THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

DEPARTMENT OF FINANCE

ENTERPRISE USE CASES FOR SMART CONTRACT TECHNOLOGY ON BLOCKCHAIN NETWORKS

DANIEL Y. ZHANG
SPRING 2019

A thesis
submitted in partial fulfillment
of the requirements
for baccalaureate degrees
in Finance and Philosophy
with honors in Finance

Reviewed and approved* by the following:

Jingzhi Huang
Professor of Finance and Mathematics
David H. McKinley Professor of Business
Thesis Supervisor

Brian Davis
Associate Clinical Professor of Finance
Honors Adviser

* Signatures are on file in the Schreyer Honors College.

ABSTRACT

Blockchain is a technology that allows for the secure storage of information on an open, distributed system. It was formally introduced as an implementable technology by Satoshi Nakamoto in 2008 and has enjoyed surges in public visibility due to the popularity of its most famous application, Bitcoin. This thesis examines the history, theory, and characteristics of blockchain in order to understand why it has the potential to be used in the business world. This thesis will specifically focus on blockchain's synergy with smart contracts to facilitate asset transfers in financial services, healthcare, real estate, and fine art. After a discussion of potential technical and legal challenges and an analysis of existing business use cases, this paper will develop a cost benefit analysis to determine the financial feasibility of enterprise blockchain solutions. This thesis will conclude with recommendations for the development and direction of enterprise blockchain solutions in the future.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

I would like to thank Professor Huang for his help and direction through the process of writing this thesis. Additionally, I would like to thank Professor Davis for keeping my research on track and focused. I am extremely grateful for all the love and support that my family and friends have shown me during my time at Penn State. I especially want to thank my parents Xiaoyong Zhang and Anlan Dai for their unconditional support in my scholastic endeavors. Lastly, I would like to thank the Schreyer Honors College for providing me with the opportunities and resources to enjoy my college career to the fullest.

Chapter 1

Introduction

Blockchain was formally theorized by Satoshi Nakamoto in his 2008 paper “Bitcoin: a peer to peer electronic cash system”. It should be noted that Satoshi Nakamoto is a merely a pseudonym hiding the true identify of the individual(s) responsible for the research paper. Nakamoto claims that the most important feature of Bitcoin is that it is a medium for the exchange of goods and “allows payments to be sent directly from one party to another without going through a financial institution” (Nakamoto 2008, p. 1). He argues that traditional forms of payment through centralized financial institutions such as fractional reserve banks are inherently flawed because they require trust between unfamiliar buyers and sellers. The trust model of transactions leads to a certain threshold of unavoidable fraud and associated transaction costs, which may include proof of service/product, payment disputes, and product returns.

The primary concern for digital currency before the creation of Bitcoin was the issue of Byzantine Fault Tolerance, more colloquially referred to by the eponymous 1982 paper “The Byzantine Generals Problem”. The paper describes a scenario wherein individuals are working to establish consensus while acknowledging the possibility of a “traitor” (Lamport 1982, pp. 1-4). The implication for digital currency is that it requires a mechanism that ensures that individuals cannot spend the same unit of currency twice, an issue that is nonexistent for paper money transactions and is solved by traditional digital currency through the authority of a centralized financial institution.

Nakamoto solved the problem through the use of cryptographically secured transactions.

Each transaction is attached to one unit of storage known as a “block”. Specific blocks contain not only the information for the transaction that they are storing, but also information about the previous transactions in the chain. In order for blocks to be verified, they are checked by other nodes through the use of cryptography puzzles requiring intensive computing power. The distributed ledger will not update the chain with the newest transaction until every other participant (“node”) has also verified the transaction and are in consensus. While Nakamoto’s original intent was to create an information system which could support the digital exchange of monetary value, blockchain has become an exciting new technology with a variety of potential use cases outside of cryptocurrency.

This thesis will begin with an explanation of the technical language and history required to understand the various components of blockchain technology. These components are then leveraged to explain the essential features of blockchain technology (most notably smart contracts) that may be relevant to the broader business world. After this discussion, there will be an overview of the various risks and concerns associated with the technology. With the theoretical features of blockchain already discussed, the focus will move to an analysis of use cases in the business world today. This thesis will develop a specific cost benefit analysis generalized for the financial services industry and utilize the results of the cost benefit analysis in conjunction with the prior analysis of existing business use cases to make a suggestion as to where the future of enterprise blockchain systems may lie.

Chapter 2

Essential Features of Blockchain

Blockchain can best be described as a distributed database of information. It is not necessarily an entirely novel ideal, but rather a combination of several existing ideas and technologies. A “block”, the fundamental unit of information in a blockchain, contains information about the structure of the blockchain, a timestamp of when the block is posted to the chain, a reference to the previous block (the chain part of blockchain refers to the ability for individual blocks to reference previous and future blocks with metadata), and a list of transactions (or information storage) that are encrypted through a process called hashing.

The first characteristic of blockchain is that it is a Peer to Peer Network (P2P). In information science, P2P networks are created when two or more network nodes share information amongst one another without first sending information to a centralized entity. The P2P network can be considered “distributed” because all nodes have the ability to share and modify information individually. The following graphic from a paper on distributed computing explains the difference between a distributed and decentralized system: (Baran 1962, p. 2)

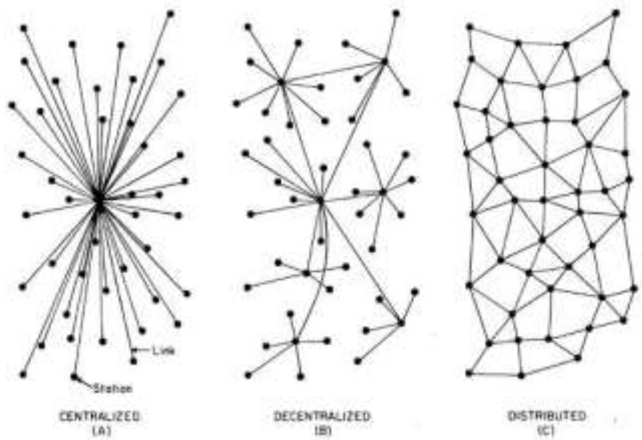

Figure 1. Baran's Model of Distributed Systems

Blockchain is frequently described as a “distributed ledger” because of its status as a distributed information system. In centralized and decentralized systems, information can is stored on a server and can be accessed after a client node makes a request that is approved by the server. In the P2P system nodes can function as both server and client, effectively allowing any node in the system to verify new transactions without the need for centralized third-party verification. The entire system will not verify the addition of new blocks unless all nodes have independently verified new transactions and are in consensus about the state of the system. This consensus is checked by consensus protocols, a set of rules coded into blockchain systems to prevent the same transaction from being posted on several blocks. The benefit of the P2P system is transparency and the risk mitigation of a single, centralized failure of the system. Because all nodes have access to an updated version of the system, past blocks are immutable and become permanent tamperproof records. Future blocks are not necessarily immune to tampering, but the risks of a 51% network attack can be mitigated and will be discussed at greater length in the chapter on risks and limitations.

Another of the core technologies contained within blockchain is cryptography. Cryptography refers to the dual processes of encryption and decryption. Encryption is the process whereby a fixed piece of raw data is run through a mathematical operation called a cipher to disguise the original contents of the data. Decryption is the reverse process, turning the disguised text into intelligible data once again. Blockchain technology utilizes asymmetric encryption (also called Public-Key Cryptography), simultaneously protecting the privacy of individual nodes and legitimizing transactions to the entire system. In asymmetric encryption, individual nodes are assigned both a public and private key. These keys are either number strings or hexadecimal strings that allow for transaction information to be both encrypted and decrypted. The public key allows other node participants to transfer information to a particular node, while the public key allows an individual to access the information at a node. Public keys and private keys are popularly compared to the username and password required to access an email account, respectively (Lisk Academy). The usage of public keys in combination with private keys produces a digital signature, effectively allowing other node participants to audit transactions and to identify which node participant is responsible for the posting of new transactions.

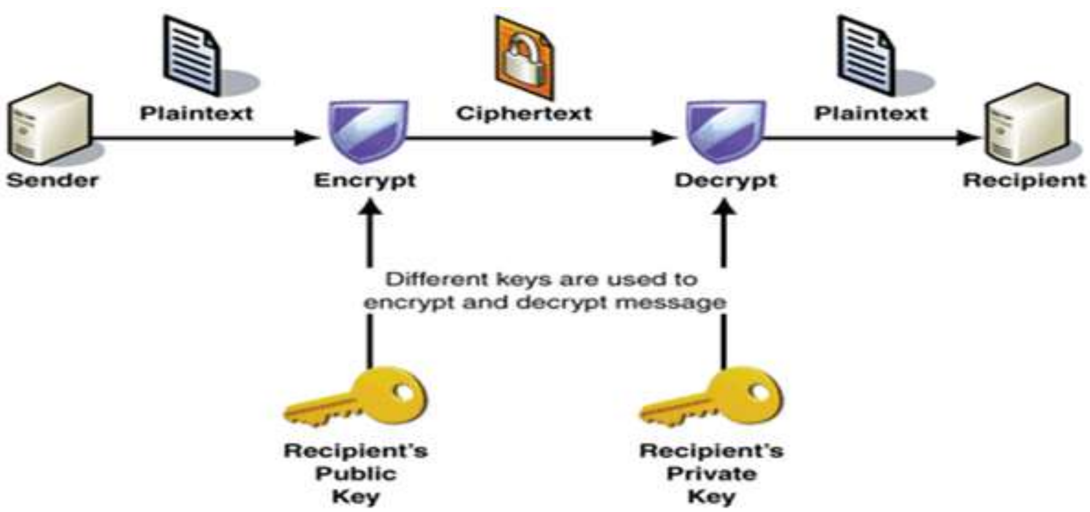

Figure 2. Encryption and Decryption, ICT Association

Most popular blockchain applications today use proof of work as the consensus protocol used to verify the blockchain to each individual node. After data for a number of transactions is encrypted by a key ("hashing"), any member of the node may "verify" the transactions by decrypting the hash through brute force decryption. Proof of work gives equal opportunity for any node to add new blocks to the chain but theoretically gives precedent to nodes with the greatest amount of computing power.

