The Past, Present, and Future of Blockchain Technology in the Financial Services Industry

Jiayi Chen

***Abstract*—Satoshi Nakamoto's blockchain paper in 2008 proposed a solution that solves key problems in current digital currency technologies by providing a decentralized distributed ledger system that uses cryptography and hashing to maintain public records of transaction records. Ever since his paper and later his Bitcoin code release in 2009, the community of blockchain supporters has grown and many consider its applications in the financial industry promising. However, just like most nascent technologies, blockchain technology faces practical challenges such as scalability and speed that are crucial for real-world applications in the financial industry. Regulatory restrictions are also in the grey area because of a lack of preexisting similar technologies. Several new solutions such as Ethereum, Corda, and Hyperledger are introduced as attempts to address these problems but they have yet to be widely adopted by the financial industry. Despite under many doubts, blockchain technology still has the potential to change the traditional technology by backing public and private ledger services.**

***Index Terms*— Authentication, computer hacking, computer networks, cryptographic protocols, digital signatures, encryption, distributed databases, financial management, public key, random number generation.**

I. Introduction

The use of blockchain is relatively new in the financial industry. Although similar ideas to decentralize money transaction ledgers had been proposed before, it was not until Satoshi Nakamoto published his 2008 paper on blockchains [1] that distributed ledger finally have an applicable structure to build upon. After several years of development, blockchain as a way of encrypting and storing transaction information can be found in the foundation to Bitcoin, a cryptocurrency, and other distributed ledger systems. In this survey I explore how blockchain solves existing problems, its key design factors, its advantages and disadvantages, its current state in applications, key players experimenting on blockchains, and finally, the future of the applications of blockchains.

A. Why is it important, what problem does it solve?

Blockchain provides trust from technological security to overcome weak points in now widely-adopted centralized ledgers by providing a decentralized model. Existing ledger systems rely on trust from a central authority such as a bank. This trust and security, however, is partially backed by the preexisting success of the system, and partially a product of the impression of authority of a big bank or a well-established company. There are some problems to this centralized model: a) centralized organization becomes an easy target for attackers; b) centralization means that there is no backup if the central authority is taken down; c) the verification of a transaction can be time consuming if human power is needed to cross-validate the parties in the transaction; d) the double spending problem common in financial transaction.

Nakamoto's blockchain implementation solves these problems of centralization with a distributed system based not on authoritative trust, but a trust built upon encryption and a decentralized network.

B. Key Considerations

A blockchain in a distributed network provides safety measures against attackers by allowing every node in the network to own a piece of the blockchain, which stores all the transactions in the network. If a fraction of the nodes in the system are attacked, the whole network can still operate normally. Furthermore, with the proper encryption protocol, the distributed ledger can prevent several attackers from infiltrating the system, thus solving thing the Byzantine Generals Problem in distributed systems [24]. Therefore problem a) and b) are solved.

Nakamoto's model solves the verification efficiency problem by using cryptograph and special designs on the blockchain structure. By having a genesis block with a hash value and designing each block to hash to the value in the previous block, the blockchain structure ensures that all the blocks are linked. If an attacker were to change a transaction in the chain, simply changing the value on a block would not be a valid method because the latest hash value on the last block will be different because the previous hash values have changed. The transaction blocks that are securely "chained" by their hash values give such a structure its name "blockchain" ("block chain" in Nakamoto's original paper) [1].

Such blockchain structure also eliminates the last problem: double spending. To verify a transaction is valid, so called "miners" which are nodes in the network, perform a proof-of-work computation to gain the right to verify a set of transactions (usually in the size of 1 MB chunks, or blocks). This proof-of-work implementation prevents malicious nodes from verifying invalid transaction. Specifically, to gain verification rights, the node need to find a hash value below a certain threshold. In Nakamoto's design, the average time to

Jiayi Chen is with the Department of Computer Science, Columbia University in the City of New York, New York, NY, 10027, USA (email: jiayi.chen@columbia.edu).

find such a value is about 10 minutes [1]. Although this design provides security measures, it creates hurdles for a blockchain structure to quickly process large amount of transactions, a problem discussed in Section III.

