CHAPTER 1

INTRODUCTION

A block chain is a distributed, append-only log of time-stamped records that is cryptographically protected from tampering and revision. In the eight years since block chains were first proposed, their use as publicly accessible and verifiable ledgers for online financial transactions has become widespread. This rapid adoption has largely been spurred by the success of Bitcoin, a digital currency that—owing to its decentralized and pseudonymous nature, support for complex financial instruments (enabled by a powerful, built-in scripting language), and capacity to facilitate fast and inexpensive transactions across the globe has proven to be a highly disruptive force in the finance and e-commerce sectors.

As Bitcoin and alternatives like Ethereal and Ripple continue to mature and grow in market value, it is becoming increasingly likely that block chains as a means to facilitate financial transactions are here to stay. Yet block chains represent far more than a mere monetary innovation, researchers and industry members alike are only just beginning to understand the true potential of blockchain-based distributed ledgers, with their strong integrity and availability guarantees and their ability to leverage community consensus to eschew centralized trusted curation.

Indeed, beyond the sorts of payment transactions for which blockchains are already widely deployed, potential applications for blockchains abound in areas as diverse as electronic voting, certificate authorities, the Internet of Things, and smart systems. Moreover, the past few years were marked by announcements from numerous companies—ranging from startups like R3 to established technology firms like IBM and financial institutions like Visa—about forthcoming products based on innovative blockchain designs that are specially tailored to meet organizational and business logic needs. The target applications for these products range from payment settlement through supply-chain management and beyond.

The ephemeral nature of users' pseudonymous identities in Bitcoin played a key role in its early success. However, eight years of intense scrutiny by privacy researchers has brought to bear an arsenal of powerful heuristics using which attackers can effectively link disparate Bitcoin transactions to a common user and, in many cases, to that user’s real-world identity.

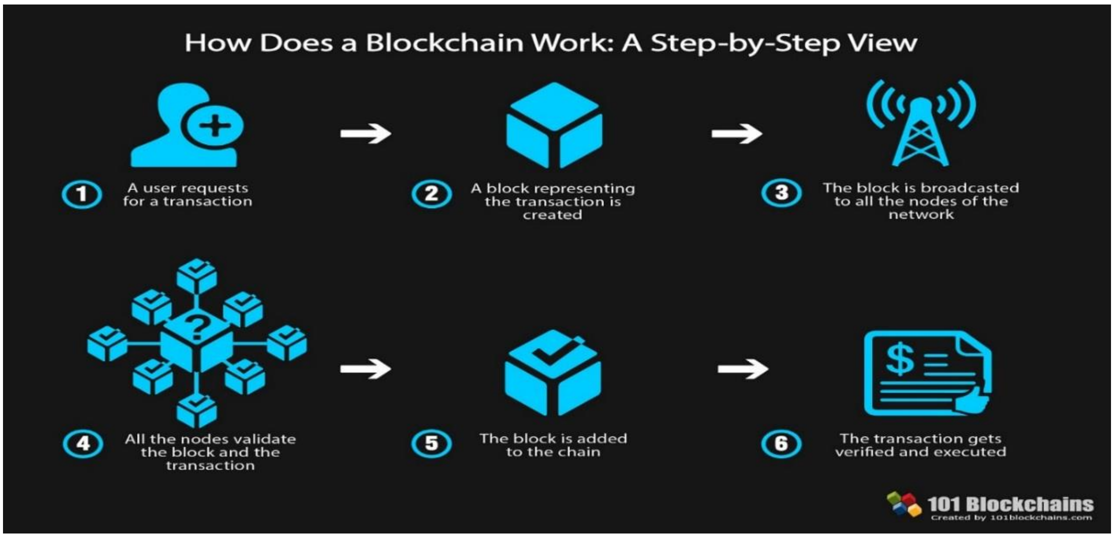
How Does a Blockchain Work: A Step-by-Step View
1 A user requests for a transaction
2 A block representing the transaction is created
3 The block is broadcasted to all the nodes of the network
4 All the nodes validate the block and the transaction
5 The block is added to the chain
6 The transaction gets verified and executed
101 Blockchains
Created by 101blockchains.com