Blockchains can be classified as either public or private information systems depending on the protocol code used to create it. Public blockchains are have no barriers to entry and can be widely disseminated and viewed by any individual node. In contrast, private blockchains (sometimes referred to as permissioned blockchains) restrict access to only authorized individuals. This control is enforced either by protocol coded into the blockchain or by the presence of what are effectively "network administrators" who delegate node access to the blockchain. In the latter case, the so called "distributed" blockchain system actually becomes more like a decentralized system with select nodes serving as locally centralized control points (Lisk Academy). Enterprise blockchain applications will more likely than not feature private blockchains as they enhance security and control over the overall system.

Major Existing Blockchain Protocols

The two most popular examples of Blockchain Protocols today are Bitcoin and Ethereum. Both are examples of cryptocurrency, with Bitcoin being more publicly visible because of its relationship to Satoshi Nakamoto's whitepaper. Bitcoin operates as a medium for value exchange without the need for a singular centralized financial entity. Chuen and Dula claim that the ability to "be programmed to represent anything of value: a company share, tax or environmental credits, vouchers, cash, votes" is the distinguishing feature of blockchain that makes it viable as a medium of exchange. Blockchain is a public blockchain and uses the aforementioned asymmetric encryption, digital signature, hashing, P2P network, and proof of work technologies. Because Bitcoin utilizes a P2P network, transaction costs are relatively lower than if a third-party financial institution were processing payments. Independent nodes utilize proof of work to independently "mine" new blocks, simultaneously verifying old transactions and receiving new bitcoins as payment for processing power. In December 2017 one unit of Bitcoin was valued at close to $20,000.

Ethereum is another cryptocurrency application of blockchain created by Vitalik Buterin in 2013 (Wood 2014, p.1). Ethereum also utilizes the same technologies as Bitcoin but differs in its essential purpose and vision. Ether, the cryptocurrency that operates on the Ethereum platform, is exchanged as digital currency the same way Bitcoin is, but Ethereum also allows nodes to independently develop applications on the blockchain infrastructure. Ethereum Homestead claims that it is particularly "suited for applications that automate direct interaction between peers or facilitate coordinated group action across a network" (2016). Whereas Bitcoin is specifically intended to represent cash value, Ethereum can potentially be programmed to execute any kind of transaction, whether it be a physical or digital asset. Ethereum runs on the "Ethereum Virtual Machine" which allows the blockchain to behave like a computational machine that reads a variety of different programming language (Edchain, 2018). Ethereum as a platform is particularly suited for integrating smart contracts into the existing blockchain and should serve as a model for businesses seeking to utilize private blockchains for enterprise use.

Features of Smart Contracts

Smart contracts, contrary to common belief, are an independent technology not specifically suited only for integration into blockchains. They were first theorized by computer scientist Nick Szabo in the September 1997 edition of the First Monday Journal. He claims that "smart contracts reduce mental and computational transaction costs imposed by either principals, third parties, or their tools. The contractual phases of search, negotiation, commitment, performance, and adjudication constitute the realm of smart contracts" (Szabo 1997). In their very essence, smart contracts are self-executing computer protocols that outline the conditions for an event to be triggered and the consequence of the conditions being met. The theory behind the code is best understood by the logical operator of material conditionality, best expressed by → (implication, "if… then…"). Szabo provides the example of a vending machine to demonstrate a rudimentary conception of a smart contract. Once coins are inserted into the machine and a selection is made, the vending machine "processes" the conditions and provides the predetermined result of dispensing the food item.

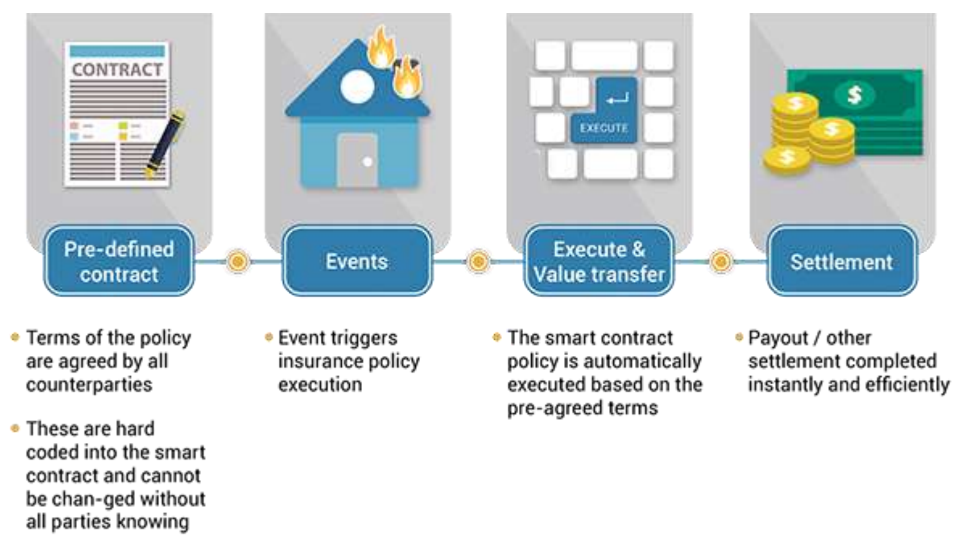

Figure 3. Smart Contracts, Coinbase

A more specific example of smart contracts is provided by Mills et al in the paper "Distributed Ledger Technology in Payments, Clearing, and Settlement" released by The Board of Governors of the Federal Reserve System.

> Smart contracts are coded programs that are used to automate pre-specified transactional events based on agreed upon contractual terms. Like with traditional contracts, a smart contract depends on participants' consent to its terms. These agreed-upon smart contracts can be used in conjunction with a distributed ledger to self-execute based on information received in the distributed ledger or from other sources. For example, several companies developing DLT products are exploring the use of smart contracts to model corporate debt issuances. In these simulations, a debt-issuing company specifies the parameters of the contract, such as its par value, tenor, and coupon payment structure. Once assigned to an owner, the smart contract would automatically make the required coupon payments until the bond reaches maturity (2016, pp. 14-15).

Smart contracts have immense potential when integrated within blockchain information systems for a variety of different industries. Mills identifies debt markets one particular industry that would benefit from adopting this new technology because the terms for payout are clearly defined as a specific set of conditions.

Chapter 3

Risks and Technological Limitations

The previous discussion on the technological features of blockchain and smart contracts have made it very evident why businesses would be interested in blockchain for enterprise use. Speculation and a bubble-like increase in the price of Bitcoin at the end of 2013 and 2017 (to a much greater degree) led to increased news coverage and public awareness of the Bitcoin platform. As a result, more individuals and businesses took it upon themselves to examine whether or not the technology could be modified as a cost-saving project or tamperproof security system. A 2015 survey conducted by the World Economic Form determined that over 55% of 800 information systems executives and experts anticipated over 10% of global GDP value being stored on various blockchain systems. This study highlights the optimistic view that blockchain has the ability to disrupt the business would in a way that can maybe only be surpassed by the development of the internet. The frenetic public coverage has died down considerably since 2017 and several key issues have emerged, all of which stand in the way of blockchain becoming a truly transformative tool in the world of business. The risks that businesses will have to consider in the near future are legality, scalability, energy cost, interoperability, and security risk.

Legal Issues

Blockchain in its essential spirit promotes transparency in such a way that might seem above regulation. The appeal of cryptocurrency platforms is that they promote a democratized version of value exchange. However, businesses cannot freely ignore law and regulation. As of 2019 there are 22 states that have either legally recognized or approved blockchain technology (National Conference of State Legislatures). The current issue integrating smart contracts into blockchains is that smart contracts are neither smart nor a contract; they are fixed lines of code integrated into a technical platform. Smart contracts lack both the cognitive process for dynamic change and formal recognition by state and federal governments. Arizona, Nebraska, New York, Ohio, Tennessee, and Vermont and Florida are the only states that recognize smart contracts as a legitimate, binding legal contract in 2019, but not all of those states have passed legislation formally acknowledging blockchain as a legitimate technology for business use.

The main issue that prevents blockchain and smart contracts from being broadly approved at both the state and federal level is the issue of liability. The self-driving car industry is facing a similar ethical dilemma; in an instance where a self-driving car is involved in an accident, who exactly is to blame? Is it the other driver, the company sponsoring the self-driving car, or even perhaps the programming team that designed the piloting system? Smart contracts have an enormous amount of practical application, but in the instances where an asset is improperly transferred due to coding issues, the issue of arbitration and conflict resolution becomes much more unclear. In order for blockchain to be properly utilized, both parties must agree to the purpose, intents, and conditions of smart contracts as well as entity with legal jurisdiction should the need for conflict resolution arise.

