**CHAPTER 1**

**INTRODUCTION**

Blockchain is the fundamental technology underlying the emerging cryptocurrencies including Bitcoin. The key advantage of blockchain is widely considered to be decentralization, and it can help establish disintermediary peer to-peer (P2P) transactions, coordination, and cooperation in distributed systems without mutual trust and centralized control among individual nodes, based on such techniques as data encryption, time-stamping, distributed consensus algorithms, and economic incentive mechanisms. As such, blockchain can offer a novel solution to the long-standing problems of high operation costs, low efficiency and potential security risks of data storage in traditional centralized systems.

With the rapid development and popularization of Bitcoin and other cryptocurrencies in the recent years, blockchain research and applications have also been witnessed to showcase an unprecedented trend of explosive increase. In blockchain is widely recognized to be in position to become the fifth disruptive innovation of computing paradigm after mainframe, personal computer, Internet, and mobile/social networks. Blockchain can be considered as the next generation of cloud computing, and is expected to radically reshape the behaviour model of individuals and organizations, and thus realize the transition from the Internet of Information today to the future Internet of Value. The fast-growing trend of blockchain has attracted a wide spectrum of interests from governments, financial institutions, high-tech enterprises, and also the capital markets.

The history of blockchain can be traced back to the late 2008, when Bitcoin was first invented by a researcher with the pseudonym of “Nakamoto” posting in a cryptography mail group, an article entitled “Bitcoin: A peer-to-peer electronic cash systems.” Technically speaking, blockchain can be narrowly defined as a kind of decentralized shared ledger that uses chronological, encrypted and chained blocks to store verifiable and synchronized data (e.g., transactions, states, behaviours, decisions, etc.) across a P2P network.

Broadly speaking, blockchain can be viewed as a novel decentralized architecture and distributed computing paradigm, which stores data with encrypted chained blocks, verifies data with distributed consensus algorithms, guarantees security and privacy in data access and transmission with cryptography, and manipulates data with self-executed program scripts (i.e., smart contracts). Blockchain has many desirable features in both its technical and organizational aspects, which can be summarized as “true” and “decentralized autonomous organization (DAO)”. The former denotes trustable, reliable, usable, and efficient, while the latter denotes distributed and decentralized, autonomous, and automated, as well as organized and ordered.

More specifically, blockchain is a distributed shared ledger, in which the recording, verification, storage, maintenance, and transmission of blockchain data are all based on the distributed architecture, and the mutual trust among distributed nodes is established via mathematical algorithms instead of centralized third-party authorities. Transaction data is stored on the blockchain in the form of chained blocks with time stamps, which can endow blockchain data with a temporal dimension and in turn strong verifiability and traceability.

Various kinds of economic incentive mechanisms are designed so as to crowd-source the mining process of blockchain to large numbers of blockchain miners, so that these miners are willing to contribute their computing power and participate in verifying the data blocks in the distributed shared ledger, as well as compete in the consensus process with the aim of winning the opportunity of creating the next data block and appending it to the main chain. Blockchain can also be empowered by programmable chain-codes and scripts, so that users can create high-level smart contracts, cryptocurrencies, or other decentralized applications (DApps).

For instance, Ethereum (ETH) platform can offer Turing-complete script language and enable users to design any arbitrary smart contracts or transactions that can be precisely defined. Finally, blockchain data will be encrypted using asymmetric cryptography, and secured via the computing power collected from the consensus algorithms among large numbers of nodes in the distributed systems.

As such, blockchain can be considered as a secured framework against outside attacks, and thus ensuring strong unforgeability and untemperability. Blockchain is a novel and fundamental technical framework, and is expected to bring profound influence to the finance, economics, science and technology, and even politics areas. According to the development trend of blockchain technology, it is widely believed that blockchain will experience three types of application patterns, i.e., blockchain 1.0 featuring programmable cryptocurrencies, blockchain 2.0 featuring programmable financial systems, as well as blockchain 3.0 featuring programmable societies.

Bitcoin is one of the most successful application scenarios of blockchain so far. According to the latest statistics reported in the monitoring website Blockchain.info [8], more than 120 000 transactions, with $75 million transferred, were written into the Bitcoin blockchain ledger on daily average, and currently more than 500 000 blocks have been created. It is also reported by the website coinmarketcap.com that there are currently more than 1500 types of cryptocurrencies in the blockchain-powered markets with the total market cap of more than $500 billion, in which Bitcoin stands in the dominant position with a market cap accounting for more than 37% of the total, and the ETH and Ripple stand in the second and third places.