C. Applications in the financial service industry

One of the most notable blockchain applications is in cryptocurrency. In fact, Nakamoto designed the blockchain structure and implemented Bitcoin currency with payments in mind. It was built with cross-validation from public keys and private keys, and double-hashing in SHA-256 to encrypt the transaction information, and finally hash chains to secure all the information in the chain. With these safety measures in place, blockchain is at an advantage to provide the backbones of a stables and controllable payment system. The daily transactions of Bitcoin have steadily increased since 2012 and now almost 300,000 transactions are made daily.

Blockchain can also be used to settle trade transactions in Asset Management by keeping track of verifications and credentials from different parties in the transactions and prevent human errors as well as securing the integrity of the data in the transaction. Similarly, blockchain can be used to process claims in the insurance industry. Blockchain's key feature that prevents double-spending and its extension applications such as smart contract make the process transparent and traceable, and secure.

II. Advantages and Disadvantages of the Blockchain Solution

A. Advantages: Secure and Economic

A distributed ledger network provides a convenient way of transaction ledger. Blockchain's public keys and private keys allow users to anonymously send transactions to other users on the network without revealing any identity if using TOR. This anonymity is beneficial for buyers and sellers who do not wish to reveal their identity and this feature means that more people can participate in the economy without worrying about their identities.

Block is also theoretically more secure because it hashes a transaction text using the hashing from the previous block so as to "chain" the encrypted public keys together. This means that the entire blockchains on each and every node will get more secure as more blocks are added to the chain. This is the reason why blockchain only becomes more secure as the chain grows as time goes on. An account balance is calculated by going through all the transactions in the chain and then adding up all the incoming and outgoing funds. This way, it is very hard to insert new transactions or blocks in to the chain because the chain need to correspond to both the previous and ensuing block's double-hashed. To alter a trade, the whole chain after the trade will need to be altered: all the encryptions need to be rehashed, verified, and chained back together.

Also the risk of losing transaction data is minimal because of the distributed system. Because each node keeps track of a copy of the chain, if a small portion of the nodes dies the whole infrastructure is still intact. The recovery for a dead node can be quickly configured because it can duplicate the chain from other nodes.

B. Disadvantage: speed, forking, scalability, perils of decentralization

Privacy concern is a roadblock for financial applications. Although the chain becomes more secure as more blocks are added, the blockchain structure and code are readily available to the public and that means that anyone can look at the blockchain code and try to figure out ways to hack it. Because of the chain structure, once the chain is hacked, the whole chain might need to be restructured or, as in the case for Ethereum, a new chain and new code will need to be implemented to keep everyone in the economy happy. However, to maintain the distributed, decentralized structure of the blockchain philosophy, there should not be too many restructuring if the economy is global [4].

Moreover, in a democratized structure like that of blockchain, it is difficult to get a sufficient consensus from everyone, especially for a huge change like a hard fork. The process of obtaining a consensus might cause catastrophic consequences for such a community that relies on individual user on each node for computational power. In addition, larger blocks might not fundamentally solve the problem of transaction congestions as wished. Because larger blocks will be added to the chain, the length of the chain will grow slower, and this low propagation speed might cause another set of problems including "orphan rate amplification, more reorg[anizations] and double-spends [7]." Furthermore, larger blocks may lead to centralization of the blockchain network because more computational power is needed to maintain larger blocks and therefore only those organizations with significant CPU power can maintain nodes with relative ease [8]. Damage to the decentralization nature of blockchain is detrimental because the merit of blockchain builds on the trust of it being a decentralized and democratically monitored network. If only a handful of nodes stores the blockchains, it is no different from a cartel with significant negotiating power against other smaller users in the economy, not to mention, if one of the main nodes is down the harm will be much more significant than if a bunch of small nodes are down in the existing blockchain network.

