BLOCKCHAIN: IT'S STRUCTURE, PRINCIPLES, APPLICATIONS AND FORESEEN ISSUES.

[1]Amos K. Kibet, [2]Demeke G. Bayyou, [3] Rosanna A. Esquivel

[1]Angeles University Foundation, [2] AMA University, 3Angeles University Foundation
[1]Graduate School,
[1]Angeles University Foundation, Angeles City, Pampanga, Philippines

Abstract: Blockchain technology is considerd as the fifth disruptive innovation that has the potential to advance cybersecurity. This technology has recently received comprehensive attention because of its impact on cryptocurrency for enabling decentralized and unchangeable transactions. With the passage of time, it has become obvious that blockchain as technology is influencing the digital market arena through different applications. Although blockchain is most frequently adopted in banking and finance, there are many areas of Blockchain-based applications, including reputation systems, IoT and others. This paper discusses the many domain applications in which blockchain has had an impact. First, we provide an overview of the structural design of blockchain and compare some typical consensus algorithms for various types of blockchains. We examine every general blockchain principle that has brought all the key innovations into practice and finally we will be discussing the foreseen issues that will affect the implementation of blockchain in our current infrastructure and the challenges that blockchain will face.

Index Terms **- Blockchain; smart contract; consensus mechanism; Etherium and internet of things.**

I. INTRODUCTION

Due the continuous development of cryptocurrencies, the potential of the blockchain has gradually been discovered and has gained considerable attention in recent years. The blockchain technology, which is also known as distributed secure ledger technology, is a time-series data block that is interconnected to form a chain structure embedded with cryptography and the distributed ledgers. Broadly speaking, blockchain technology uses blockchain data structures to validate and store data; distributed consistent algorithms to generate and update data; encryption to ensure data transfer and access security; and automated scripting code to form a new distributed infrastructure and computing paradigm associated with smart contract **[1].**

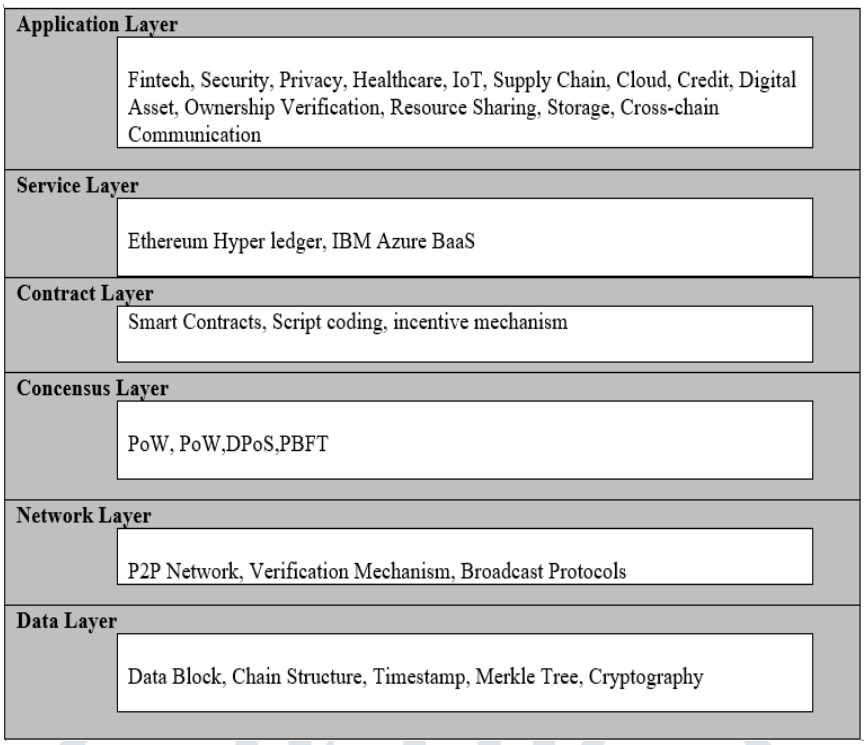
The technological innovation of blockchain includes the concept of blockchain technology and also the structure of an ecological blockchain system **[2].** Blockchain is now not limited to tokens used in crypto-currencies but also has potential for IoT, Industry **[3].** Governance, security and privacy, healthcare, cloud computing, big data and smart cities transportation system. The blockchain technology typically has key principles of decentralization, persistence, anonymity and auditability.With these features; blockchain may greatly save costs and improve efficiency.

In this paper, we describe and explain detailed fundamentals of blockchain infrastructure and architecture, features and Principles. We do deep exploration on Blockchain application areas. We also discuss industry survey expectation of blockchain and finally we address and discuss open issues and future research in blockchain.