Figure 1: - Working of Blockchain

Ultimately, instead of providing the bastion of privacy for financial transactions that its early adopters envisioned, Bitcoin and its altcoin brethren are in many ways less private than traditional banking, where government regulations mandate basic privacy protections. In an attempt to address this situation, the cryptography and privacy research communities have proposed and implemented several protocols aiming to improve blockchain privacy. These protocols all try to decouple users’ pseudonymous identities from the specific transactions they make, thereby frustrating attempts to link transacting parties based on data that appears in the blockchain. However, none of the proposed protocols attempts to hide the identities of users from network-level adversaries as the users publish or retrieve data from the blockchain. Instead, the proposed protocols “outsource” this crucial step, relying on an external anonymous communications network such as Tor.However, running complex protocols over general-purpose, low-latency anonymity networks such as Tor is fraught with risks and can expose users to subtle-yet-devastating DE anonymization attacks, thereby undermining the privacy guarantees of the entire blockchain system. It can do better!

`

CHAPTER 2

SYSTEM ARCHITECTURE

Most blockchains are, at their core, massively distributed and publicly accessible databases; therefore, beyond ensuring that the data they store does not, in and of itself, betray user privacy, any research program that seeks to fully address blockchain privacy must additionally consider (at the very least) privacy for two fundamental types of transactions: reading data from and writing data to a blockchain. In the context of cryptocurrencies like Bitcoin, the database represented by the blockchain is a publicly accessible and verifiable ledger of financial transactions.

Specifically, whenever a transaction occurs, the originating party publicly announces the transaction to a handful of selected entities, who then spread the details of that transaction throughout the network via a gossip protocol. The transaction is ultimately aggregated with several other (unrelated) transactions into a discrete block, which then gets irreversibly appended to a chain comprising all earlier blocks. The chain of blocks can—indeed, to obtain strong integrity and availability, must—be replicated and shared in its entirety among many nodes in a network, thereby providing each node with a global, eventually consistent view of every transaction that has ever taken place. New transactions are reflected in all replicas of the blockchain within some predefined expected time, which can range from a few seconds (for instance, in Ripple) to a few minutes (for instance, in Bitcoin). Each transaction is associated with a pair of pseudonyms (often called *wallets*), respectively identifying the sender and receiver of some digital assets.

Users can generate new pseudonymous wallets with which to receive digital assets arbitrarily and at will, it is considered a best practice for Bitcoin users to generate a fresh, ephemeral wallet whenever they wish to conduct a new transaction. The primary motivation for generating such ephemeral wallets is to protect user privacy by making it difficult for an attacker to link together the various transactions involving a given user by simply examining the sender and receiver pseudonyms appearing in transactions recorded in the ledger. However, as Bitcoin and related altcoins grow ever-more prevalent, there is a growing concern that the “privacy” offered by this approach is illusory at best.

Indeed, the past eight years of research into blockchain privacy has given rise to a veritable treasure trove of effective heuristics using which attackers can link Bitcoin transactions back to a common user, despite the widespread use of ephemeral wallets.