The transparency created by a distributed ledger also leads to a variety of privacy issues. Healthcare and financial services are two of the industries that that have the greatest capacity to integrate blockchain technology replacing existing information systems. However, these are also two of the industries that have the highest restrictions on how personal information from consumers can be viewed and used. The Federal Trade Commission protects consumer privacy in the financial services industry under the Financial Modernization Act of 1999 in the same way the US Department of Health enforces HIPAA regulations for medical patients. There are no doubt countless other industry examples where having an entirely open book of information would be a disadvantage rather than an advantage. Because all of the information on a distributed ledger is open and immutable, many of these personal files may violate privacy laws. This risk can be partially mitigated by utilizing private permissioned blockchains, effectively restricting access to personal information to only relevant personnel. An added level of complexity arises when considering the cases where Blockchain as a Service (BaaS) come into play. Not all companies will want to hire developers to privately design an enterprise blockchain and many may prefer that one or several BaaS companies develop widely adaptable blockchain systems to save on upfront capital costs. BaaS companies must also be sure to adhere to proper privacy regulation just like their clients and may have to create clear legal boundaries for access to client information to clear some of the ambiguity involving distributed ledgers and private information.

Scalability Issues

The scalability of any information system refers to the ability to continue operating efficiently as the amount of information increases. After a new transaction is posted on a block, every participant in the distributed ledger must independently identify and verify the new transactions. As a result, the cryptography systems that support blockchains become increasingly complex and require exponentially increasing amounts of computing power as new blocks are added to the existing chain.

In order for blockchain to impact the core business in an industry like financial services, there must be drastic improvements in performance at scale. Danezis and Meiklejohn state that "Despite their success, existing cryptocurrencies suffer from a number of limitations. Arguably the most troubling one is their poor scalability: The Bitcoin network (currently by far the most heavily used) can handle at most 7 transactions per second and faces significant challenges in raising this rate much higher, whereas PayPal handles over 100 and Visa handles on average anywhere from 2,000 to 7,000" (2015, p.1). Cryptography puzzles, which allow for verification and security within blockchain systems, also happen to limit scalability because the puzzles become increasingly complex as more transactions are added to the chain The Bitcoin platform requires approximately 10 minutes to verify a transaction while the Ethereum platform requires roughly 15 seconds. Ethereum has the benefit of having an uncapped block size (compared to a capped 1 Megabyte block size for Bitcoin) which allows for a greater number of transactions to be recorded on a singular block.

The most promising solution for blockchain's scalability issues is the Lightning Network. The Lightning Network is a secondary information system that operates behind a blockchain system to reduce the final number of posted transactions (Coin Telegraph, "Bitcoin Energy Consumption Index"). It works in pretty much the same way a customer can open up a tab at a bar; orders are continuously posted on the customer's account, but only the final closed tab is handed to the customer as a receipt. On the Lightning Network, two network participants can open up a payment channel that is continuously updated until the channel is closed. After closure, the net balance of the transaction is posted as a singular transaction on the blockchain.

This is an attractive solution for the business world because many companies frequently engage the same parties for transactions. Depending on the complexity of the transaction or the need to record and timestamp essential transactions on the blockchain, the Lightning Network can be updated on a daily or monthly basis to increase the speed of transaction processing. An example of how the Lightning Network may operate is the Plasma protocol, an application on the Ethereum platform that is based on the same principle of storing extraneous transactions on a secondary information system.

Other solutions for the issue of blockchain scalability aim to overcome the technological barriers that limit processing speed by directly changing the characteristics of the blockchain. One breakthrough solution is Zilliqa, a prototype blockchain developed by researchers at the National University of Singapore. Zilliqa utilizes a technique called sharding which “partitions transaction block verification to machines in a network by running parallel subcommittees (shards) that process and then collate the verified data into a final block” (Blockchain News). Preliminary tests have shown that Zilliqa can process between 1400 to 2800 transactions per second, which is much closer to the processing speed required for large scale implementation.

Energy Issues

An issue that is closely tied to scalability is blockchain’s enormous dependence on computing power and, consequently, dependence on electricity. Cocco et al. states that “the Bitcoin system, as every system using [Proof of Work], an ecologically unfriendly consensus mechanism, incurs high electricity and hardware expenses in order to increase the probability of mining bitcoins by buying hardware more and more powerful” (2017, pp. 25-26). The security of blockchain provided by complex cryptographic hashing systems also hinders cost effectiveness as the amount of information increases in the data system. An estimate by Digiconomist concluded that the worldwide electricity required to power Bitcoin totaled 50 Terawatts on an annualized basis, a figure that is approximately the annual electricity produced by Singapore. Based on a 2016 Corporate Sustainability Report, Visa as a company processed 111.2 billion transactions while consuming approximately 674 Gigajoules of energy (joules/second is converted to watts on a 1:1 basis). For comparison, the energy required to power 1 bitcoin transaction is displayed next to the energy output required to power 100,000 Visa Transactions:

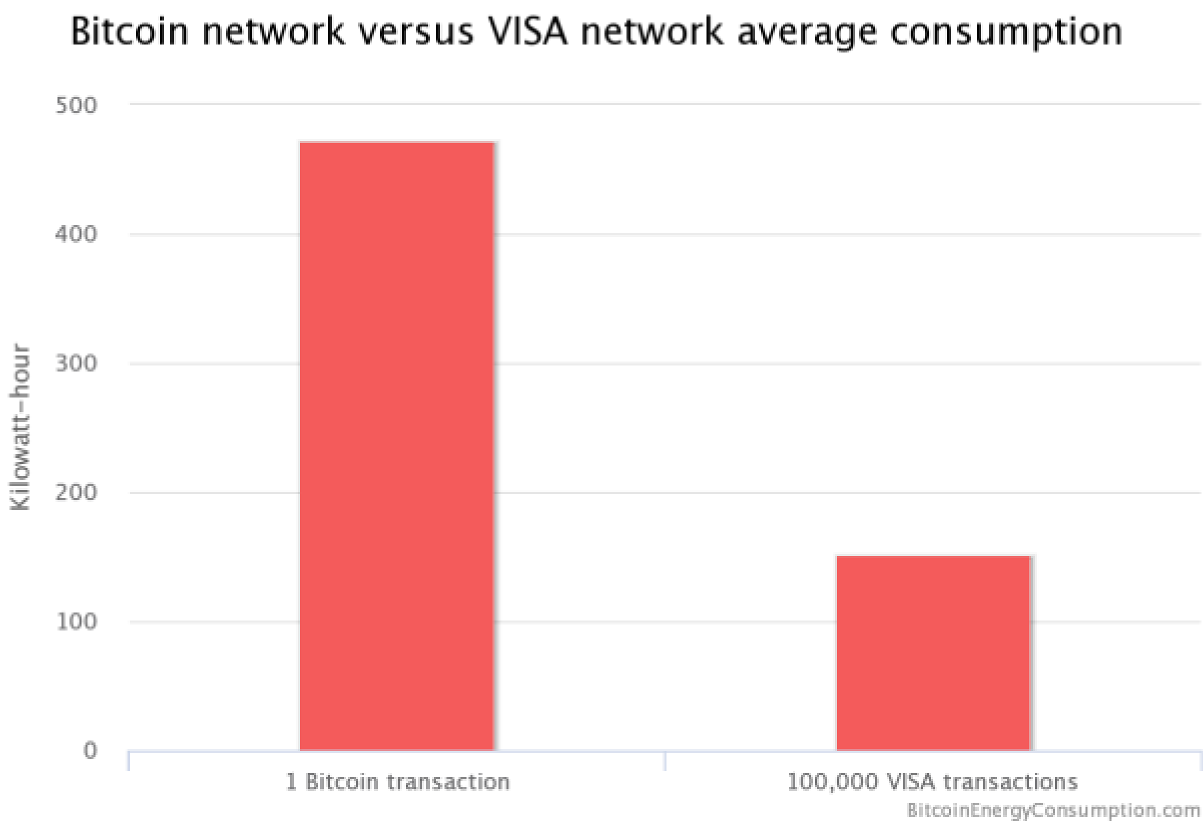

Figure 4. Bitcoin vs Visa Power Consumption, Digiconomist

While it may not be entirely appropriate to compare Visa transactions to Bitcoin transactions due to scale, this graph gives a clear visualization as to the staggering amount of energy costs required to power blockchain systems. One potential solution for excessive energy usage is to switch from a proof of work consensus protocol to a proof of stake consensus protocol. As previously described, proof of work is essentially a like brute force solving a password by trying all possible solutions and requires an enormous amount of computing power to decrypt previous transactions. This requires excess energy that will not actually contribute to the final chain. Proof of stake is nonrandom and delegates block creation to specific nodes based on past contribution to the chain rather than computer power. While many blockchains currently utilize proof of work because it is democratic and fair for public blockchains, businesses may strongly consider proof of stake to create more cost effective blockchain systems. One of the primary reasons that businesses would want to invest in enterprise blockchain solutions is as cost-saving project; if blockchain technology cannot reduce operational costs associated with electricity, project managers will be extremely hesitant to switch to a less cost-effective data system in the name of security and transparency.

