessed April 30, 2019. https://www.engadget.com/2018/09/24/walmart-blockchain-leafy-green-tracking/.

[34] Fingas, Jon. "FDA Explores Using Blockchain to Track Drug Supplies." Engadget. February 22, 2019. Accessed April 30, 2019. https://www.engadget.com/2019/02/10/fda-pilot-may-use-blockchain-to-track-drug-supply/.

[35] "Humana, MultiPlan, Optum, Quest Diagnostics and UnitedHealthcare Launch Blockchain-Driven Effort to Tackle Care Provider Data Issues." Humana, MultiPlan, Optum, Quest Diagnostics and UnitedHealthcare Launch Blockchain-Driven Effort to Tackle Care Provider Data Issues | Business Wire. April 02, 2018. Accessed April 30, 2019. https://www.businesswire.com/news/home/20180402005181/en/Humana-MultiPlan-Optum-Quest-Diagnostics-UnitedHealthcare-Launch.

[36] Wirth, Christian, and Michael Kolain. "Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data." https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf.

[37] Mehdi Benchoufi, and Philippe Ravaud. "Blockchain Technology for Improving Clinical Research Quality." Trials. July 19, 2017. Accessed April 30, 2019. https://trialsjournal.biomedcentral.com/articles/10.1186/s13063-017-2035-z.

[38] Staines, Richard. "60% of Pharma Companies Using or Trying Blockchain - Survey." Pharmaphorum. October 01, 2018. Accessed April 30, 2019.

https://pharmaphorum.com/news/60-of-pharma-companies-using-or-trying-blockchain-survey/.

[39] Kenton, Will. "Supply Chain Management (SCM)." Investopedia. March 12, 2019. Accessed April 30, 2019. https://www.investopedia.com/terms/s/scm.asp.

[40] https://www.philanthropy.com/article/1-in-3-Americans-Lacks-Faith/233613

[41] "Blockchain for Good." Alice. Accessed April 30, 2019. https://alice.si/.

[42] "Blockchain Against Hunger: Harnessing Technology In Support Of Syrian Refugees." WFP. Accessed April 30, 2019. https://www.wfp.org/news/news-release/blockchain-against-hunger-harnessing-technology-support-syrian-refugees.

[43] Zhang, Z., & Zhao, L. (2018). A Design of Digital Rights Management Mechanism Based on Blockchain Technology. Lecture Notes in Computer Science Blockchain – ICBC 2018, 32-46. doi:10.1007/978-3-319-94478-4_3

[44] Ibid.

[45] "Proof of Existence - An Online Service to Prove the Existence of Documents." Proof of Existence - An Online Service to Prove the Existence of Documents. Accessed April 30, 2019. http://docs.proofofexistence.com/#/.

[46] Music On The Blockchain - Middlesex University. (n.d.). Retrieved from https://www.mdx.ac.uk/__data/assets/pdf_file/0026/230696/Music-On-The-Blockchain.pdf

[47] Press, Associated. "Uber Drivers Are Growing Angrier over Price Cuts." Business Insider. March 02, 2017. Accessed April 30, 2019. https://www.businessinsider.com/uber-drivers-are-growing-angrier-over-price-cuts-2017-3.

[48] Marte, Jonnelle. "Thinking of Renting out Your Home on Airbnb? Consider These Costs First." The Washington Post. July 27, 2015. Accessed April 30, 2019. https://www.washingtonpost.com/news/get-there/wp/2015/07/24/the-many-unseen-costs-of-renting-out-your-home-through-sites-like-airbnb/?noredirect=on&utm_term=.a6fe58630fa8.

[49] "Book Rentals and Homes for Your Business." Beenest. Accessed April 30, 2019. https://www.beenest.com/.

[50] Holotiuk, Friedrich, et al. "Radicalness of Blockchain: an Assessment Based on Its Impact on the Payments Industry." *Technology Analysis & Strategic Management*, 2019, pp. 1–14., doi:10.1080/09537325.2019.1574341.

[51] Tapscott, Don. TED. Accessed April 30, 2019. https://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business.

[52] Chengevelyn. "$24 Million Iced Tea Company Says It's Pivoting to the Blockchain, and Its Stock Jumps 200%." CNBC. December 26, 2017. Accessed April 30, 2019. https://www.cnbc.com/2017/12/21/long-island-iced-tea-micro-cap-adds-blockchain-to-name-and-stock-soars.html.