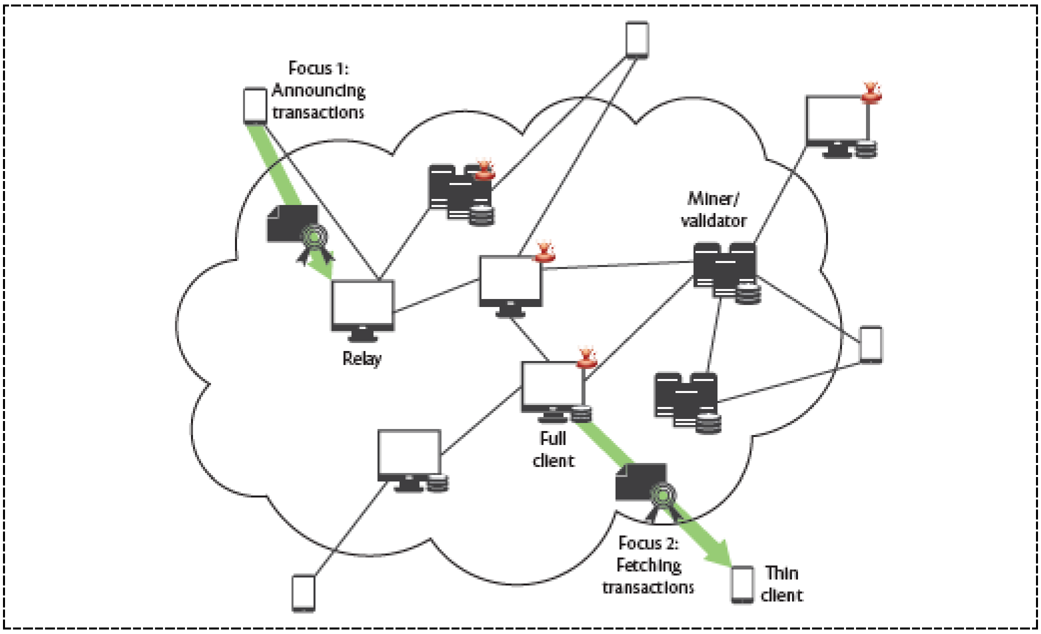

Figure 2. Topology of a typical blockchain system. The two bold arrows (highlighted in green) illustrate sensitive information flows that must be protected to prevent attackers from leveraging network-level information to compromise the privacy of blockchain users.

Figure 2 depicts a traditional blockchain architecture. (use the qualifier "traditional" here to differentiate the blockchain architectures we consider from those involving payment channels and other layer-2 applications, which introduce a host of new privacy concerns that are beyond the scope of this article.) For the purposes of this article, we focus on the two arrows that are bold and highlighted in green; specifically, we focus on the need for innovative mechanisms that allow users to

■ announce and publish transactions anonymously, a task for which the envision a tailor-made anonymity mechanism that is integrated directly into the blockchain architecture

■ fetch transactions privately, a task for which the envision using special private information retrieval (PIR) protocols designed and optimized to support efficient and expressive queries for transactions stored in a blockchain.

A handful of second-generation altcoins—including Zcash and Monero natively employ cryptographic techniques to prevent the contents of transaction on the blockchain from leaking private information about transacting parties. Likewise, the research literature contains several proposals that aim to Bitcoin, Ripple, and Ethereum blockchains. While such approaches are effective at protecting blockchain users against a subset of the DE anonymization heuristics that plague mainstream deployed blockchains, to emphasize that the existing approaches, so far, focus on preventing the data stored in a blockchain from leaking private information—they do nothing significant to mitigate against inferences that leverage network-level information (for example, IP addresses) or access patterns (for example, specific blocks or portions thereof) revealed when users interact with the blockchain data.As such, the existing proposals all fall far short of solving the blockchain privacy problem in its entirety.

CHAPTER 3

TECHNOLOGY USED

3.1 P2P Architecture

A Peer to Peer (abbreviated to P2P) network is a very important part of how blockchain technology works, and why it is so solid and secure. Here we will explore what is P2P and why it is such a vast improvement on the centralized systems we are familiar with today.

In a P2P network, the user utilizes and provides the foundation of the network at the same time, although providing the resources is entirely voluntary. Each peer (a "peer" being a computer system on the network) is considered equal and are commonly referred to as nodes. A peer makes a portion of computing resources such as disk storage, processing power or network bandwidth, directly available to other participants without the need for any central coordination by servers or stable hosts.

This method of transferring information is a huge improvement because data is not held in one centralized point, making it far less vulnerable to being hacked, exploited or lost.

No central point of storage means there is no need for a dominant authority and therefore no single party can control and use the network to push its own agenda. Instead, the user becomes the true owner of their personal data, as long as they secure it properly. This is a bold step away from the centralized systems of today, wherein a social network becomes the owner of all the data that the user uploads or a company that provides payment systems deciding when to access the own funds, reserving the right to freeze the money whenever they see fit.

The emergence of the P2P network and the central role it plays within blockchain technology could be seen as welcoming a new system of communication. With blockchain trust in all powerful third parties is no longer need as users can rather deal directly with one another across a secure and distributed and decentralized network.