Interoperability Issues

The prevailing sentiment among blockchain enthusiasts from 2013-2017 was that eventually there would be one optimized blockchain that would dominate usage and application. However, the years since that time have seen numerous independent blockchains being development and it would be fair to say that the world is moving away from the vision of a singular unified blockchain. As a result, interoperability has become an important issue for businesses seeking to utilize blockchain. Interoperability refers to the ability of two systems to exchange information and operational protocol. While it may not be an issue for businesses that solely rely on private permissioned blockchains for information storage, any business that anticipates a B2B relationship utilizing blockchain must consider the problem of interoperability. For example, if two financial firms were to agree on the terms of a large loan on a blockchain system, it is possible that the individual blockchain systems will not be able to exchange information. Vitalik Buterin, the founder of Ethereum, has suggested 3 solutions for this issue in a paper titled “Chain Interoperability” (2016, p. 25):

1. Centralized or multi-signature notary schemes: “Where a party or a group of parties agree to carry out an action on chain B when some event takes place”
2. Sidechains/relays: “Systems inside of one blockchain that can validate and read events and/or state in other blockchains”
3. Hash-locking: “Setting up operations on chain A and chain B that have trigger, usually the revelation of the preimage of a particular hash”

The advantages of overcoming the issue of interoperability are obvious within the context of the business world. Any asset or piece of information could be tokenized, divided, and transferred to a foreign blockchain owned by another company. Buterin himself suggests that one potential application of having two discrete blockchains cooperate is storing asset A on blockchain X and having dividends paid to asset owners on Blockchain Y though information sharing.

Security Issues

Satoshi Nakamoto's paper on Bitcoin points out that there is one obvious way to undermine a blockchain, namely a 51% attack. If an individual or group of individuals is able to control over 50% of the total hashrate (total mining/computing power), they would be able to both prevent new transactions and alter the information stored on new blocks. It is unrealistic for a platform like Bitcoin to experience a 51% attack because of the number of node participants makes gaining a majority nearly impossible. Private blockchains are more secure because the validators of new blocks are restricted to specific individuals, but this still leaves the possibility of one rogue employee ruining an entire information system because of the smaller (by comparison to a larger public cryptocurrency) size of the network. Enterprise blockchains are particularly susceptible to a 51% attack because they are likely to be permissioned blockchains; a smaller number of verified users on the blockchain naturally implies less nodes on the system and results in a greater probability that one particular individual will be able to control the majority of nodes. The following graphic illustrates how 51% attacks may occur on a blockchain system.

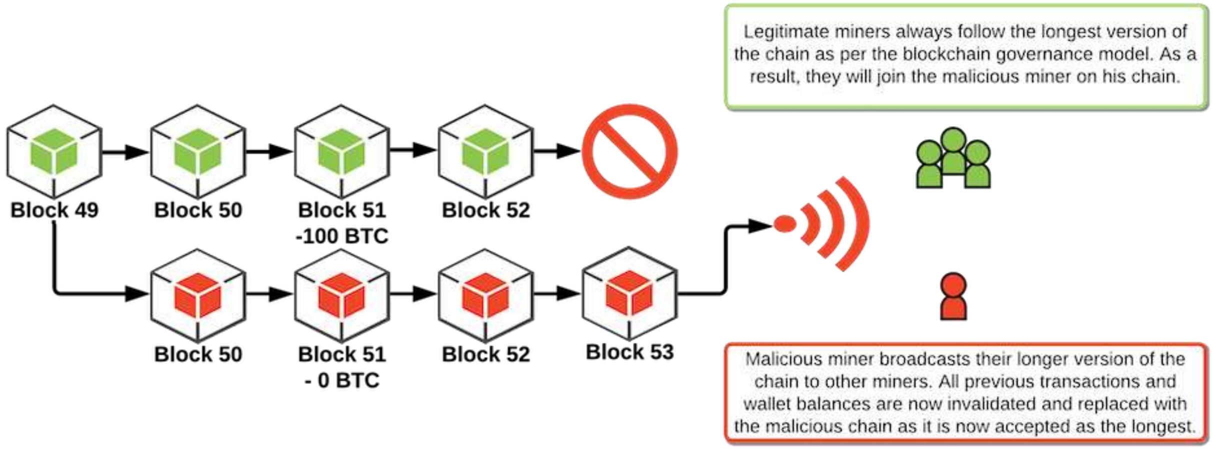

Figure 5. 51% Attack on Blockchain, CoinExchange

While the immutability of blockchains is considered an advantage due to increased transparency, it also can lead to potential issues. One of the key draws of blockchain is the ability to eliminate third party intermediators between transactions; however, these third-party entities also serve the purpose of auditing the veracity of transactions. Blockchain systems supporting physical asset transfers may suffer less, but digital blockchains being used purely for information storage requires an incredibly low threshold for error because data is stored permanently and visible to all members on the network.

Additionally, private enterprise blockchains may have coding issues or may be particularly susceptible to abuse from a single permissioned employee. A 2016 project called the DAO (Decentralized Autonomous Organization) raised $150 Million from over 11,000 investors (Coindesk, "Understanding the DAO Attack"). The organization was effectively a self-governed investment fund that operated through smart contracts written by investors. The investors were not buying equity shares, but rather voting rights on how the smart contracts should be structured. However, on June 17th, 2016 an anonymous hacker was able to subvert a poorly written recursion code and deposit 3.6 million Ethereum into a private account, valued at roughly $70 million at the time of the theft. In February of 2019, the founder of a cryptocurrency exchange called QuadrigaCX reported travelled to an Indian hospital and died from complications from Crohn’s disease (Futurism). While not explicitly confirmed, many blockchain enthusiasts claimed that QuadrigaCX CEO Gerald Cotton had personally transferred over $150 million into private wallets and procured a fake death license from a notoriously corrupt hospital. These two incidents showcase the need for employee education and additional security precautions should businesses choose to store valuable information or exchange assets through a blockchain medium.

Chapter 4

Existing Use Cases and Implications for Business

Blockchain is ideally suited for transactions with multiple business partners and has the capability to integrate smart contracts to automate and accelerate transaction contracts. The following chapter will review some of the companies that have already made efforts to integrate smart contracts and blockchain into their business in order to draw conclusions on where the future of enterprise blockchain development may lie.

Industrial and Commercial Bank of China

The Industrial and Commercial Bank of China (ICBC) is one of the largest banks in the world as well as one of China's four state-owned banks. In 2018, the ICBC filed a patent with China's national IP office for a blockchain system that allows consumers to save personal information on blockchain while using personal banking services (Coinbase, "ICBC Patent"). After any given individual has their personal information verified by the bank and stored on the blockchain, the ICBC can use these credentials to fulfill smart contract conditions stored on the blockchain. If there is a specific banking service or outside entity that requires reauthentication, the smart contract will automatically process existing user information and provide service to the customer. This patent automates the process of repetitive documentation and should help to reduce instances of fraud.

Agricultural Bank of China

The Agricultural Bank of China (ABC) is another one of China's state-owned banks. The ABC issued a $300,000 loan on a private blockchain system (Coinbase, "Land-Backed Loans"). The loan was collateralized by agricultural land, but the ABC is continuing to develop blockchain systems that will allow them to utilize smart contracts to offer small unsecured loans to small farms, effectively establishing a niche microcredit edge.

Fizzy by AXA

Fizzy is a parametric insurance product developed by French insurance company AXA that launched in 2017 focusing on the airline industry. Insurance for individual flights is dynamically priced and recorded onto a public blockchain application managed by AXA on the Ethereum platform (Fizzy FAQ). In the case that a flight is delayed more than two hours, Ethereum smart contracts will automatically execute and reimburse the purchaser for the full ticket amount. Fizzy is a highly specific type of insurance and does not protect against cancellations.

Propy

Propy is a San Francisco based real estate company that made headlines in 2017 when it engineered the sale of a $60,000 apartment in Ukraine using smart contracts (New Scientist). Like Fizzy by AXA, the purchase was executed using the Ethereum platform to execute the terms of a smart contract. Once the purchaser supplied proper identification and Ether cryptocurrency equivalent to $60,000, the property deed was automatically transferred to the buyer. Blockchain technology may help to document and automate domestic and international real estate transfers in the future, but not all countries allow smart contracts to be used in the case of a real estate sale.

Slock.It (Share&Charge)

Slock.It is a small BaaS company that supporting the enforceability of smart contracts involving physical assets. Share&Charge is an electricity renting company that operates using Slock.It blockchain. Owners of electric vehicles can rent out their specialized charging stations by enrolling in the Share&Charge network (effectively AirBnB for charging stations). After a customer pays for the use of a charging station, it is recorded onto a public blockchain and triggers a smart contract notifying the station owner of payment. Prices are dynamically priced and both customer and owner can view the market rate before agreeing to the smart contract.

IBM Blockchain

IBM released its proprietary BaaS service in 2017. Its announced clients include Bank of Tokyo, Northern Trust, China Construction Bank, and Walmart. (Forbes, "The 10 Largest Companies In the World Are Now Exploring Blockchain") The system was priced at 4 nodes for enterprise use at $10,000 per month in 2017. IBM claimed in the public statement announcing the service that its BaaS system was capable of supporting up to 1000 transactions per second at peak efficiency.

Enterprise Blockchain Trends

In general, smart contracts are most useful in industries where business to business ("B2B") and business to customer ("B2C") relationships are defined by a definite, quantified exchange of value. As expected, the Financial Services industry has many different companies using smart contracts to achieve a variety of goals. It can be reasonably inferred that industries that depend on service relationships like tourism, entertainment, and restaurants struggle to tokenize intangible products like quality of service and will benefit less from smart contract integration.

Despite household names like IBM and several of the largest banks in the world dabbling in blockchain, one potential question mark for blockchain's future potential is the fact that very few large companies are looking for ways to integrate smart contracts into their core business rather than smaller side business. The Chinese banks mentioned are working on auxiliary services like personal identification and microfinance loans rather than working on integrating blockchain systems into core transaction processing for banking services. In addition to the listed cases, there have been no instances of a company on the scale of Visa or Paypal announcing an initiative to transform their mainframe data processing with blockchain. The rationale is most likely that the aforementioned cost and transaction speed issues are hindering the adoption of blockchain systems at scale and that companies are more comfortable developing granular, targeted business solutions.