II. BLOCKCHAIN ARCHITECTURE AND ALGORITHMS USED

Blockchain technology is not a single technical subject, but integration of encryption, theoretical physics, communication networks and other techniques are integrated **[4].**The blockchain architecture is divided into six layers which is shown in Fig. 1. The data layer, the network layer, the consensus layer, the contract layer, the service layer, and the application layer. The data layer and the network layer considered as lower level that create, validate and store data. The upper level is at the top of the architecture, including the service and application platform **[5].**The consensus and contract layers are the middleman between the lower and the upper level. The consensus layer consists mainly of Proof of Work(PoW), Proof of Stake(PoS), Delegated proof of stake (DpoS) and Proof of Byzantine Fault Tolerance (PBFT). The contract layer involves an intelligent contract, a consensus directive and an incentive mechanism.

Figure 1: The architecture of Blockchain.



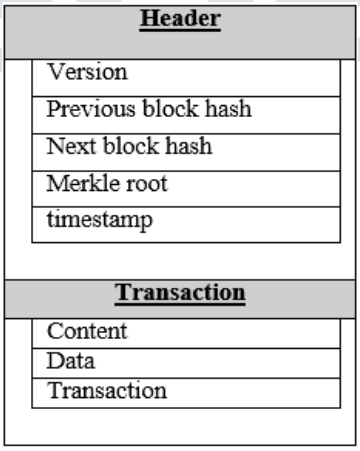
Data layer

Data layer is responsible for receiving and storing raw data and it contains Data Block, Chain Structure, Timestamp, Merkle Tree and Cryptography.

Data block: The data block is a metadata framework used to archive interactive data and information, in which the raw data must be further sifted for block storage. The data block does not indicate the preceding data and consequent data in the data structure clearly and uses only the interactive public key and signature, each interaction is therefore independent of each other, forming a chained relationship only at the logical level. It includes timestamps and information of inputs and outputs. The input information contains a pointer to the input interaction and an index of the output interaction and an unlocking script. The output information contains interaction data and locking scripts. Because the node lacks mutual trust, the data block does not contain any account or identity information of the recipient or holder **[6].**

***Chainstructure*:** A block is a blockchain component which consisting of a block header and a content or data or transaction. The block header is an 80 byte long string and comprised of five fields, which are version, previous block hash, next block hash, Merkle root and timestamp. The blockchain consists of previous and present block **[7].**

Figure 2: Blockchain Component.



The timestamp*:* It determines the block generation time by marking the time for each transaction on the blockchain. Timestamp proves when and what has happened on the blockchain, and it's tamper-proof. Timestamp plays to role of a notary, and it's more credible than a traditional one **[8].**

The Merkel tree or Hash Tree: The Merkle tree is part of the block, the leaf node is the recorded information, and the intermediate node is the hash of the next two nodes **[9]**. It guarantees the authenticity, integrity, consistency and non-repudiation of the data. It allows for consistent and secure verification of content in a large body of data **[10].**

Cryptography: Cryptography is the method of disguising and revealing, otherwise known as encrypting and decrypting information through complex mathematics **[11].** Blockchain technology utilizes cryptography as a means of ensuring transactions are done safely, while securing all information and storages of value. Therefore, anyone using blockchain can have complete confidence that once something is recorded on a blockchain, it is done legitimately in a manner that preserves security. Asymmetric encryption and hashing algorithms are the foundation of blockchain technology to ensure the security requirements and verification requirements of untrusted blocks. The hash algorithm is used to generate the previous block address, record the brief message and the interaction address, and construct the Merkel Tree data structure. Asymmetric encryption algorithm is used for information encryption, signatures, and authentication. Elliptic Curve Cryptography (ECC) is one of the most secure encryption algorithms used in blockchain.

Table 1: Types of Cryptographic Hash Algorithm.