**CHAPTER 2**

**SYSTEM ARCHITECTURE**

The first block of Bitcoin blockchain, also known as, the genesis block, was created on January 4, 2009 by Nakamoto, who sent 10 bitcoins to a cryptographer Finney one week later. This is widely considered as the first transaction in the Bitcoin history. In May 2010, a programmer in Florida bought two pizzas worth $25 using 10 000 bitcoins, resulting in the initial exchange rate of Bitcoin to U.S. dollars. Since then, the price of Bitcoin raises rapidly, and peaked at $1242 each bitcoin, exceeding the price of gold, that is, $1241 per ounce at that time. It is estimated by Coin Desk that there are more than 60 000 of merchants in the world accepting Bitcoin transactions, and China is among the most fast-growing countries in Bitcoin transactions.

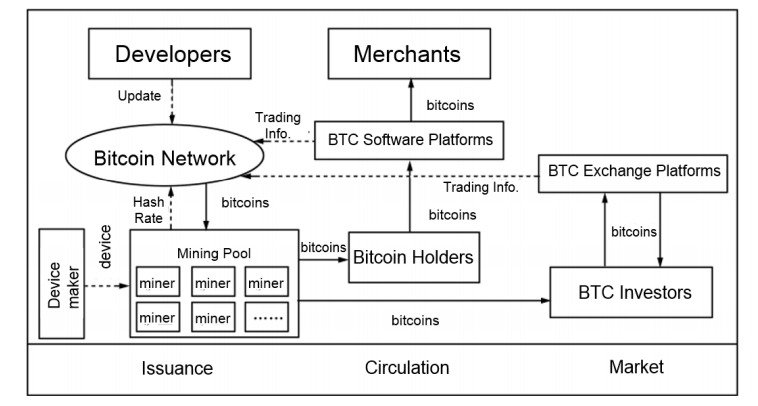


Fig 1: Bitcoin Ecosystem

Bitcoin is in essence an electronic cash generated in the distributed systems. The issuance of Bitcoin relies on a consensus competition among distributed network nodes, known as proof-of-work (PoW)-based mining, instead of a specific centralized authority. In the PoW-based consensus process, each and every computing node in the P2P network contributes its computing resource (CPU) and competes to solve a mathematically hard puzzle with dynamically adjustable difficulties.

More specifically, in each round of the consensus process, new Bitcoin transactions will be broadcasted to the P2P network. Each node keeps listening to the network, and adds the received transactions to a memory pool. Every node is competing to compute a nonce satisfying certain requirements. The miner who first successfully find such a correct nonce will win the consensus competition, and also win the right of creating the next new block. The winner will package transactions in the memory pool into a new block, partly according to a decreasing order of their associated transaction fees, and then broadcast this new block into the entire blockchain network.

The block will be accepted by other nodes if and only if the transactions in it is valid and not received before. Other nodes append this block into the main chain, and start the next round of consensus process competing for the right of packaging new transactions. In this process, the Bitcoin system will generate a specific amount of bitcoins as a reward to the winning miner, and also as an incentive to encourage other miners to continue contribute their computing power. The circulation process of Bitcoin will be secured by cryptography, with each Bitcoin transaction being hashed, encrypted and written into blockchain ledger after validation from all miners.

The transaction can be programmed and controlled by algorithm-driven scripts and non-Turing complete smart contracts, so as to realize the programmable and automatic circulation for Bitcoin. Bitcoin blockchain typically has the following five key components, i.e., a public shared blockchain ledger, a distributed P2P networking system, a decentralized consensus algorithm, a well-designed economic incentive mechanism, and programmable smart contracts. Bitcoin, like most other cryptocurrencies, is a self-contained ecosystem consisting of the issuance, circulation and the exchange market of bitcoins.

In the issuance part, the Bitcoin network is maintained and updated by the developers, and the network receives hash-based computing power from the mining pool or individual miners, and generates bitcoins as rewards to these miners. The miners can participate in the mining process individually, and can also cooperate by joining the mining pool so as to increase the possibility of successfully creating a block. The device maker produces and sells mining computers to the miners.