One surprising finding is that companies may choose to partner with a BaaS provider instead of developing a private blockchain or developing custom applications on a public blockchain like Ethereum. In the future, we could see more BaaS providers building applications on public blockchains like Ethereum rather than building customized private blockchains.

Businesses that utilize BaaS negate the need for upfront capital investment and human capital/programming expertise while making the tradeoff for control over blockchain customizability. An unexpected benefit that could arise from widespread BaaS adoption is that interoperability would be much less of a problem in a B2B setting if many companies flock to an established provider like IBM.

Implication for Selected Industries

Based on the trends found in existing blockchain use cases that utilize smart contract technology, I have identified four applications in various industries that have the potential for blockchain applications to be developed for enterprise use. Potential impact is ranked from a 1-5 scale, where 1 represents low/negligible effect and 5 represents the potential for transformational change in the core business. Probability of development and adoption is also ranked on a 1-5 scale with 1 representing low/negligible chance of development and 5 representing widespread application and adoption.

Table 1. Feasability of Smart Contracts and Blockchain for Select Industries

Industry	Application	Potential Impact	Probability of Development/Widespread Adoption
Utilities	Resource allocation, Peer to Peer trading	4	4

Art Market	Transfer of asset ownership	3	2
Healthcare	Data management & reduction of intermediaries	5	3
Real Estate	Transfer of asset ownership, Renting	4	4

Utilities

The most obvious application of blockchain and smart contracts in the utilities industry is within the B2C relationship; utility companies can design smart contracts to only provide service to a consumer when payment has been transferred. Additionally, utilities companies can design smart contracts for the buying and selling of power from power producers, eliminating intermediaries and dynamically adjusting the amount paid when demand for energy varies from normal consumption. In the same spirit, individual consumers can enter into smart contracts to buy and sell energy in order to more efficiently allocate resources. Like the financial services industry, the main roadblock for utilities companies is that utilizing blockchain would fundamentally alter payment structure and scalability remains a large issue. For now, companies should focus on a granular project like allowing individual consumers to exchange energy on a peer to peer basis.

Art Market

At first glance, the art market might be not be the first industry that comes to mind for blockchain implementation. However, fraud and forgeries will always be a concern for the art market and established art authorities have the potential to keep ownership records on blockchain. Additionally, smart contracts have the potential to facilitate transactions, although they would be much more effective for digital pieces like photographs. Art pieces can range into the hundreds of millions USD on the higher side, so there is some justification for tokenizing the sale of physical pieces and breaking ownership into pieces to allow for partial ownership or group buyers. Christie's, a famous art auction house, sold a piece by Barney Ebsworth for $318 million on blockchain in 2018 through a partnership with art blockchain company Artory (Forbes, "How Blockchain Changed The Art World In 2018"). However, it was likely done as a publicity stunt and the bottom line is that there is potential for blockchain, there is probably not enough of an efficiency incentive to justify widespread development.

Healthcare

Healthcare is one of the industries that has the most to gain in terms of cost reduction when integrating blockchain and smart contracts. As the current system holds, the relationship between pharmaceutical companies and individual consumers is separated by several levels of middlemen that might include insurance companies, health providers, doctors influenced by corporate drug salesmen, pharmacies, etc. Each layer of complexity introduces new costs to the end consumer, making the process extremely inefficient. In an ideal world, pharmaceutical companies would engage only with insurance companies and consumers to optimize drug pricing by using smart contracts. However, there are a vast number of players in the healthcare sphere and interoperability would be an enormous issue. In addition, drug pricing is horribly inconsistent to both hospitals and individuals and it is unclear whether smart contracts can fix this issue, especially since they require specific fixed instructions. Insurance companies and healthcare providers such as doctors and hospitals should consider looking at smaller scale projects to store patient information on blockchains before setting out on the more ambitious goal of revolutionizing the way drugs are paid for.

Real Estate

The example case from Propy clearly illustrates the fact that smart contracts can viably be used to transfer ownership of a real estate property. The main benefit of using blockchain would be to reduce the inefficient paper trail that a normal transaction would require. Combining blockchain and smart contract technologies allows for ease of mind for both buyer and seller because it reduces the possibility of fraud and transfers the property deed upon verified payment. The main barrier for the real estate industry is whether or not smart contracts will be recognized as a legitimate contract in a property sale. An alternative usage of smart contracts that real estate companies might want to consider is processing rent payments through blockchain to create an accurate timestamped record of payments. The ability to automate the collection of rent payments is somewhat less revolutionary than paying for an entire property through blockchain but nonetheless it provides a certain level of convenience and recordkeeping for the tenant.

Chapter 5

Cost Benefit Analysis

The primary purpose of a cost benefit analysis is to help businesses or individuals analyze the financial feasibility of a particular decision. The theory behind a cost benefit analysis is relatively similar to a net present value analysis. For a given time horizon, annual costs and benefits are added together to generate a net benefit value for every applicable year. These net benefit values are then discounted to the present to determine whether the present value of the future benefits is less than, equal to, or more than 0. For instances where the present value of future benefits is equal to a value other than 0, IRR can be used to determine the appropriate discount rate that would force the model to return 0 as the resulting benefit.

The model company for the following cost benefit analyses will be Visa. Visa is an appropriate company to use because it represents the kind of financial services company with the greatest amount of theoretical benefits from blockchain due to the large number of credit card transactions processed. As previously discussed in chapter 3, Visa processes about 111.2 billion transactions while consuming 674 Gigajoules of energy on an annualized basis. The primary implicit benefit of utilizing a blockchain system is the realized electricity savings from no longer using their existing transaction processing system. The following chart shows the calculations for annual benefits on a new blockchain system.

Transaction Costs	
VISA	
Average Cost of Electricity in the US ($/kilowatt hours)	$ 0.12
Conversion into ($/Gigajoules)	$ 33.00
674 Gigajoules per year	$ 22,242.00
111.2 Billion Transactions	111,200,000,000
Ethereum	
Implied Electricity/Transaction (kWh)	43.00
Yearly Implied Total Electricity Usage (kW)	4,781,600,000,000
Yearly Electricity Usage	$ 573,792,000,000

Figure 6. Transaction Cost Calculations

The average cost of electricity is provided by an NPR article examining data from the Energy Information Administration. One major assumption contained in the model is that Visa consumes electricity on a smoothly distributed state to state basis. Most states range from 8-16 cents per kilowatt hours, with the notable exceptions of New York (18 cents) and Hawaii (33 cents). With electricity cost established, $/kilowatt hours is converted into ($/Gigajoules using a conversion factor of approximately 277, yielding $33 per gigajoule. This ratio is multiplied by Visa's 674 Gigajoules of annualized energy usage to yield $22242 in annual electricity costs. This amount is used as the implied energy savings from switching to a blockchain system in the following cost benefit analyses.

If benefits are to be modelled using electricity costs, then it would make sense to also model the costs by looking at the financial feasibility of maintaining a blockchain system using electricity. However, the following calculations using Ethereum as a base show why this analysis would fail. Major public blockchains more often than not operate on a proof of work consensus protocol and generate an enormous amount of extraneous electricity. Digiconomist estimates that the implied electricity per transaction is 43-kilowatt hours ("Ethereum Energy Consumption Index"). When this figure is multiplied by Visa's annual number of transactions multiplied by .12 cents per kilowatt hours, the resulting cost is a staggering 573 billion dollars. It can be reasonably inferred from this analysis that if businesses are to create large scale blockchain system, they would most likely have to utilize proof of stake consensus protocol alongside a private, permissioned blockchain to control the scalability of energy costs.

As an alternative to using electricity costs, the following cost benefit analyses instead use quotes from IBM’s enterprise BaaS service to model cost. As discussed in Chapter 4, IBM was charging $10000 per month in their 2017 launch, but more recent quotes locate the monthly amount to $1000. Assuming that IBM’s BaaS can support the 2000 transactions per second as required by Visa, the annualized cost of $12000 is used as an input in the cost benefit analyses.

Cost Benefit Analysis							
Enterprise Blockchain System							
Year	Benefit	Development Cost	Maintenance Cost	Net Benefit	Discount Factor	Discounted Benefit	Discount Rate
0		$ (200,000.00)	$ -	$ (200,000.00)	1	$ (200,000.00)	7.25%
1	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.932400932	$ 9,549.65	
2	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.869371499	$ 8,904.10	
3	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.810602796	$ 8,302.19	
4	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.755806803	$ 7,740.97	
5	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.704714968	$ 7,217.69	
6	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.657076893	$ 6,729.78	
7	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.612659108	$ 6,274.85	
8	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.571243923	$ 5,850.68	
9	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.532628367	$ 5,455.18	
10	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.496623186	$ 5,086.41	
11	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.463051921	$ 4,742.58	
12	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.431750043	$ 4,421.98	
13	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.402564143	$ 4,123.06	
14	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.375351182	$ 3,844.35	
15	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.349977792	$ 3,584.47	
16	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.32631962	$ 3,342.17	
17	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.304260718	$ 3,116.24	
18	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.283692977	$ 2,905.58	
19	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.264515596	$ 2,709.17	
20	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.246634589	$ 2,526.03	
21	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.22996232	$ 2,355.27	
22	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.214417082	$ 2,196.06	
23	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.199922687	$ 2,047.61	
24	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.1864081	$ 1,909.19	
25	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.173807086	$ 1,780.13	
26	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.162057889	$ 1,659.80	
27	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.151102927	$ 1,547.60	
28	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.14088851	$ 1,442.98	
29	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.131364578	$ 1,345.44	
30	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.122484455	$ 1,254.49	
						$ (76,034.29)	NPV of Benefits
						3.03%	IRR

Figure 7. Base Case Cost Benefit Analysis

The annual cost and benefit for years in which the blockchain system is active net to the amount of $10242. Azati Software estimates that the development of a proprietary blockchain system ranges from $50000 to $200000 depending on the scale and scope of the project ("How Much Does it Cost to Develop Blockchain in 2018"). As Visa is a large corporation, the upper end of the range is assumed to be the development cost associated with such a large-scale transaction processing system. The discount rate of 7.25% was determined by pulling Visa's weighted average cost of capital (WACC) from a Bloomberg Terminal.