The mining process could also mean that computational power-rich nodes might become central nodes and dominate. Nowadays China is one of the leaders in Bitcoin mining, accounting for 70% of the mining powers worldwide [21]. The centralization of mining resources is not a direct threat to the blockchain network; they do not control the nodes or directly manage the chains. However, miners are a central part of the blockchain ecosystem that makes sure transactions are settled and added to the chains. Without enough miners competing to solve the SHA-256 string, transactions are just logged in the transaction pool and payments are processed slowly. Of course the platform managers can change the settings of the difficulty of the puzzles to reduce the computational power for a puzzles, but that could mean a compromise to the security that blockchain boasts.

The mining design causes another problem for blockchain systems: speed. Proof-of-work validation is an important mechanism to keep blockchain safe, but the average time it takes to solve a puzzle is ten minutes. Currently, the maximum

size for a typical valid block is 1MB, a size that limits the number of transactions than can be mined and published per second. The blockchain protocol does not put speed at its first priority. Satoshi's paper [1] made sure that blocks are added to the chain at a controlled rate, by increasing or decreasing the difficulty of the puzzle needed to be solved to add the block to the chain. While this design is immensely beneficial for security and transparency, it limits the number of transactions that can be verified. Satoshi thought of this mechanism to solve the Byzantine Generals Problem [24], preventing malicious miners from adding dishonest blocks to the chain (because the chance of solving two blocks successively is extremely low), but for blockchain to be practical and be used for a global economy, it needs to be able to verify transactions not only securely, but also quickly. 10 minutes per 1MB block is simply not fast enough in an economy where debit cards can be processed immediately and other peer-to-peer money service handle small transactions instantly. The convenience of trust, rather than technology-backed security can be an important factor as to why Bitcoins still has not entered the mainstream consumer realm despite the its inception in 2009.

Money transfer through a blockchain-backed can also be sometimes costly. According to Bitcoin.org, original site created by the blockchain proposer Satoshi Nakamoto himself, currently the transaction fee is 9.95% of the total traded currency [9], 0.58% of the trading volume, and averages to 8.05 USD per transaction. This is number is on par with Western Union's "No more than $10 fee" [9] plus exchange earnings [10]. However, this cost does not make bitcoin transactions dramatically more preferable compared to traditional methods considering its speed and transparency. If the customer does not mind anonymity, Venmo or PayPal might still be a more viable choice.

III. Challenges: Implementation, Adoption and Regulatory Challenges

A. Implementation challenges

The bridge between the distributed ledger system and the application layer, the replacement for miners in the private setting, and protocol changes can be a few of the implementation challenges.

Integration to the application level can be a challenge. Blockchain provides the backbone of the distributed ledger system. Public solutions such as Bitcoin and Ethereum are largely established and successful. However, to bring these solutions into the corporate setting means that they need to provide a blockchain access layer that links the services of the financial institutions with the blockchain structure. One proposed solution comes from Software AG, a software company that provides enterprise solutions to some of the largest banks in the US. They envisioned their product to act as a broker who "abstracts the complexities of smart contracts and exposes blockchain application functionalities and communicates them to legacy applications [20]."

Because of the complexities in the nature of some transactions in the financial service industry, it is possible that multiple blockchains protocols are needed and intertwined together to make the network application effective. Such network would require specific protocols and would be company specific. The private and enterprise setting certainly reduces the power of a "distributed" ledger network, but for a global company with many nodes in different network, blockchain can be a good solution, despite the complication in the implementation level.

Another problem lies in the mining aspect of the transaction processing step. In a public blockchain system miners add transactions. But in an enterprise setting there needs to be a sector that exclusively solves the puzzles and add transactions. Because of a decrease in scale and a need for speed processing, the processors can be susceptible to attacks and therefore malicious addition of transaction blocks. Whether it is efficient to have a dedicated miner section as opposed to an alternative to solving puzzles is another problem. Even though the total number of solutions in the order of magnitude of 46, or 2^160 [10] total solutions to be precise, and the blockchain core development team keeps tweaking the difficulty for puzzles to keep the solving time to about 10 minutes per solution, for an enterprise, the processing need to be much faster to it to be practical. Ethereum has a solution that is described in Section IV.