3.2 Ethereum Blockchain

The structure of the ethereum blockchain is very similar to bitcoin's, in that it is a shared record of the entire transaction history. Every node on the network stores a copy of this history. The big difference with ethereum is that its nodes store the most recent state of each smart contract, in addition to all of the ether transactions

For each ethereum application, the network needs to keep track of the 'state', or the current information of all of these applications, including each user's balance, all the smart contract code and where it's all stored. Bitcoin uses unspent transaction outputs to track who has how much bitcoin. While it sounds more complex, the idea is fairly simple. Every time a bitcoin transaction is made, the network 'breaks' the total amount as if it was paper money, issuing back bitcoins in a way that makes the data behave similarly to physical coins or change.

To make future transactions, the bitcoin network must add up all pieces of change, which are classed as either 'spent' or 'unspent'. Ethereum, on the other hand, uses accounts. Like bank account funds, ether tokens appear in a wallet, and can be ported (so to speak) to another account.

3.3 CoinJoin

CoinJoin lets multiple users combine all inputs and outputs from several transactions into a single, big transaction. This single transaction spends bitcoins from different addresses to different addresses – and since none of the sending addresses pay none of the receiving addresses specifically; there's no link between any of them.

This can be compared to a group of people who throw their cash together and go shopping. While everyone could make sure no one spends more than they should, the shoppers wouldn't necessarily spend the exact bills they originally put into the shared wallet themselves.

In Bitcoin, this can be accomplished perfectly securely. All inputs require a corresponding signature from their respective owner, while the content of a transaction cannot be changed after a signature is added. As such, participants of a CoinJoin transaction simply announce which inputs and outputs they want to include in the transaction, and sign the aggregate only if these inputs and outputs are correctly included. Once all participants have signed (and only once they have signed), the transaction is broadcast.

A key feature of CoinJoin: once the transaction is broadcast and included on the blockchain, there is no way of knowing which bitcoins went where; not even the recipients of the transaction will know from which addresses they got paid. Additionally, CoinJoin improves privacy even of those who don't use it at all. Since a combination of inputs no longer necessarily means that all of the input-addresses belong to the same user, clustering has become a less powerful analytics tool in general.

3.4 Mix Coin:

MIX is an Ethereum blockchain. A blockchain is a shared database that has a built-in cryptocurrency that is used to financially incentivize the neutrality of the database. No-one can be in charge of a blockchain. The first blockchain was called Bitcoin. Pretty much the only thing in the Bitcoin database is how much Bitcoin each account has. Ethereum takes this concept much further. Computer programs called smart contracts can be uploaded into the blockchain and these programs can then store data in the database that everyone has a copy of.

Many big projects are deployed on the Ethereum blockchain. But this presents a problem. One must assume that every software project has fatal bugs that will need to be fixed once they are discovered. Bitcoin had fatal problems early on that needed to be fixed and so did Ethereum. Unfortunately, when the projects that are deployed on Ethereum need to be fixed they will have a very hard time because they will need to convince the entire blockchain to deploy their fix. This was the problem with The DAO crowdfunding project. An attacker stole $150m because of a bug in the smart contract. In attempting to fix this problem the Ethereum was split into two blockchains: Ethereum and Ethereum Classic.

The only purpose of the MIX blockchain is to run MIX. This means that whenever there is a problem that can only be fixed with a hard fork, it will not be difficult to convince the MIX community to adopt it. The cryptocurrency of the MIX blockchain is also called MIX.

3.5 Tumble Bit:

An unlinkable payment hub. To present Tumble Bit, a unidirectional unlinkable payment hub that uses an untrusted intermediary, the Tumbler T , to enhance anonymity. Every payment made via Tumble Bit is backed by bitcoins. We use cryptographic techniques to guarantee Tumbler T can neither violate anonymity, nor steal bitcoins, nor "print money" by issuing payments to itself. TumbleBit allows a payer Alice A to send fast off-block chain payments (of denomination one bitcoin) to a set of payees (B1, ..., BQ) of her choice. Because payments are performed off the blockchain, TumbleBit also serves to scale the volume and velocity of bitcoin-backed payments. Today, on-blockchain bitcoin transactions suffer a latency of ≈ 10 minutes. Meanwhile, TumbleBit payments are sent off-blockchain, via the Tumbler T , and complete in seconds. (Our implementation1 completed a payment in 1.2 seconds, on average, when T was in New York and A and B were in Boston.) TumbleBit Overview. TumbleBit replaces on blockchain payments with off-blockchain puzzle solving, where Alice A pays Bob B by providing B with the solution to a puzzle. The puzzle z is generated through interaction between B and T , and solved through an interaction between A and T . Each time a puzzle is solved, 1 bitcoin is transferred from Alice A to the Tumbler T and finally on to Bob B.