In the circulation part, Bitcoin holders or users buy specific types of goods or services from the merchants via the Bitcoin software platforms, such as Bitcoin wallets. The trading information will be broadcast to the Bitcoin network and also validated by the miners. In the exchange market part, since Bitcoin price fluctuates frequently, which results in a good investment opportunity for the investors. So buying and selling of bitcoins from the Bitcoin exchange platform, and the trading information will also be broadcast to the Bitcoin network, and validated by the miners. Inspired by the great success of Bitcoin, thousands of other blockchain-powered cryptocurrencies emerge and develop rapidly in this novel market.

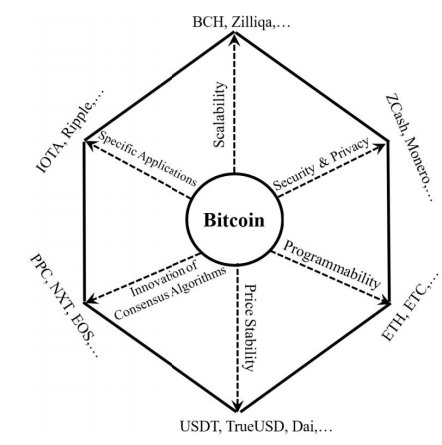


Fig 2: Six dimensions in cryptocurrency innovation.

Most of these cryptocurrencies, also known as altcoins, are invented with the aim of improving the performance of the Bitcoin system. Currently, there are six major dimensions and directions in the innovation of altcoins. The first dimension focuses on the scalability. For instance, Bitcoin cash, forked from the Bitcoin blockchain, extends the block size from 1 to 8 MB. This allows more transactions packaged into a single block in each round of consensus competition, and thus results in improved capability of transaction processing and reduced time in transaction confirmation.

Zilliqa can improve the throughput using the network sharing technique, which can automatically divide the blockchain network into multiple shards that validate transactions in parallel. The second dimension aims to improve the security and privacy protection with cryptographic techniques including zero-knowledge proof and homomorphic encryption. Examples include ZCash (ZEC) and Monero (XMR), among others. The third dimension is enhancing the programmability of blockchain systems, and the most well-known example is ETH, which supports Turing complete smart contracts and in turn DApps.

The fourth dimension is targeted at the price stability. For instance, USDT and other Tether currencies are endorsed by and equivalent in value to U.S. dollar, and can help facilitate the transfer of national currencies, provide users with a stable alternative to Bitcoin. The fifth dimension is based on the innovation of consensus algorithms, such as Peer Coin and EOS.The sixth type of crypt-currencies are devoted to specific application scenarios, such as the IOTA oriented to Internet of Things, Ripple used for global financial settlement, as well as Augur created for prediction market applications.

Although blockchain has imposed significant impacts on cryptocurrency, finance, and even socio-economic activities, it is not a new technology invented from scratch. Actually, blockchain can be considered as an ensemble innovation combining a group of extant technologies in cryptography, economics, and computer sciences fields. A six-layer reference model for characterizing and standardizing the typical architecture and major components of blockchain systems, and discuss the key techniques in each layer. Similarly, as the well-known open system interconnection reference model of the Internet, a complete blockchain system can also be decoupled into six layers stacked.

* Data Layer

This layer provides the key techniques for manipulating a variety of data collected from cyber, physical, and social. Reference model of blockchain. spaces. These data will be bundled into chained blocks, stored on all the full nodes in the blockchain network using the data structure of asymmetrically encrypted, hashed, and time-stamped Merkle trees. More specifically, each node, once winning the consensus competition, will be empowered to package all data generated in the period of the competition into a new block with a time-stamp indicating its creating time.

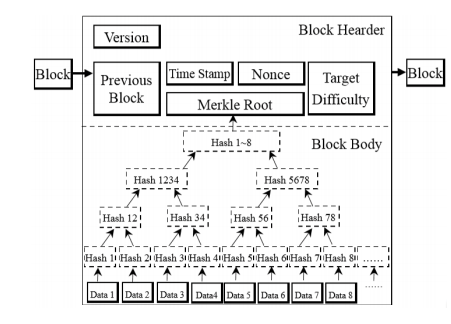


Fig 3: Data layer of blockchain

If there are conflicting data such as Bitcoin’s double spending, only one agreed version to all or a majority of nodes will be selected and appended into the block. A typical Bitcoin block consists of a header and a body part. The former contains all the meta-information while the latter stores a Merkle tree of verified and hashed data (e.g., via double SHA256 algorithm). The blocks are chained one by one in chronological order, forming the entire history from the genesis block to the newly generated one. In this layer, Merkle tree and time stamp can be considered as two important components for the blockchain ledger. The former helps realize rapid, efficient, and secured verification of the existence and integrity of blockchain data, while the latter enables the traceability and precise positioning of blockchain data. As such, blockchain is expected to be widely used in time sensitive application scenarios. More importantly, time-stamp has the potential of endowing blockchain data with a time dimension, and thus makes it possible to recur the past data history.