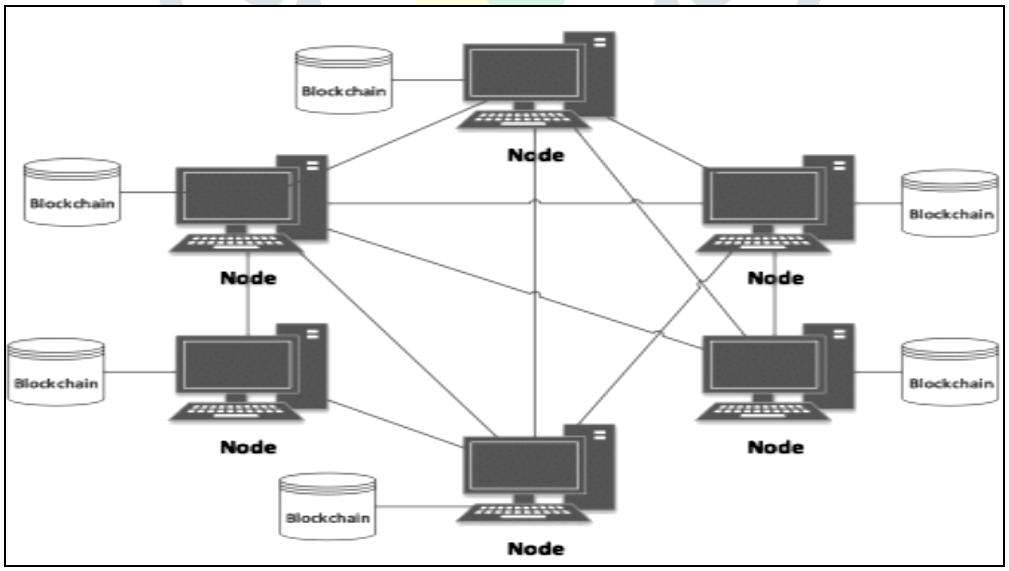
No.	Cryp togphic Hash Algorithm	used by
1	SHA-256 algorithm**ra**	Bitcoin
2	SHA- 512 algorithm	Ripple
3	SCRYPT algorithm	Litcoin
4	Scrypt-N algorithm	Vertcoin
5	Ethash algorithm	Ethereum
6	SHA-256, Keccak-512,Grøestl -512 and BLAKE-512 HVC	Heavycoin
7	Ethash algorithm	Ethereum
8	Cunningham chains and bi-twin chains Algorithm	Primecoin

The algorithm that has been used by Blockchain includes - **SHA-256 algorithm** which was used by Bitcoin. However, due to the rise of mining graphics cards and mining pools, the problem of centralization became serious. Litecoin 7 started using the **SCRYPT algorithm**. SCRYPT It is designed to reduce CPU load, minimize CPU dependencies, and use CPU idle time for calculations. In order to pursue greater memory consumption and computing time, the SCRYPT algorithm was improved and formed the **Scrypt-N algorithm** and the **ASIC mining machine**. Similarly, **Heavycoin (HVC)** 8 attempts parallel algorithms and implements games on the blockchain. Ethereum uses the transition algorithm **Ethash** which is an improved algorithm of Dagger–Hashimoto that is mainly used to resist the performance of mining machines and achieve quick verification of customers.

Network layer

The network layer: manages addressing and routing of packets between different physical routers **[12].** ***Peer-to-Peer (P2P)*** network is created when two or more PCs are connected and share resources without going through a separate server computer. **[13].**The endpoints are intertwined to form a network without a fixed topology, and each node can transmit and verify data. Each node has a routing function to ensure correct distribution of network data.

Figure 3: Blockchain P2P.



Verification Mechanism: Verification is a safeguard measure invoked on the node. The node has the ability to verify data integrity and ensure the correctness and reliability of the information and data being transported in the network. Blockchain nodes can freely join or leave the blockchain system without affecting the normal operation of the blockchain. Blockchain nodes have the right to process received data independently without intervention **[14].**

The broadcast protocol: is responsible for message to every node in the network, or a selective broadcast message to a specified group of nodes. A blockchain network needs to transmit two kinds of information: interaction information and block information. The interaction record or block generated by the sender is sent to multiple neighboring nodes. An approximate exponential broadcast process allows information to be sent throughout the network in seconds or minutes. Each interaction record or block

must pass validation to continue to spread and return to the sender to verify the information passed; otherwise, the transaction is discarded and a rejection message is returned to the sender **[15].**

Consensus layer:

Consensus mechanism is a fault-tolerant mechanism that is used to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems. The mechanisms designed to ensure the accuracy and consistency of information stored by all nodes in a distributed ledger. The more dispersed the decision system, the lower the consensus efficiency, but the higher the satisfaction and stability of the system. Equally, the more centralized the decision-making system, the easier it is to reach consensus, but the lower the satisfaction and stability of the entire system. The design of the consensus mechanism depends primarily on the needs of the business and performance. From PoW to PoS to DPoS to PBFT. **[16].**The consensus procedure is also known as the cryptocurrency mining process. Consensus mechanisms have the capability of eliminating contradictory or invalid transactions **[17].** Currently, there is no perfect consensus mechanism, and only optimal solutions exist for specific scenarios. (PoW) is the consensus algorithm used by Bitcoin. Before Bitcoin, there were loads of variants of peer - to - peer decentralized currency systems that failed because they were unable to solve the biggest problem when consensus was reached. This problem is called the "Byzantine General Problem". The consensus mechanisms of blockchain aims to eliminate mainly two known problems with digital currency (1) Remove the problem of double spend and (2) Eliminate Byzantine Generals problem. **[18].** We are now going to go through a list of consensus mechanisms which can solve the Byzantine Generals problem.