The third challenge is the difficulty for a hard-fork and upgrade. The difficulty comes from the sheer number of transactions such as smart contracts that goes through the database and in the case of a hard-fork like Ethereum did [6], all the rules and settings in the contract might be changed and for banks this could be a huge mess to resettle and change if there is ever a glitch. In addition, if changes are to be made frequently, smart contract does not seem efficient since all the changes will need to be traced back to its beginning, making the alteration process long.

B. Adoption

The most prominent use of blockchain technology is in the cryptocurrency Bitcoin. Today, Bitcoin is exchangeable in 20 countries and has a trade volume of 164,636.17617949 BTC, which is equivalent to 161,471,053.92 USD as of March 18th, 2017 [11].

According to a report by PwC in May 2016 [12], financial services have yet to fully respond to the uprising of distributed ledger technologies such as blockchain. It is reported that, "While the majority (56%) recognize its importance, 57% say they are unsure or unlikely to respond to this trend."

The report also points out advantages of the blockchain technology that makes it appealing to not only participants in the financial industry but also regulatory institutions: "Not only could there be huge cost savings through [blockchain's] use in back-office operations but also large gains in transparency that could be very positive from an audit and regulatory point of view [12]."

The public nature of blockchains made it appealing to communities that believe in transaction transparency, but for institutions with concerns for user privacy blockchains is not ideal. Even though the information is encrypted using SHA-256, the information being just "out-there" means that hackers can access the information and there is a risk of information leakage. Therefore, a lot of large companies such as Morgan Stanley, Barclays, and Credit Suisse are investigating private blockchains that provides security but

without putting its clients' data under public scrutiny [14]. As of 2016, Deloitte and IBM have announced usage of blockchains, and yet other large financial institutions seem not to have made their move public yet [15].

There are some adoptions by exchanges. For example, Nasdaq executes its first trade on blockchain in 2015 through a blockchain developer called Chain.com [23]. Nasdaq has since been actively exploring options to exploit the blockchain technology and "expects its blockchain initiative, Linq, could reduce settlement risk by more than 99 percent [26]."

C. Regulations

Like all financial instruments Bitcoin is a subject for financial abuse, its anonymity and accessibility make it especially susceptible to money-lauders. Yet currently there is little regulations on Bitcoins and standards on blockchain implementations.

In 2013, China banned financial institutions from Bitcoin transactions. Then recently in February 2017 the Chinese central bank asked two largest Chinese Bitcoin exchanges to strictly monitor any activities in money-laundering and foreign exchange. The enforcement has an immediate negative impact on the price of Bitcoin but it has since slowly regaining momentum. Nevertheless, the Chinese regulators alarmed blockchain developers to build stronger anti-fraud and legally compliant platforms to impose overall financial securities.

The U.S. Securities and Exchange Commissions (SEC) just declined a proposal to enlist a Bitcoin exchange traded fund (ETF) by Winklevoss Bitcoin Trust (WBT) because of its unregulated status: "The Commission believes that the significant markets for Bitcoin are unregulated. Therefore, as the Exchange has not entered into, and would currently be unable to enter into, the type of surveillance-sharing agreement that has been in place with respect to all previously approved commodity-trust ETFs—agreements that help address concerns about the potential for fraudulent or manipulative acts and practices in this market—the Commission does not find the proposed rule change to be consistent with the Exchange Act [3]." It seems that the unstable performance of the blockchain structures lead to a risk in fraudulent behaviors and that is the reason why SEC is turning WBT down.

The current deregulated cryptocurrency market is perhaps a result of US regulators not seeing the blockchain-backed public platforms as a huge threat to the general safety of US economy and has not taken aggressive measures to regulate the market.

IV. Key players in the industry

A. Bitcoin:

BitCoin.org was initially registered by Satoshi Nakamoto and has since been handed to Gavin Andresen and others. Since then Bitcoin.org has been responsible for tracking the number of coins and transactions, providing Bitcoin wallet services, and educating the public on the application of Bitcoins [15].