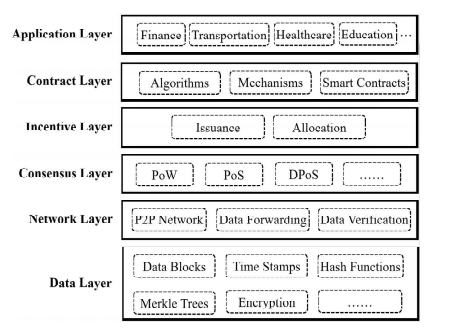


Fig 3: Reference model of blockchain

* Network Layer

This layer specifies the decentralized communication models and the related mechanisms of distributed networking, data forwarding, and verification. In most cases, blockchain application scenarios involves an open and dynamic environment with large number of distributed and connected devices or vehicles. The blockchain focuses on the important part of decentralized environments that can be topologically modelled as P2P networks. All participating nodes in the network are equally privileged without central authorities or middle-mans, so that the blockchain system is under decentralized, emergent, and bottom-up control. These nodes keep listening to the network, verifying the broadcasted data or blocks according to predefined check lists. Invalid blocks will be discarded and others will be forwarded to neighbouring nodes. This way, only one block accepted by the majority will be appended into blockchain. It is worth noting that this P2P-based decentralized network makes blockchain a potential architecture for the next generation of cloud computing. Blockchain data is stored on each and every node, and can be synchronized and restored even in the worst case of failure in all but one nodes. This evolves the cloud model with multiple central servers to a completely decentralized model, which is particularly useful in communication and interaction among decentralized entities.

* Consensus Layer

Blockchain uses a variety of consensus algorithms to guarantee the data consistency and the fault-tolerant ability of the shared ledger among distributed nodes. Traditional application scenarios typically are relatively closed ecosystems with entities trusting in each other, where early algorithms such as PAXOS might be sufficient to reach consensus efficiently. Blockchain models, however, mainly focus on open and dynamic environments with a large number of trust less entities with possible Byzantine failures, so that more complex algorithms are needed, such as practical Byzantine fault tolerance for semi open environments and proof-of-X (POX) type consensus for open environments. For instance, PoW is the most widely used algorithm, which asks nodes to compete repeatedly to do a mathematically difficult computation to validate the data. The winning node will be allowed to append its block on the ledger; proof-of-stake (PoS) requires the node with the largest amount of predefined stakes to create the new block; Other POX algorithms include delegated PoS (DPoS), proof-of-movement. Among all POX algorithms, no compute-intensive algorithms such as PoS and DPoS are particularly suitable for most lightweight systems in blockchain ecosystems.

* Incentive Layer

This layer incorporates economic rewards into blockchain systems. In essence, the data verification and block creation process driven by consensus competitions can be considered as a crowdsourcing task to participating nodes that contribute their computing power. These nodes are actually self-interested agents, so that incentive compatible mechanisms must be designed to make individual behaviour of revenue maximization aligned with the system-wide target of guaranteeing a secured and trusted ecosystem. Toward this end, cryptocurrencies such as Bitcoin and ETH can serve as a natural form as motivating reward. Its issuance mechanism is simple once a new block is created, a certain amount of cryptocurrencies will be issued as reward and allocated to the winning node to motivate the entire network continuing their efforts in data verification and block creation. This incentive layer is a key component and the main driving force for blockchain, especially for those based on public block chains. It cannot only serve as the engine for powering blockchain, but also establish an imbedded, cryptocurrency-based financial system in blockchain, so that disintermediated trading and real-time micro-payment can be easily supported. It is worth noting that, however, this layer is optional for some partially centralized blockchain applications, typically called private blockchain for closed environments and consortium blockchain for semi open scenarios, where trusted entities participate mandatorily without payment and financial requirements.