Bitcoin compatibility. TumbleBit is fully compatible with today's Bitcoin protocol. We developed (offblockchain) cryptographic protocols that work with the very limited set of (on-blockchain) instructions provided by today's Bitcoin scripts. Bitcoin scripts can only be used to perform two cryptographic operations: validate the preimage of a hash, or validate an ECDSA signature on a Bitcoin transaction. The limited functionality of Bitcoin scripts is likely here to stay; indeed, the recent "DAO" theft has highlighted the security risks of complex scripting functionalities. Moreover, the Bitcoin community is currently debating whether to deploy a solution ("segregated witnesses") that corrects Bitcoin's transaction malleability issue. TumbleBit, however, remains secure even if this solution is not deployed. No coordination. In contrast to earlier work, if Alice A wants to pay Bob B, she need not interact with any other TumbleBit users. Instead, A and B need only interact with the Tumbler and each other.

CHAPTER 4

IMLEMENTATION

By their very design, blockchain systems require extensive overlay networks through which participants announce transactions and agree on what transactions should ultimately appear on the blockchain. Thus, it seems natural to leverage the existing overlay structure to realize anonymous transaction publishing, rather than relying on an external service like Tor. We propose that blockchain privacy protocols should de-link users' network-level information from their transactions using mechanisms that piggyback on the overlay network that is already in place for announcing transactions.

The specifics of how such a mechanism might work vary, depending on the structure of the overlay network imposed by the consensus protocol—that is, depending on how participants decide which transactions qualify for inclusion in the blockchain. Proposed and deployed blockchains fall into two distinct categories based on the mechanism they use to build a consensus around what data to immortalize in the blockchain: permission less and permissioned. The blockchains underlying Bitcoin and Ethereum constitute two prominent examples of permissionless blockchains. As their name implies, permissionless blockchains place no restrictions on who participates in the consensus process.

Instead, unrestricted entities called miners collectively decide which blocks should be appended to the chain by providing an associated proof of work. In the case of Bitcoin, this proof of work takes the form of a "partial hash inversion," wherein the miners seek inputs that lead a cryptographic hash function to produce a digest whose numerical value does not exceed some global-parameter target. Such a permissionless consensus guarantees that only valid blocks get appended to the blockchain (approximately) under the assumption that more than half of all mining resources in the network are controlled by honest—or, at least, no colluding—entities.

The blockchains underlying Ripple and the Linux Foundation's Hyper ledger (https://www.hyperledger .org) are two prominent examples of permissioned blockchains. In contrast to permissionless blockchains, permissioned blockchains do place restrictions on who participates in the consensus process. A group of highly available entities (with strong identities) collectively decide which blocks should be appended to the chain by leveraging a Byzantine fault-tolerant atomic broadcast protocol. This approach allows permissioned blockchains to reach consensus very rapidly, requiring as little as a few seconds for each transaction to be reflected in the ledger.

The contrasting security assumptions and efficiency guarantees of permissionless and permissioned blockchains make them well suited to different use cases, and indeed, the two varieties are prospering together: traditionally structured organizations/consortiums are increasingly adopting permissioned blockchains, while peer-to-peer (P2P) solutions continue to leverage permissionless blockchains.

4.1 Publishing to Permissionless Blockchains

Permissionless blockchain systems (like Bitcoin and Ethereum) employ P2P networks of relays to propagate transactions and blockchain updates throughout the network using a best-effort gossip protocol. Such P2P networks typically experience considerable churn, with relays joining, leaving, and re-joining the network at will; however, the average number of relays in the network at any given time can remain relatively high.