B. Ethereum:

Ethereum is another main player in the public distributed ledger business, currently offering their Ethereum Wallet services and supporting the Decentralized Autonomous Organization in managing funds, and smart contract functionalities. Based on the Ethereum Virtual Machine, it uses "Ether" as currency and has gone through several hard forks since its inception due to technical errors and hacking. Ethereum's processing time is faster (between 14-15 seconds) and encourages decentralized mining. In fact, in Ether mining there is no advantage to pool mining because of their philosophy [22].

C. IBM

IBM released a blockchain service on the IBM cloud that allow developers to transfer digital assets "more securely and privately" (IBM). IBM stresses the merit in blockchain's "security, availability and performance for handling sensitive and regulated data" but shies away from what the blockchain community tries to embody -- public data. Indeed, the privacy of sensitive data is a priority for a lot of Financial Service institutions, and IBM is adapting the blockchain technology to fit the industry's needs. Yet it tries to preserve the nature of the original blockchain technology by making the 44,000 lines of its Hyeperledger Project to the Linux Foundation open-source. IBM stresses the promising future of smart contracts and the "fine-grained privacy and confidentiality control" that appeals to its customers. But as of now, they are only opening up "Garages" in global financial hubs like New York and Singapore to encourage developers to collaborate, without a specific product [20].

D. R3 CEV

R3 CEV is another visible force in big financial institutions' effort in responding to the blockchain technology. It pulls together 73 financial companies, including Barclays, Citi, Deutsche Bank, Morgan Stanley, Credit Suisse, and HSBC, and aims to develop Corda, with directly responds to the "privacy and scalability for challenges facing decentralized applications" like Bitcoin and Ethereum [13]. Built from a business perspective, Corda is different in that it claims to restrict data sharing to only those in the transaction, and allows pluggable consensus to abide to regulatory requirements. Interestingly, Hearn, who decried the shortcoming of the Bitcoin design scheme such as scalability, is one of the authors for Corda's introductory white papers released in August 2016 [19]. His personal move from the public domain to a private setting might not reveal much about the future of blockchain technology, but his mobility indicates the adaptability of distributed ledger systems.

V. Outlook

To borrow Arvind Narayanan's idea [25], expecting a data structure and protocol like blockchain to revolutionize the finance industry is like expecting the Merkle Tree or arrays to revolutionize the finance industry [26]. Ultimately, the usefulness of a piece of technology is largely dependent on how it fits with other pieces already in place and the actual needs of the industry. Indeed, using blockchain as a part of a data encryption and broadcasting protocol provides numerous possible applications listed in this survey, but we are not sure if it is the most applicable structure for it to truly become a staple in the financial service industry.

While the Bitcoin and Ethereum communities continue to add blocks to chains, large financial institutions are still on the lookout on whether to hop on to the blockchain ship or not. Blockchain technology is still new and it takes a lot of time to experiment and explore its compatibility with the current systems. So far a few problems have risen and they range from security loopholes to scalability issues. Just as any tool, for it to be practical changes will need to be made, and we expect future developers exploit its advantages in immutability and ease of verification and seek solutions to its problems.

REFERENCES

[1]S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", *bitcoin.org*, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: 20- Mar- 2017].

[2] IBM Institute for Business Value, "Blockchain rewires financial markets", IBM, Somer, NY, 2016.

[3]E. Aleman, "Order Disapproving a Proposed Rule Change, as Modified by Amendments No. 1 and 2, to BZX Rule 14.11(e)(4), Commodity-Based Trust Shares, to List and Trade Shares Issued by the Winklevoss Bitcoin Trust", 2017. [Online]. Available: https://www.sec.gov/rules/sro/batsbzx/2017/34-80206.pdf. [Accessed: 20- Mar- 2017].

[4]M. Peck, ""Hard Fork" Coming to Restore Ethereum Funds to Investors of Hacked DAO", *IEEE Spectrum: Technology, Engineering, and Science News*, 2016. [Online]. Available: http://spectrum.ieee.org/tech-talk/computing/networks/hacked-blockchain-fund-the-dao-chooses-a-hard-fork-to-redistribute-funds. [Accessed: 20- Mar- 2017].

[5]"Bitcoin currency statistics", *Blockchain.info*, 2017. [Online]. Available: https://blockchain.info/stats. [Accessed: 20- Mar- 2017].