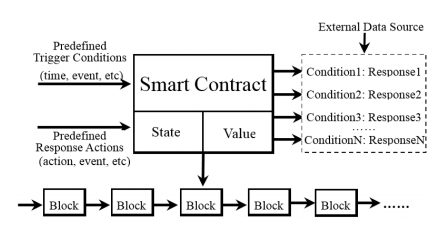


Fig4: Blockchain-enabled smart contracts.

* Contract Layer

In this layer, various smart contracts, mechanisms, and algorithms are packaged, and can serve as the high-level business logics to activate the static data, money, or assets stored on blockchain. Smart contracts can be narrowly defined as a group of self-verifying, self-executing and self-enforcing state response rules that are stored and secured by the blockchain. Once a group of parties consent to a set of predefined terms or rules, they can codify them as a smart contract, cryptographically sign it, and broadcast it to the P2P network for verification. The verified contract will be packaged into a block on the ledger. Once one or more preconditions are triggered, the stipulations and associated actions will be activated and self-executed without human interventions. This self-execution feature has the potential of transforming physical or digital assets into smart properties, which can be controlled and managed in an automatic and programmable fashion, thus significantly reducing the social complexity.

* Application Layer

This layer packages all possible application scenarios and use cases of blockchain. Although blockchain technology is still in its infancy, it has witnessed a tremendous growth in recent years in both research and industrial applications.

**CHAPTER 3**

**TECHNOLOGY USED**

Cryptocurrency

A cryptocurrency (or crypto currency) is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets.

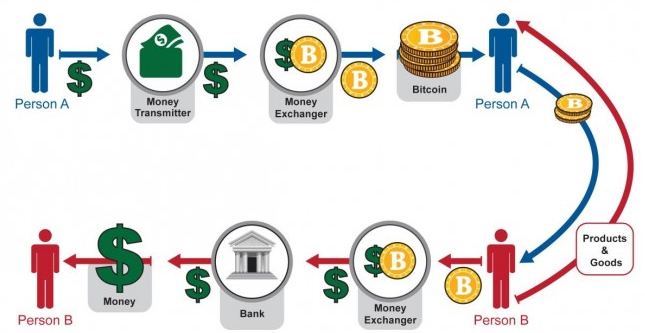


Fig 5: Working of cryptocurrency

A cryptocurrency has a ledger, where all transactions are made public so that total visibility is provided. Having a ledger forces everyone to "play fair" and takes away the risk of double spending. The ledger is a list of entries in a database that nobody can change without fulfilling specific conditions. Nobody owns the ledger or the cryptocurrency blockchain; instead, it’s decentralized meaning self-run and self-governed without the interference of outside parties.

Cryptocurrency Miners verify the transactions and then add them to the public ledger. It use powerful computers to solve complex math problems that are the key to the verification process. Cryptocurrency Mining is open source, so anyone can confirm a transaction, and the first miner to solve the problem gets to add a block to their transaction ledger.

Cryptocurrencies are systems that allow for the secure payments of online transactions that are denominated in terms of a virtual "token," representing ledger entries internal to the system itself. "Crypto" refers to the fact that various encryption algorithms and cryptographic techniques, such as elliptical curve encryption, public-private key pairs, and hashing functions, are employed.

he first cryptocurrency to capture the public imagination was Bitcoin, which was launched in 2009 by an individual or group known under the pseudonym, Satoshi Nakamoto. As of February 2019, there were over 17.53 million bitcoins in circulation with a total market value of around $63 billion (although the market price of bitcoin can fluctuate quite a bit). Bitcoin's success has spawned a number of competing cryptocurrencies, known as "altcoins" such as Litecoin Namecoinand Peercoin, as well as Ethereum, EOS, and Cardano. Today, there are literally thousands of cryptocurrencies in existence, with an aggregate market value of over $120 billion.

Cryptocurrencies hold the promise of making it easier to transfer funds directly between two parties in a transaction, without the need for a trusted third party such as a bank or credit card company; these transfers are facilitated through the use of public keys and private keys for security purposes. In modern cryptocurrency systems, a user's "wallet" or account address, has the public key, and the private key is used to sign transactions. Fund transfers are done with minimal processing fees, allowing users to avoid the steep fees charged by most banks and financial institutions for wire transfers.