For example, at the time of writing, the number of online relays in the Bitcoin network at any given time is about one-and-a-half times the number of Tor relays. As of 4 October 2017, Tor Metrics estimates about 6,300 Tor relays [https://metrics.torproject.org] versus the Bit node estimate of about 9,900 full Bitcoin nodes. One might, therefore, consider employing the elaborate Bitcoin communication infrastructure toward improving the anonymity of users' announcements. Given the P2P nature of the network, we believe it may be possible to leverage the existing academic research on P2P anonymous communications networks. For instance, such a solution could be based on Pisces,8 employing the social trust links to construct anonymous communication paths that are robust to compromise in the presence of route-capture attacks and Sybil nodes.

However, given the dynamic and open nature of permissionless blockchains such as Bitcoin, establishing trust in relays will be a prominent challenge. The Kovri project (https://www.getcorvi.org), an offshoot of the Monero and Bitcoin developers' recent interest in the Dandelion networking policies,9 clearly indicates the blockchain community's awareness of the problem; nevertheless, significant efforts are necessary going forward. In general, it will be an interesting challenge to analyze and establish security, privacy, and viability of P2P anonymous communications system over permissionless blockchain systems. Publishing to Permissioned Blockchains Permissioned blockchain systems (like Ripple, Corda [https://www.corda.net], and Hyperledger) employ a clique of highly available validator nodes for agreeing on transactions and blocks.

These nodes employ traditional asynchronous Byzantine-tolerant consensus protocols to append a block of transactions to the blockchain. Here, validators select valid transactions to be agreed on from those transactions forwarded by system users. As typically transactions from several users are added to any given block, a simple approach to provide anonymity here will be to perform all the communication between users and validators over an anonymous communications network. However, we advocate improving efficiency and reducing the overhead by combining the consensus process for agreeing on transactions with the process of mixing users' announcements.

This can be modeled as an asynchronous multiparty computation (AMPC) problem and can be solved using the generic AMPC techniques; however, we propose development of tailored solutions to further improve the efficiency. A possible tailored approach for agreeing on a randomly permuted set of transactions can involve combining Newton's identity method for power sums (as employed by Ruffing and colleagues5) with asynchronous verifiable secret sharing and asynchronous Byzantine consensus. Nevertheless, a key challenge will be to make these solutions scale well (possibly sublinearly) with the number of mixed transactions.

CHAPTER 5

APPLICATIONS

1. Financial Services:

Blockchain financial services are redefining the existing rails of our current financial markets infrastructure. Areas of this sector experiencing significant activity range from backend clearing and settlement, to global capital markets architecture. Distributed ledger systems in some of these cases do not need to be entirely decentralized, and several financial institutions are looking at creating their own "private block chains".

2. Government:

Blockchain Technology (also called Distributed Ledger Technology (DLT)) is a potential vehicle to improve government services and foster more transparent government-citizen relations. The distributed tech can work to dramatically optimize business processes through more efficient and secure data sharing.

3. Healthcare:

Blockchain Technology has the potential to disrupt the healthcare industry's centralized operations, opening the door for optimized business and service delivery. The Distributed Ledger Technology (DLT) is an innovation fertile with the possibility of improved transparency, security, and efficiency. Smart contracts on the block chain operate automatically without third-party personnel needed to verify documents or specific steps using pen-and-paper processes. With automation comes a reduction in the notorious bureaucracy that currently stands in the way of patients receiving the best care possible.

4. Identity:

Blockchain technology provides the ideal engine to power digital identities. While digital identities are emerging as an inevitable part of our connected world, how we secure our online information is coming under intense scrutiny. Block chains based identity systems can provide a solution to this issue with hardened cryptography and distributed ledgers.

5. Internet of Things (IoT):

Blockchain technology provides the ideal engine to power a fairly new concept regarding our new connected world: *Internet-of-Things*. Spending on the internet-of-things market is expected to top the $1 Trillion mark in the coming years. This opportunity is poised for Blockchain Internet-of-Things to step in and provide the ultimate system to track the unique histories of the billions of smart-devices coming online over the next few years.

6. Insurance:

Blockchain Insurance allows for the entire insurance industry to dramatically optimize business processes by sharing data in an efficient, secure, and transparent manner. Using block chain to revolutionize insurance policies shifts systems onto smart contracts operating autonomously on peer-to-peer networks, helping to phase out antiquated pen and paper processes and eliminate red tape the insurance industry is notoriously riddled with.