As the model shows, blockchain systems are clearly not financially feasible using the previous assumptions. The model assumes that blockchain systems will be a long-term project, hence the 30-year projection horizon. The cost benefit ratio, which divides the NPV of future benefits by the initial investment, yields a value of approximately .62, much lower than the CBR ratio of 1 required for a positive NPV investment. For this current model, the IRR suggests that a discount rate of lower than 3.03% would result in a positive project value. However, it is possible that future developments in blockchain research result in lower costs associated with maintenance and operations. Alternatively, the following 30-year model uses the solver function in Excel to suggest an appropriate annualized cost for breakeven.

Cost Benefit Analysis

Enterprise Blockchain System

Year	Benefit	Development Cost	Maintenance Cost	Net Benefit	Discount Factor	Discounted Benefit	Discount Rate
0		$ (200,000.00)	$ -	$ (200,000.00)	1	$ (200,000.00)	7.25%
1	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.932400932	$ 15,406.92	
2	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.869371499	$ 14,365.43	
3	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.810602796	$ 13,394.34	
4	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.755806803	$ 12,488.89	
5	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.704714968	$ 11,644.66	
6	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.657076893	$ 10,857.49	
7	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.612659108	$ 10,123.53	
8	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.571243923	$ 9,439.19	
9	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.532628367	$ 8,801.11	
10	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.496623186	$ 8,206.16	
11	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.463051921	$ 7,651.43	
12	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.431750043	$ 7,134.20	
13	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.402564143	$ 6,651.94	
14	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.375351182	$ 6,202.27	
15	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.349977792	$ 5,783.01	
16	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.32631962	$ 5,392.08	
17	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.304260718	$ 5,027.58	
18	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.283692977	$ 4,687.72	
19	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.264515596	$ 4,370.84	
20	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.246634589	$ 4,075.37	
21	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.22996232	$ 3,799.88	
22	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.214417082	$ 3,543.01	
23	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.199922687	$ 3,303.51	
24	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.1864081	$ 3,080.19	
25	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.173807086	$ 2,871.98	
26	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.162057889	$ 2,677.83	
27	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.151102927	$ 2,496.81	
28	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.14088851	$ 2,328.03	
29	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.131364578	$ 2,170.66	
30	$ 22,242.00	$ -	$ (5,718.08)	$ 16,523.92	0.122484455	$ 2,023.92	
						$ (0.00)	NPV of Benefits
						7.25%	IRR

Figure 8. Base Case Cost Benefit Analysis, Solver Solution

In this solution, the annual costs of maintenance are fixed at $5718 to set the NPV of all future benefits equal to 0. If a company is able to achieve a greater than 50% cost reduction on existing blockchain maintenance costs, then it would be advisable to switch to blockchain as the preferred payment processing system due to this cost breakeven point.

Cost Benefit Analysis							
Enterprise Blockchain System							
Year	Benefit	Development Cost	Maintenance Cost	Net Benefit	Discount Factor	Discounted Benefit	Discount Rate
0		$ (200,000.00)	$ -	$ (200,000.00)	1	$ (200,000.00)	7.25%
1	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.932400932	$ 9,549.65	
2	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.869371499	$ 8,904.10	
3	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.810602796	$ 8,302.19	
4	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.755806803	$ 7,740.97	
5	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.704714968	$ 7,217.69	
6	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.657076893	$ 6,729.78	
7	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.612659108	$ 6,274.85	
8	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.571243923	$ 5,850.68	
9	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.532628367	$ 5,455.18	
10	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.496623186	$ 5,086.41	
11	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.463051921	$ 4,742.58	
12	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.431750043	$ 4,421.98	
13	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.402564143	$ 4,123.06	
14	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.375351182	$ 3,844.35	
15	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.349977792	$ 3,584.47	
16	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.32631962	$ 3,342.17	
17	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.304260718	$ 3,116.24	
18	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.283692977	$ 2,905.58	
19	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.264515596	$ 2,709.17	
20	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.246634589	$ 2,526.03	
21	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.22996232	$ 2,355.27	
22	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.214417082	$ 2,196.06	
23	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.199922687	$ 2,047.61	
24	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.1864081	$ 1,909.19	
25	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.173807086	$ 1,780.13	
26	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.162057889	$ 1,659.80	
27	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.151102927	$ 1,547.60	
28	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.14088851	$ 1,442.98	
29	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.131364578	$ 1,345.44	
30	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.122484455	$ 1,254.49	
Terminal Period				$ 141,268.97	0.11420462	$ 16,133.57	
						$ (59,900.72)	NPV of Benefits
						4.60%	IRR

Figure 9. Cost Benefit Analysis into Perpetuity

The last variation of the base cost benefit analyses keeps many of the assumptions from Figure 7 but introduces the concept of a terminal period. The previous assumption was that blockchain would be considered a long-term project, but if it is assumed that blockchain is maintained as the primary transaction processing system into perpetuity, then it becomes necessary to account for the benefits past year 30. The net benefit for the terminal period is calculated using the perpetuity formula by simply dividing the annual benefit by the discount rate ($12000/7.25%). However, the terminal period is so far in the future that discounting takes away much of the impact that the large net benefit value could make. Shorter term analyses (5 and 10 year) have a smaller discount factor on the terminal period but are still fail to reach breakeven because they don’t capture the extra 20 or 25 years of benefits.

Growth Model Cost Benefit Analysis

Under the assumptions of the previous models, the annual benefits are assumed to be fixed, implying that Visa processes a fixed number of transactions per year. In actuality, Visa as a business seeks a yearly increase in number of processed transactions per year to stimulate revenue growth. The following model looks at the scenario wherein all other assumptions are fixed but Visa now grows transactions at 2% per year. A Sensitivity table is also provided to explore the relationship between discount rate and benefit growth rate on the NPV of benefits.

Cost Benefit Analysis
Enterprise Blockchain System

Year	Benefit	Development Cost	Maintenance Cost	Net Benefit	Discount Factor	Discounted Benefit	Discount Rate	Growth Rate
0		$ (200,000.00)	$ -	$ (200,000.00)	1	$ (200,000.00)	7.25%	2%
1	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.932400932	$ 9,549.65		
2	$ 22,686.84	$ -	$ (12,000.00)	$ 10,686.84	0.869371499	$ 9,290.83		
3	$ 23,140.58	$ -	$ (12,000.00)	$ 11,140.58	0.810602796	$ 9,030.58		
4	$ 23,603.39	$ -	$ (12,000.00)	$ 11,603.39	0.755806803	$ 8,769.92		
5	$ 24,075.46	$ -	$ (12,000.00)	$ 12,075.46	0.704714968	$ 8,509.75		
6	$ 24,556.97	$ -	$ (12,000.00)	$ 12,556.97	0.657076893	$ 8,250.89		
7	$ 25,048.10	$ -	$ (12,000.00)	$ 13,048.10	0.612659108	$ 7,994.04		
8	$ 25,549.07	$ -	$ (12,000.00)	$ 13,549.07	0.571243923	$ 7,739.82		
9	$ 26,060.05	$ -	$ (12,000.00)	$ 14,060.05	0.532628367	$ 7,488.78		
10	$ 26,581.25	$ -	$ (12,000.00)	$ 14,581.25	0.496623186	$ 7,241.39		
11	$ 27,112.87	$ -	$ (12,000.00)	$ 15,112.87	0.463051921	$ 6,998.05		
12	$ 27,655.13	$ -	$ (12,000.00)	$ 15,655.13	0.431750043	$ 6,759.10		
13	$ 28,208.23	$ -	$ (12,000.00)	$ 16,208.23	0.402564143	$ 6,524.85		
14	$ 28,772.40	$ -	$ (12,000.00)	$ 16,772.40	0.375351182	$ 6,295.54		
15	$ 29,347.85	$ -	$ (12,000.00)	$ 17,347.85	0.349977792	$ 6,071.36		
16	$ 29,934.80	$ -	$ (12,000.00)	$ 17,934.80	0.32631962	$ 5,852.48		
17	$ 30,533.50	$ -	$ (12,000.00)	$ 18,533.50	0.304260718	$ 5,639.02		
18	$ 31,144.17	$ -	$ (12,000.00)	$ 19,144.17	0.283692977	$ 5,431.07		
19	$ 31,767.05	$ -	$ (12,000.00)	$ 19,767.05	0.264515596	$ 5,228.69		
20	$ 32,402.39	$ -	$ (12,000.00)	$ 20,402.39	0.246634589	$ 5,031.94		
21	$ 33,050.44	$ -	$ (12,000.00)	$ 21,050.44	0.22996232	$ 4,840.81		
22	$ 33,711.45	$ -	$ (12,000.00)	$ 21,711.45	0.214417082	$ 4,655.31		
23	$ 34,385.68	$ -	$ (12,000.00)	$ 22,385.68	0.199922687	$ 4,475.41		
24	$ 35,073.39	$ -	$ (12,000.00)	$ 23,073.39	0.1864081	$ 4,301.07		
25	$ 35,774.86	$ -	$ (12,000.00)	$ 23,774.86	0.173807086	$ 4,132.24		
26	$ 36,490.36	$ -	$ (12,000.00)	$ 24,490.36	0.162057889	$ 3,968.86		
27	$ 37,220.17	$ -	$ (12,000.00)	$ 25,220.17	0.151102927	$ 3,810.84		
28	$ 37,964.57	$ -	$ (12,000.00)	$ 25,964.57	0.14088851	$ 3,658.11		
29	$ 38,723.86	$ -	$ (12,000.00)	$ 26,723.86	0.131364578	$ 3,510.57		
30	$ 39,498.34	$ -	$ (12,000.00)	$ 27,498.34	0.122484455	$ 3,368.12		
Terminal Period				$ 534,253.42	0.11420462	$ 61,014.21		
						$ 45,433.28	NPV of Benefits	
						8.57%	IRR	