Central to the appeal and function of Bitcoin is the blockchain technology it uses to store an online ledger of all the transactions that have ever been conducted using bitcoins, providing a data structure for this ledger that is exposed to a limited threat from hackers and can be copied across all computers running Bitcoin software. Every new block generated must be verified by the ledgers of each user on the market, making it almost impossible to forge transaction histories. Many experts see this blockchain as having important uses in technologies such as online voting and crowdfunding, and major financial institutions such as JPMorgan Chase see potential in cryptocurrencies to lower transaction costs by making payment processing more efficient. However, because cryptocurrencies are virtual and do not have a central repository, a digital cryptocurrency balance can be wiped out by a computer crash if a backup copy of the holdings does not exist, or if somebody simply loses their private keys.

At the same time, there is no central authority, government, or corporation that has access to your funds or your personal information.

The semi-anonymous nature of cryptocurrency transactions makes them well-suited for a host of nefarious activities, such as money laundering and tax evasion. However, cryptocurrency advocates often value the anonymity highly. Some cryptocurrencies are more private than others. Bitcoin, for instance, is a relatively poor choice for conducting illegal business online, and forensic analysis of bitcoin transactions has led authorities to arrest and prosecute criminals. More privacy-oriented coins do exist, such as Dash, ZCash, or Monero which are far more difficult to trace.

Since prices are based on supply and demand, the rate at which a cryptocurrency can be exchanged for another currency can fluctuate widely. However, plenty of research has been undertaken to identify the fundamental price drivers of cryptocurrencies. Bitcoin has indeed experienced some rapid surges and collapses in value, reaching as high as $19,000 per bitcoin in December of 2017 before returning to around $7,000 in the following months. Cryptocurrencies are thus considered by some economists to be a short-lived fad or speculative bubble. There is concern especially that the currency units, such as bitcoins, are not rooted in any material goods. Some research has identified that the cost of producing a bitcoin, which takes an increasingly large amount of energy, is directly related to its market price.

Cryptocurrencies' blockchains are secure, but other aspects of a cryptocurrency ecosystem are not immune to the threat of hacking. In Bitcoin's 10-year history, several online exchanges have been the subject of hacking and theft, sometimes with millions of dollars’ worth of 'coins' stolen. Still, many observers look at cryptocurrencies as hope that a currency can exist that preserves value, facilitates exchange, is more transportable than hard metals, and is outside the influence of central banks and governments.

**CHAPTER 4**

**IMLEMENTATION**

Blockchain-Powered Smart

Devices Blockchain, when integrated with smart contracts and Internet of Things (IoT) technologies, has the potential of transforming devices into automatic “smart properties,” and in the future establishing an ecosystem and economy of autonomous agents. Three levels of intelligence, namely data-level, individual-level, and social-level intelligence, may emerge in the life-time management and control of devices or vehicles. First, the data-level intelligence basically takes advantages of the techniques in the data layer, and helps maintain a globally shared and secured ledger. The data in life-time events including manufacturing, registration, sales, leasing, maintenance, and insurance, as well as real-time sensor data including position, speed, and mileage, can be perceived and recorded in the blockchain ledger and synchronized to all stakeholders.

This can radically reduce costs in device management, for instance, for used car sale and leasing industries. Second, mobile devices or vehicles, especially driverless cars or drones, may become autonomous and adaptive agents that possess individual intelligence, and interact and trade with other devices without intermediation. The cyber driver manages, controls, and even own a physical vehicle, constituting a parallel driverless vehicle . Also, the cryptocurrency in the incentive layer makes it possible for vehicles to trade and pay for services such as self-parking, tolls, Wi-Fi hotspots, radars, laser rangefinders, among others. Using blockchain based E-wallets, vehicles can send and receive bitcoin-like cryptocurrencies in a disintermediated fashion, and maximize its revenue on behalf of its human owner, or even itself.

Third, in the consensus and network layers, the P2P consensus-based control makes it possible to apply blockchain idea in swarm robotic systems with social intelligence. Generally speaking, one of the striking features of swarm robots is lacking of global knowledge, explicit communication models and central authorities, and relying on local communication among neighbouring robots. Using blockchain, the globally shared ledger can serve as a good solution to decentralized control problem.