[6]G. Andresen, "Time to Roll Out Bigger Blocks", *gavinadressen.ninja*, 2015. .

[7]"Block size limit controversy - Bitcoin Wiki", *En.bitcoin.it*, 2016. [Online]. Available: https://en.bitcoin.it/wiki/Block_size_limit_controversy. [Accessed: 20- Mar- 2017].

[8]M. Hearn, "The Resolution of the Bitcoin Experiment", *blog.plan99.net*, 2016. .

[9]"Send Money Internationally | Western Union", *Westernunion.com*, 2017. [Online]. Available: https://www.westernunion.com/au/en/send-money-internationally.html. [Accessed: 20- Mar- 2017].

[10]S. Driscoll, *How Bitcoin Works*. 2013.

[11]"USD Exchange Trade Volume", *Blockchain.info*, 2017. [Online]. Available: https://blockchain.info/charts/trade-volume. [Accessed: 20- Mar- 2017].

[12]M. Kashyap, "Blurred lines: How FinTech is shaping financial services", PwC, 2016.

[13]L. Parker, "30 top banks and Mike Hearn have now joined R3 Global Consortium » Brave New Coin", *Bravenewcoin.com*, 2015. [Online]. Available: https://bravenewcoin.com/news/30-top-banks-and-mike-hearn-have-now-joined-r3-global-consortium/. [Accessed: 20- Mar- 2017].

[14] Deloitte, "Deloitte Launches Blockchain Lab in New York, Increasing Focus on Key Technology in 'Make-or-Break' Year", 2017.

[15]"Bitcoin - Open source P2P money", *Bitcoin.org*, 2017. [Online]. Available: https://bitcoin.org/en/. [Accessed: 20- Mar- 2017].

[16]"Ethereum Project", *Ethereum.org*, 2016. [Online]. Available: https://ethereum.org/. [Accessed: 20- Mar- 2017].

[17] IBM, "IBM Continues Expansion of Global Cloud Centers to Support Hybrid Cloud Growth", 2015.

[18]J. Lambert, "SURVEY OF CONFIDENTIALITY AND PRIVACY PRESERVING TECHNOLOGIES FOR BLOCKCHAINS", *The R3 Report*, 2017. .

[19]R. Brown, J. Carlyle, I. Grigg and M. Hearn, "Corda: Introductory White Paper", *r3cev.com*, 2016. [Online]. Available: https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/57bda2fdebbd1acc9c0309b2/1472045822585/corda-introductory-whitepaper-final.pdf. [Accessed: 20- Mar- 2017].

[20]J. Gil-Pulgar, "Overcoming Blockchain Implementation Challenges", *Bitcoin News*, 2017. [Online]. Available: https://news.bitcoin.com/blockchain-implementation-challenges/. [Accessed: 24- Mar- 2017].

[21]Denyer, Simon. "The Bizarre World Of Bitcoin 'Mining' Finds A New Home In Tibet". *Washington Post*. N.p., 2017. Web. 24 Mar. 2017.

[22]"Why Is Ethereum Different To Bitcoin?". *CryptoCompare*. N.p., 2017. Web. 24 Mar. 2017.

[23] "Nasdaq Linq Enables First-Ever Private Securities Issuance Documented With Blockchain Technology (NASDAQ:NDAQ)". *Ir.nasdaq.com*. N.p., 2015. Web. 24 Mar. 2017.

[24] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals prob- lem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, 1982.

[25] Narayanan, Arvind. "Arvind Narayanan On Twitter". Twitter. N.p., 2017. Web. 24 Mar. 2017.

[26] Observation: Use Of The Word Blockchain As An Uncountable Noun ("I'm Interested In Blockchain") Is A Predictor Of Technical Cluelessness • R/Bitcoin". reddit. N.p., 2016. Web. 24 Mar. 2017.

Jiayi Chen is a second-year student pursuing a B.S. in Computer Science at Columbia University in the City of New York. Her research interests include cryptography, anonymity networks, financial transaction systems, and cyber security.