7. Money:

Cryptocurrencies provide people across the globe with instant, secure, and frictionless money, and blockchains provide the permanent record storage for their transactions. Prior systems required users to trust a central authority that the monetary supply and payment transfer will not be tampered with. Blockchain technologies obsolete this method of payment transfer by providing a trustless environment so that there is no longer a need to rely on a third-party to ensure your payment transfers, thus creating a Person-to-person(Peer-to-peer) environment.

8. Music:

Applying block chain technology to music applications allows for a paradigm shift in the way artists can control their musical work. From ownership rights, to royalty payments and first edition rights, block chain technology applications empower artists to extend ownership of their works.

9. Real Estate:

Blockchain technology will inevitably become a foundational pillar of the real estate industry. In a mostly paper-record based industry, block chain real estate allows for an unparalleled upgrade in how records are stored and recorded. Utilizing blockchain applications in essential functions such as payment, escrow, and title can also reduce fraud, increase financial privacy, speed up transactions, and internationalize markets.

10.Supply Chain:

Managing the modern, often global, supply chain is a series of intensive processes that require perfect orchestration between many moving parts and actors. Linking and creating the links to distribute goods and services looks much more like a web than a chain in our increasingly “smaller” global world.

CHAPTER 6

FUTURE SCOPE

1. **Blockchain in Digital Advertising:** Presently, digital advertising faces a lot of challenges like domain fraud, bot traffic, lack of transparency and long payment models, due to the issue like incentives are not affiliated. Because of this the promoters and publishers feel they are dropping the deal. Blockchain has provided a solution to carry transparency to the supply chain as it fetches trust in a trustless environment. Blockchain allows right companies to succeed, by decreasing the number of bad players in the supply chain. Publishers can also gather a vast percentage of the total advertisement dollars arriving the ecosystem. The Blockchain technology is still in its beginning; however, this technology should stay here, and all advertisement companies are observing that how blockchain will help to enhance their business.

2. **Blockchain in Cyber Security:** Though the blockchain is a public ledger, the data is verified and encrypted using innovative cryptography technology. In this manner, the information or data is less likely to be attacked or altered without authorization.

3. **Blockchain will remove the requirement of the third party:** With the help of Blockchain technology, basically, it is possible to impact a varied range of processes and techniques. It eliminates the need of trusted third party in the transactions. Well most prominent organizations in the world exist today to function as a trusted third party, for instance, SWIFT, and the Depository Trust Cleaning Company. Corporate chances flourish for companies that can build applied Blockchain technologies aiming for particular transactions, like the mortgage industry. The existing mortgages needed a complicated web of title searches, title insurance, and uncountable minor transaction fees which are required to keep the system running. These systems occur because traditionally, the transfer of land has been a process which requires a significant amount of belief in the old records. The Blockchain technology was going to address all these

concerns, and a particular property's ledger consists of a verifiable and validated transactions history, lowering the necessity of institutions to provide risk modification and trust services.

4. **Governments will provide their digital currencies:** It is confirmed that the paper money at its last phase, but it is also found that the authorized currency is facing a severe competition by cryptocurrencies. In 2017, it is observed that the price of Bitcoin has flown which was never seen by any single service or money all around the world. The currency is still one of the most appreciated properties available in the market, and the nation took notice, due to the price of Bitcoin is denied by the basic idea of demand and supply. The need for Bitcoin will again climb at some point, with a fixed limit of twenty-one million units of Bitcoin. Because of this, a few governments will get a chance to create their digital currencies to avoid dropping face to an independent and unregulated property and participate in an open market.

5. **Blockchain beyond the world of computing:** In 2017, the world had seen the infinite collection of options in the **use of blockchain technology**. Currently, most of the countries are developing their blockchain strategies to hold the future. Also, it is highly possible that the rest of the advanced European countries will follow suit by accepting the blockchain technology to create a constant financial environment that helps nations on ruins like Greece and Spain. There are specific problems associated with the security of finances, and Blockchain will be used to address these kinds of issues. Blockchain will also be used to generate registries which are used for medical purposes, to manage insurance policies, and to interrupt the model of useless data storage.