The robots, such as a fleet of unmanned vehicles, vessels, or drones, can reach a decentralized consensus by competing for the right of encapsulating their beliefs, desires, or intentions in blocks on the shared ledger, using specific consensus algorithms ranging from the inefficient but secured PoW to the simple majority voting. Meanwhile, the self-executing smart contracts agreed among robots can help reduce the social complexity caused by human interventions to the systems, and thus evolve the swarm system from a complex Merton system to a predictable and tractable Newton system. This blockchain-based swarm robotics idea is particularly effective for dynamic and open systems, and can help realize the so-called device democracy and decentralized robot autonomy.

Decentralized Sharing Economy

Blockchain can serve as a key enabling technology for the next generation of sharing economy. Although representing an important step toward economic disintermediation, most of sharing economy applications including Uber and Lyft are essentially centralized with online platforms serving as middle-mans, resulting in unsatisfactory centralized decisions or risks such as surge pricing and privacy leaks. Blockchain-powered sharing economy can be considered as a completely decentralized and disintermediated model, which offers secured, immutable, and P2P-stored shared ledgers for all those transactions, representing the future shared economy 2.0.

One of the most successful application scenarios, so far, is real-time ride-sharing. As illustrated in, Lazooz, widely publicized as the blockchain version of Uber, aims to build an open-source, worldwide, and decentralized social transportation network. Lazooz enables private car owners to share their empty seats with others traveling the same route. The underlying operation mechanism of Lazooz basically follows our six-layer blockchain model. Any device running the DApp of Lazooz, e.g., smartphones, wearable devices, and computers of its community of users, can be registered as a “road miner” in the Lazooz blockchain network.

The real-time data generated in the network will be verified and stored in a community-maintained crypto-ledger, through which all ridesharing behaviour, schedules, and payments are coordinated and executed (the data layer). Road miners are interconnected in a P2P fashion without any central authority (the network layer). Rather than the commonly used consensus algorithms such as PoW, PoS, and DPoS, Lazooz designed a novel consensus algorithm called “proof-of-movement,” which encourages road miners to drive with Lazooz’s DApp running on their devices. This way, road miners can contribute to the community by sharing their data along the way and helping Lazooz weave the local social transportation Web (the consensus layer).

As reward, Lazooz automatically generates new tokens called zooz to road miners, and these tokens can be used to pay for ride-sharing and other transportation services (the incentive layer). Furthermore, various algorithms are designed and integrated into Lazooz’s DApp. These algorithms can be used to make specific decisions without human intervention, e.g., detecting the usage rate of specific geographic region and activating the service in the region where the number of active users exceeds the “critical mass,” and so on (the contract layer). Lazooz can be viewed as a decentralized, self-managed DAO.

Its formal decisions are collectively made by the community according to each user’s weight, which represents the user’s contribution to the community and will be updated via public voting process. Lazooz, together with Arcade City and other companies with the similar business model, represent the future trend of blockchain-enabled social transportation and will reshape the sharing economy.

Blockchain-Powered Freight Transportation

Freight transportation, especially the global shipping industry, plays a vital role in modern transportation systems and international economy, many long-standing problems, especially the undesirable operational costs, efficiency, and data interoperability, remain open in this area. Blockchain can serve as a potential solution to tackling these problems. Using blockchain, service providers can create a permanent digital shared ledger of transactions, on which a distributed network of stakeholders can communicate and coordinate with each other according to unified standards and procedures.

Designated parties can cryptographically add record to and retrieve data from the ledger using any devices including mobile phones, tablets, and personal computers, eliminating the need for costly and proprietary infrastructure and radically reducing the complexities. the blockchain-based solution has the potential of evolving traditional freight transportation to better track orders and assets, reduce errors and frauds, increase operational transparency, and offer greater security.

As an illustrative example, introducing a Block freight, a start-up aiming at designing open-source, immutable, and distributed end-to-end blockchain solution specifically for the shipping industry. Technically, the primary payload of transactions is the important commercial documents including electronic bill of landings, stored using the Interplanetary File System protocol.

The blockchain network runs with the P2P gossip protocol for broadcasting and transmitting unconfirmed transactions, which will be validated using the Tender mint consensus. Block freight issues tradeable tokens, typically worth $1 each, to be used to pay for the transaction and network fees and eliminate spam on the decentralized systems. Finally, in the contract layer, customers can use smart contracts to permanently and securely define the bill of lading, payment terms, and other elements to a completed cargo shipment, built on the ETH blockchain.