Figure 10. Cost Benefit Analysis, Growth Model

	Sensitivity Analysis		
	1%	**2%**	3%
6.25%	$ 22,107.12	$ 109,469.10	$ 249,597.06
7.25%	$ (15,490.03)	$ 45,433.28	$ 134,366.07
8.25%	$ (42,422.59)	$ 2,574.69	$ 64,257.59

Figure 11. Growth Model Sensitivity Table

This model shows that in the scenario where only annual benefits are affected by a growth rate, blockchain becomes a lucrative project to undertake. It should be noted that the largest difference between the growth and the non-growth models is the terminal value. In the previous model, the only calculation for terminal period benefit was dividing annual net benefit by the discount rate. With the addition of a growth rate, the net benefit is multiplied by the growth rate while the discount rate subtracts the growth rate to account for net discounting.

$$Terminal\ Period\ Net\ Benefit = \frac{(Annual\ Net\ Benefit * Growth\ Rate)}{(Discount\ Rate - Growth\ Rate)}$$

While it is still subject to heavy discounting due to being far in the future, the base benefit to be discounted increases dramatically. However, just accounting for the growth in yearly transactions may not account for all of the yearly change in Visa's costs and benefits. In order to process an increasing number of transactions, the maintenance costs associated with the blockchain system will likely grow as well. The following model grows benefits and maintenance costs at a fixed rate of 2% per year. A second sensitivity table is provided to examine the relationship that benefit growth rate and cost growth rate have on the NPV of benefits.

Cost Benefit Analysis

Enterprise Blockchain System

Year	Benefit	Development Cost	Maintenance Cost	Net Benefit	Discount Factor	Discounted Benefit	Discount Rate	Growth Rate	YoY Cost Increase
0		$ (200,000.00)	$ -	$ (200,000.00)	1	$ (200,000.00)	7.25%	2%	2%
1	$ 22,242.00	$ -	$ (12,000.00)	$ 10,242.00	0.932400932	$ 9,549.65			
2	$ 22,686.84	$ -	$ (12,240.00)	$ 10,446.84	0.869371499	$ 9,082.18			
3	$ 23,140.58	$ -	$ (12,484.80)	$ 10,655.78	0.810602796	$ 8,637.60			
4	$ 23,603.39	$ -	$ (12,734.50)	$ 10,868.89	0.755806803	$ 8,214.78			
5	$ 24,075.46	$ -	$ (12,989.19)	$ 11,086.27	0.704714968	$ 7,812.66			
6	$ 24,556.97	$ -	$ (13,248.97)	$ 11,308.00	0.657076893	$ 7,430.22			
7	$ 25,048.10	$ -	$ (13,513.95)	$ 11,534.16	0.612659108	$ 7,066.31			
8	$ 25,549.07	$ -	$ (13,784.23)	$ 11,764.84	0.571243923	$ 6,720.59			
9	$ 26,060.05	$ -	$ (14,059.91)	$ 12,000.14	0.532628367	$ 6,391.61			
10	$ 26,581.25	$ -	$ (14,341.11)	$ 12,240.14	0.496623186	$ 6,078.74			
11	$ 27,112.87	$ -	$ (14,627.93)	$ 12,484.94	0.463051921	$ 5,781.18			
12	$ 27,655.13	$ -	$ (14,920.49)	$ 12,734.64	0.431750043	$ 5,498.18			
13	$ 28,208.23	$ -	$ (15,218.90)	$ 12,989.33	0.402564143	$ 5,229.04			
14	$ 28,772.40	$ -	$ (15,523.28)	$ 13,249.12	0.375351182	$ 4,973.07			
15	$ 29,347.85	$ -	$ (15,833.75)	$ 13,514.10	0.349977792	$ 4,729.64			
16	$ 29,934.80	$ -	$ (16,150.42)	$ 13,784.38	0.32631962	$ 4,498.11			
17	$ 30,533.50	$ -	$ (16,473.43)	$ 14,060.07	0.304260718	$ 4,277.93			
18	$ 31,144.17	$ -	$ (16,802.90)	$ 14,341.27	0.283692977	$ 4,068.52			
19	$ 31,767.05	$ -	$ (17,138.95)	$ 14,628.10	0.264515596	$ 3,869.36			
20	$ 32,402.39	$ -	$ (17,481.73)	$ 14,920.66	0.246634589	$ 3,679.95			
21	$ 33,050.44	$ -	$ (17,831.37)	$ 15,219.07	0.22996232	$ 3,499.81			
22	$ 33,711.45	$ -	$ (18,188.00)	$ 15,523.45	0.214417082	$ 3,328.49			
23	$ 34,385.68	$ -	$ (18,551.76)	$ 15,833.92	0.199922687	$ 3,165.56			
24	$ 35,073.39	$ -	$ (18,922.79)	$ 16,150.60	0.1864081	$ 3,010.60			
25	$ 35,774.86	$ -	$ (19,301.25)	$ 16,473.61	0.173807086	$ 2,863.23			
26	$ 36,490.36	$ -	$ (19,687.27)	$ 16,803.09	0.162057889	$ 2,723.07			
27	$ 37,220.17	$ -	$ (20,081.02)	$ 17,139.15	0.151102927	$ 2,589.78			
28	$ 37,964.57	$ -	$ (20,482.64)	$ 17,481.93	0.14088851	$ 2,463.00			
29	$ 38,723.86	$ -	$ (20,892.29)	$ 17,831.57	0.131364578	$ 2,342.44			
30	$ 39,498.34	$ -	$ (21,310.14)	$ 18,188.20	0.122484455	$ 2,227.77			
Terminal Period				$ 353,370.77	0.11420462	$ 40,356.57			
						$ (7,840.14)	NPV of Benefits		
						6.98%	IRR		

Figure 12. Cost Benefit Analysis, Alternative Growth Model

			Sensitivity Analysis	
			Growth	
		1%	**2%**	3%
	1.00%	$ (37,956.81)	$ 21,468.12	$108,197.40
Cost	**2.00%**	$ (65,288.11)	$ (7,840.14)	$ 75,981.85
	3.00%	$ (98,698.21)	$(43,851.53)	$ 36,145.01

Figure 13. Alternative Growth Model Sensitivity Table

This model is exactly the same as the one displayed in figure 11 with the notable exception of maintenance cost also growing on a 2% annual basis. As expected, the sensitivity table shows that the greatest lever for reaching breakeven on NPV of Benefits is growth rate. Unlike the growth in cost, the growth rate of benefits impacts both the yearly net benefit and is directly factored into the calculation for terminal period net benefit. The implication is that as long as yearly transactions continues to grow, the realized benefits of switching to a blockchain system will contribute towards breakeven given that costs also grow at a fixed rate.

The overall conclusion from all of the cost benefit analyses is that many of the scenarios feature an NPV value or require a large amount of favorable assumptions to reach breakeven. The existing costs of maintaining a blockchain system remain high and the electricity required to process transactions on Visa’s existing system is not necessarily expensive. The initial development cost is relatively high due to the lack of specialized blockchain programmers and development companies. There are two possible solutions for businesses to pursue in light of these observations. They could consider implementing smaller scale granular solutions, most of which would be relatively cheaper to develop. A second solution is simply to wait until blockchain technology develops to the point where implicit energy costs make it affordable to implement on a larger scale (potentially by using proof of stake consensus protocol). If blockchain systems do become more energy efficient, companies may choose to forgo private development altogether and seek out specialty BaaS companies for blockchain solutions. Utilizing BaaS would remove the large initial development cost but the key tradeoff is the ability to fully customize the way the blockchain is designed and structured to hold data.

Chapter 6

Conclusion

The public interest in blockchain has died considerably since the Bitcoin bubble of 2017, but companies are continuing to investigate blockchain and smart contract solutions. Chuen and Dula have suggested that “Banks… have been reluctant to adopt technologies like Bitcoin, given its nefarious press and association with illicit money transfers… distributed ledger technologies and peer-to-peer lending is alien to the banks’ middleman business practices and highly centralized nature” (2018, p. 15). This distrust of new blockchain technology closely corroborates with a report from Nasdaq that suggests that as of August 2018, only 3% of Fortune 500 companies have integrated blockchain into their core business operations. It is possible that companies are being conservative and waiting for others to “make the first move”, but it is also equally likely that financial institutions recognize the essential spirit of blockchain as democratized and open threatens their existing position as institutions of financial authority. Other industries may be following the lead of financial services, which happens to have the greatest incentive to come up with innovative blockchain projects.