6. **Managing World trade with the help of Blockchain Technology:** Blockchain is valuable to business particularly how it makes easy for anybody to track the supply chain of everything provided using the technology. It will be outdated to track the numbers, and no company wants to lose a shipment because of human inability. Well, it is easy to register a cargo shipment in the Blockchain, this enables the parties involved in the job operation to follow the delivery procedure from point A to B. With the help of Blockchain technology, it is easy for the

custom agents to track down the forbidden products like fake medicines, changed food products, false clothes reproduction, fake auto parts, electronic apparatus and other piracy agents which are trying to provide the low-quality goods inside any country without talking about the internal laws.

7. **Supply chain Management:** With the help of blockchain technology, it is possible to document the transaction in an everlasting distributed record, and supervise the transactions more sturdily and transparently. This also helps to minimize human errors and time delays. It is also used monitor costs, employment, and releases at each point of the supply chain. But this has severe effect for understanding and monitoring the actual ecological impacts of products. Not only this the decentralized ledger can also be utilized to check the legitimacy or fair trade status of products by following them form their source.

8. **The Blockchain in Forecasting:** The blockchain technology is set to alter the complete methodology for research, consulting, analysis and forecasting. The global distributed prediction markets are created with the help of online platforms.

9. **Use of Blockchain in the Internet of Things and Networking:** Different companies like Samsung and IBM are utilizing the blockchain technology for a new concept called ADEPT, this will help to create a distributed network of IoT devices. The blockchain technology will remove the requirement for a central location to manage the communication between them; this will function as a public ledger for a massive number of devices. The devices may communicate with each other to upgrade the software, handle the errors and observe energy practice.

10. **Blockchain in cloud storage:** The data on a centralized server is exposed to hacking, loss of data, or human error. With the help of blockchain technology, it is possible to make the cloud storage more protected and robust against hacking.

CONCLUSION

The application of Blockchain technology is not limited only to the finance industry. It has a fantastic future in different sectors such as supply chain management, digital advertising, forecasting, cyber security, Internet of things, networking, etc. Blockchain technology also has a huge prospective to provide the new openings for occupation in the industry. It also enhances the professional's capability to upgrade themselves. With the help of Blockchain technology, it is possible to transform the whole world into a much smaller place. The transactional activities can be performed much faster and efficiently using Blockchain. Blockchain technology is going to be used in many more sectors in the future such as in government systems as these systems are slow, dense, and likely to corruption. Implementing Blockchain technology in government system can make their operations much more secure and efficient. It is useful to understand blockchains in the context of bitcoin, but you should not assume that all blockchain ecosystems need bitcoin mechanisms such as proof of work, longest chain rule, etc. Bitcoin is the first attempt at maintaining a decentralized, public ledger with no formal control or governance.

BIBLIOGRAPHY

1. M. Meiklejohn et al., “A Fistful of Bitcoins: Characterizing Payments among Men with No Names,” Communications of the ACM, vol. 59, no. 4, 2018, pp. 86–93; https://doi.org/10.1145/2896384.

2. P. Koshy, D. Koshy, and P.D. McDaniel, “An Analysis of Anonymity in Bitcoin Using P2P Network Traffic,” Proceedings of FC, LNCS 8437, 2019, pp. 469–485; https://doi.org/10.1007/978-3-662-45472-5_30.

3. E. Androulaki et al., “Evaluating User Privacy in Bitcoin,”Proceedings of FC, LNCS 7859, April 2019, pp. 34–51;https://doi.org/10.1007/978-3-642-39884-1_4.

4. E. Heilman et al., “TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub,” Proceedings of NDSS, 2017; https://doi.org/10.14722/ndss .2017.23086.

5. T. Ruffing, P. Moreno-Sanchez, and A. Kate, “P2P Mixing and Unlinkable Bitcoin Transactions,” Proceedings of NDSS, 2017; https://doi.org/10.14722/ndss.2017.

6. D. Das et al., “Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency—Choose Two,” Proceedings of IEEE S&P, 2018; https://eprint.iacr.org/2017/954.

7. A. Biryukov and I. Pustogarov, “Bitcoin over Tor Isn’t a Good Idea,” Proceedings of IEEE S&P, 2018

8. P. Mittal, M.K. Wright, and N. Borisov, “Pisces: Anonymous Communication Using Social Networks,”Proceedings of NDSS, 2013; https://arxiv.org/abs/1208.6326.