Blockchain-Based Enterprise Management and Knowledge Automation

Blockchain, together with blockchain-powered smart contracts, have the potential of reshaping traditional enterprise management process, especially in its knowledge automation workflows including modelling, validation, integration, and implementation. Knowledge automation can be considered as a novel research direction for further development of artificial intelligence technology, and also a general framework for dealing with management of complex business processes.

The goal of knowledge automation is from UDC to AFC, that is, dealing with complex management issues of uncertainty, diversity, and complexity with capacity of agility, focus, and convergence. More specifically, blockchain can be integrated into enterprise business process in the following aspects. First, blockchain-powered smart contracts can help automate the rules and regulations predefined by enterprise managers, so as to reduce the operation costs and the human intervention. Second, internal tokens or coins can be designed and issued as incentives to help improve the employees’ performance. Third, enterprise data can be stored in a decentralized and secured fashion, and validated using a consortium blockchain by all departments in the enterprise. Finally, employees can cooperate with each other on a specific task, forming various DAOs. This can help flatten the organization structure, and improve the management efficiency and effectiveness.

**CHAPTER 5**

**APPLICATIONS**

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”.

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.

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.

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.

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.

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.

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.

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.

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.

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**

As fundamental technologies with transformative potentials, blockchain and cryptocurrencies have found a wide spectrum of application scenarios in various types of industries, ranging from the underlying techniques of data storage, encryption, and verification, to the middle level of finance and asset management, and to a variety of high-level business models. In this paper, we present the technical details of Bitcoin and other cryptocurrencies, propose a six-layer reference model for the blockchain framework, and discuss several potential application scenarios. The main aim of this paper is to stimulate more detailed investigation and innovative research in this new direction.

Cryptocurrencies such as BitCoin still have numerous significant obstacles to overcome before they could totally replace current currency systems. The most immediate is the simple opposition from existing financial institutions, which wield great power and have incentives to discourage the proliferation of cryptocurrencies. Other large corporations, even when amenable to the idea of cryptocurrencies, do not currently consider them stable enough to keep as assets for long periods of time

In addition to battling the current economic system, cryptocurrencies have some internal challenges to overcome. Attempting to convert the entire world financial system to the BitCoin model, for example, could cause such a massive growth in blockchain size that the distributed ledger model would become impractical. It is also still unclear whether blockchain technology could be successfully adapted to use cases which require very high speeds with high volumes (on the order of seconds instead of hours), and would be poorly suited for any application which required some degree of reversibility. Finally, because of the substantial energy costs and diminished rewards over time associated with the "mining" process, users may eventually be forced to bear increasingly high and unreasonable transaction costs.

**BIBLIOGRAPHY**

[1] A Privacy-Aware PKI System Based on ermissioned BlockchainsRong Wang; Juan He; Can Liu; Qi Li ; Wei-Tek Tsai ; Enyan Deng 2018

[2] Understanding Blockchain Technology: Abstracting the Blockchain**,**Morgen Peck,Year:2018  
[3] A Blockchain-based key Management Scheme for Named Data Networking Junjun Lou ; Qichao Zhang ; Zhuyun Qi ; Kai Lei 2018

[4]Detection of Blockchain Transactions Used in Blockchain Mixer of Coin Join Type Artem A Maksutov ; Maxim S. Alexeev ; Natalia O. Fedorova ; Daniil A. Andreev 2019

[5] Y. Yuan and F.-Y. Wang, “Blockchain: The state of the art and future trends,” Acta Automatica Sinica, vol. 42, no. 4, pp. 481–494, 2016.

[6] Y. Yuan and F.-Y. Wang, “Towards blockchain-based intelligent transportation systems,” in Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC), Rio de Janeiro, Brazil, 2016, pp. 2663–2668.

[7] F.-Y. Wang, “Blockchain intelligence: Cornerstone of the future smart economy and smart societies,” in Proc. 2nd World Intell. Congr., Tianjin, China, 2018.

[8] Blockchain Monitoring Website. Accessed: Jan. 8, 2016.

[9] Cryptocurrency Monitoring Website. Accessed: Nov. 24, 2015

[10] World Economic Forum Survey. Accessed: Feb. 21, 2016.

[11] CoinDesk Report. Accessed: Feb. 21, 2016.

[12] N. Modiri, “The ISO reference model entities,” IEEE Netw. Mag., vol. 5, no. 4, pp. 24–33, Jul. 2017.