A key takeaway from the analysis of existing enterprise use cases is that businesses are at least willing to engage in blockchain projects that provide data storage/management and to harness the potential automation that smart contracts provide. While many businesses may seek to take a conservative approach instead of altering the fundamental structure of their business using blockchain, any company that is hesitant to hire specialized blockchain programmers should consider partnering with a BaaS or another blockchain specialty company like a blockchain lab.

The cost benefit analysis alongside the analysis of existing use cases show that blockchain is most likely not currently suitable for large scale transformative impact. Because of the relatively high costs of developing a blockchain system independently, businesses may seek to partner with BaaS companies to eliminate upfront costs or to develop cheaper, lower complexity systems to be used as granular solutions for specific data storage applications. Most of the existing business use cases focus on a particular small-scale application that combine smart contracts with blockchain technology. Because of the lack of businesses integrating blockchain into their core business operations, it is likely that the cost reductions supposedly promised by blockchain are tough to realize in application and at scale.

Proponents of blockchain technology claim that distributed ledgers can revolutionize business while detractors pass it off as an inefficient waste of resources. The reality of the situation is that the potential to utilize blockchain and smart contracts within businesses probably lies somewhere in the middle of these two views: there are existing applications providing a look into the extreme potential of the future and technical limitations preventing integration into core business operations. The issues of energy costs and scalability are questions for computer science to solve, but if they are successfully resolved then blockchain will truly have the ability to change a variety of business industries in a transformative fashion by providing automation, transparency, and security.

BIBLIOGRAPHY

“Bitcoin Energy Consumption Index.” *Digiconomist*, https://digiconomist.net/bitcoin-energy-consumption. Blenkinsop, Connor. “Blockchain’s Scaling Problem, Explained.” *Cointelegraph*, 22 Aug. 2018, https://cointelegraph.com/explained/blockchains-scaling-problem-explained.

Blockchain State Legislation. http://www.ncsl.org/research/financial-services-and-commerce/the-fundamentals-of-risk-management-and-insurance-viewed-through-the-lens-of-emerging-technology-webinar.aspx.

Board of Governors of the Federal Reserve System (U.S.), et al. “Distributed Ledger Technology in Payments, Clearing, and Settlement.” *Finance and Economics Discussion Series*, vol. 2016, no. 095, Dec. 2016. *Crossref*, doi:10.17016/FEDS.2016.095.

Buterin, Vitalik. *Chain Interoperability*. p. 25.

Butler, Andrew. “Ethereum Classic Attacked! How Does the 51% Attack Occur?” *Hacker Noon*, 8 Jan. 2019, https://hackernoon.com/ethereum-classic-attacked-how-does-the-51-attack-occur-a5f3fa5d852e.

Castillo, Michael del. “The 10 Largest Companies In the World Are Now Exploring Blockchain.” *Forbes*, https://www.forbes.com/sites/michaeldelcastillo/2018/06/06/the-10-largest-companies-exploring-blockchain/.

Cocco, Luisanna, et al. “Banking on Blockchain: Costs Savings Thanks to the Blockchain Technology.” *Future Internet*, vol. 9, no. 3, Sept. 2017, p. 25. *www.mdpi.com*, doi:10.3390/fi9030025.

Collette, Benjamin, et al. “Blockchain and the Impact on Fund Distribution.” Deloitte Luxembourg, 25 Sept. 2017, www2.deloitte.com/lu/en/pages/technology/articles/impacts-blockchain-funddistribution.html.

Danezis, George, and Sarah Meiklejohn. “Centrally Banked Cryptocurrencies.” *ArXiv:1505.06895 [Cs]*, May 2015. *arXiv.org*, http://arxiv.org/abs/1505.06895.

“Did a Crypto CEO Fake His Own Death to Abscond with $190 Million?” *Futurism*, https://futurism.com/growing-suspicion-crypto-ceo-faked-death.

Dula, Christopher, and David LEE Kuo Chuen. “Reshaping the Financial Order.” Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1, Elsevier, 2018, pp. 1–18. Crossref, doi:10.1016/B978-0-12-810441-5.00001-4.

edChain. “A Comparison Between 5 Major Blockchain Protocols.” *EdChain*, 19 May 2018, https://medium.com/edchain/a-comparison-between-5-major-blockchain-protocols-b8a6a46f8b1f.

Elhanani, Zohar. “How Blockchain Changed The Art World In 2018.” *Forbes*, https://www.forbes.com/sites/zoharelhanani/2018/12/17/how-blockchain-changed-the-art-world-in-2018/.

“Ethereum Energy Consumption Index (Beta).” *Digiconomist*, https://digiconomist.net/ethereum-energy-consumption.

Falkon, Samuel. “The Story of the DAO — Its History and Consequences.” *Medium*, 24 Dec. 2017, https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee.

"Financial Privacy." *Federal Trade Commission*, 22 July 2013, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/financial-privacy.

Fizzy. https://fizzy.axa/en-gb/faq.

Heaven, Douglas. "A House Has Been Bought on the Blockchain for the First Time." *New Scientist*, https://www.newscientist.com/article/mg23631474-500-a-house-has-been-bought-on-the-blockchain-for-the-first-time/.

"How Much Does It Cost to Develop Blockchain in 2018." *AI, ML, NLP Consulting and Software Development.*, 8 Feb. 2019, https://azati.com/how-much-does-it-cost-to-blockchain/.

"ICBC's First Blockchain Patent Is Now Public." *CoinDesk*, 30 Apr. 2018, https://www.coindesk.com/chinese-bank-giant-wants-to-view-users-certificates-on-blockchain.

Kastelein, Richard. "Zilliqa Breaks 2,400 Transactions per Second with Their 'Sharding' Blockchain." *Blockchain News*, 13 Oct. 2017, https://www.the-blockchain.com/2017/10/13/zilliqa-breaks-2400-transactions-per-second-sharding-blockchain/.

Lamport, Leslie, et al. "The Byzantine Generals Problem." *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, July 1982, pp. 382–401. *Crossref*, doi:10.1145/357172.357176.

Mills, David, Kathy Wang, Brendan Malone, Anjana Ravi, Jeff Marquardt, Clinton Chen, Anton Badev, Timothy Brezinski, Linda Fahy, Kimberley Liao, Vanessa Kargenian, Max Ellithorpe, Wendy Ng, and Maria Baird. "Distributed ledger technology in payments, clearing, and settlement", 2016, Finance and Economics Discussion Series 2016-095.

Washington: Board of Governors of the Federal Reserve System, https://doi.org/10.17016/FEDS.2016.095.

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*.

P2626.Pdf. https://www.rand.org/content/dam/rand/pubs/papers/2005/P2626.pdf.

Rizzo, Pete. "World Economic Forum Survey Projects Blockchain 'Tipping Point' by 2023." *CoinDesk*, 24 Sept. 2015, https://www.coindesk.com/world-economic-forum-governments-blockchain.

"Share&Charge - Peer-To-Peer Solutions." *Share&Charge*, https://shareandcharge.com/solution/.

Siegel, David. "Understanding The DAO Attack." *CoinDesk*, 25 June 2016, https://www.coindesk.com/understanding-dao-hack-journalists.

Smart Contracts State Legislation – Sagewise. https://www.sagewise.io/smart-contracts-state-legislation/.

Szabo, Nick. "Formalizing and Securing Relationships on Public Networks." *First Monday*, vol. 2, no. 9, Sept. 1997. *firstmonday.org*, doi:10.5210/fm.v2i9.548.

"The Price Of Electricity In Your State." *NPR.Org*, https://www.npr.org/sections/money/2011/10/27/141766341/the-price-of-electricity-in-your-state.

THEMABLOG: BITCOIN, BLOKCHAIN AND CRYPTOCURRENCY. /themablog-bitcoin-blokchain-and-cryptocurrency/.

Visa-2016-Corporate-Responsibility-Report.Pdf. https://usa.visa.com/dam/VCOM/download/corporate-responsibility/visa-2016-corporate-responsibility-report.pdf.

What Is a 51% Attack? : CoinExchange.Io. https://coinexchangeio.freshdesk.com/support/solutions/articles/9000155990-what-is-a-51-attack-.

"What Is a Digital Signature? » The Basics | Lisk Academy." *Lisk*, https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/digital-signatures.

What Is Ethereum? — Ethereum Homestead 0.1 Documentation. http://ethdocs.org/en/latest/introduction/what-is-ethereum.html.

Why Aren't More Companies Using The Blockchain? - Nasdaq.Com. https://www.nasdaq.com/article/why-arent-more-companies-using-the-blockchain-cm1007922. Accessed 28 Sept. 2018.

Wood, Dr Gavin. *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER*. p. 1.

Zhao, Wolfie. "Banking Giant Trials Blockchain for Issuance of Land-Backed Loans." *CoinDesk*, 31 July 2018, https://www.coindesk.com/banking-giant-trials-blockchain-for-issuance-of-land-backed-loans.

ACADEMIC VITA

Daniel Y. Zhang
Dzhang57@gmail.com

Education

B.A. in Philosophy, Spring 2019, The Pennsylvania State University

B.S. in Finance, Spring 2019, The Pennsylvania State University

Honors in Finance

Thesis: Enterprise Use Cases for Smart Contract Technology on Blockchain Networks

Thesis Supervisor: Jingzhi Huang

Honors Advisor: Brian Davis

Professional Experience

Business Valuation Intern at Ernst and Young, June 2018 – August 2018

Finance Intern at Thomas Jefferson University Hospital, June 2017 – August 2017

Honors and Awards

Schreyer Honors College

Phi Beta Kappa

Dean’s List