Proof of Work: Satoshi Nakamoto, Bitcoin's creator, was able to bypass the problem by inventing the proof of work protocol. Protocol requires all nodes on the network to solve cryptographic puzzles by brute force. The miners solve cryptographic puzzles to "mine" a block in order to add to the blockchain. This process requires immense amount of energy and computational usage. The puzzles have been designed in a way which makes it hard and taxing on the system. When a miner solves the puzzle, they present their block to the network for verification. Verifying whether the block belongs to the chain or not is an extremely simple process. The proof-of-work mechanism definitely answered a lot of questions when it came to solving the Byzantine General's Problem, but unfortunately there are some issues with proof-of-work. First and foremost, proof of work is an extremely inefficient process because of the sheer amount of power and energy that it eats up. People and organizations that can afford faster and more powerful ASICs usually have better chance of mining than the others **[19], [20].**

Proof of Stake: Proof of stake protocol of block verification does not rely on excessive computations. It has been implemented for Ethereum and certain altcoins. Instead of splitting blocks across proportionally to the relative hash rates of miners (i.e. their mining power), proof-of-stake protocols split stake blocks proportionally to the current wealth of miners. The idea behind Proof of Stake is that it may be more difficult for miners to acquire sufficiently large amount of digital currency than to acquire sufficiently powerful computing equipment. It is also an energy saving alternative Currently, Ethereum will move from (POW) to (POS). Proof of stake will make the entire mining process virtual and replace miners with validators. Peer-to-peer distributed networks lack trust between nodes and each node cannot operate with trust. This is how the process will work: The validators will have to lock up some of their coins as stake. After that, they will start validating the blocks, meaning, when they discover a block which they think can be added to the chain, they will validate it by placing a bet on it. If the block gets appended, then the validators will get a reward proportionate to their bets. Derived from PoW, PoS has low latency that can lower computing power and resource usage **[21], [22].**

Practical Byzantine Fault Tolerance:It is also known as proof of stock authority, is the consensus mechanism proposed by the BitShares community. DPoS is a new algorithm for protecting the security of cryptocurrency networks on the basis of PoW and PoS. All nodes in the DPoS vote for up to 101 accounting representatives based on stock rights (coin age). The representatives are responsible for the packaging and mining of transactions. All delegates will receive a transaction fee equal to 10% of the average amount. DPoS reduces the number of accounting and verifying **[23].**

Table 2: Different Consensus Protocols.

	PoW	**PoS**	**DPoS**	**PBFT**
Energy Consumption	High	Low	Very Low	Very Low
Transaction Per Second	7-30	30-173	2.3-2,500	100-2,500
Transaction Fee	High	Low	Low	Very Low
Structure	Decentralized	Decentralized	Centralized	Decentralized
Used by	Bitcoin	Dash	BitShare	Stellar

Contract layer

The contract layer largely includes various types of script code and algorithms required for the operation of the blockchain system and more complex intelligent contracts. The contract layer is a logic, algorithm or rule strategy built at the bottom of the blockchain to enable flexible programming and operational data functions for the blockchain system **[24].**

The smart contract: A smart contract is a computer code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other. If and when the pre-defined rules are met, the agreement is automatically enforced. The smart contract code facilitates, verifies, and enforces the negotiation or performance of an agreement or transaction. It is the simplest form of decentralized automation **[25], [26].** It is a mechanism involving digital assets and two or more parties, where some or all of the parties deposit assets into the smart contract and the assets automatically get redistributed among those parties according to a formula based on certain data, which is not known at the time of contract initiation. Smart contracts come in many forms, such token systems, savings wallets, crop insurance, multi-signature smart contracts, etc. These are typical applications of Ethereum.

Service layer

The service layer, a combination of low-level data and computing tools, provides services for upper-level specificc application services **[27].** The service platform is mainly developed independently by companies. Some technology companies are beginning to focus on the development of blockchain platforms. Such as IBM's Azure BaaS14 and Linux's Hyperledger. The application layer is primarily used for specific services that will be delineated in applications. Example is Blockchain as a Service (BaaS) is an offering that allows customers to leverage cloud-based solutions to build, host and use their own blockchain apps, smart contracts and functions on the blockchain while the cloud-based service provider manages all the necessary tasks and activities to keep the infrastructure agile

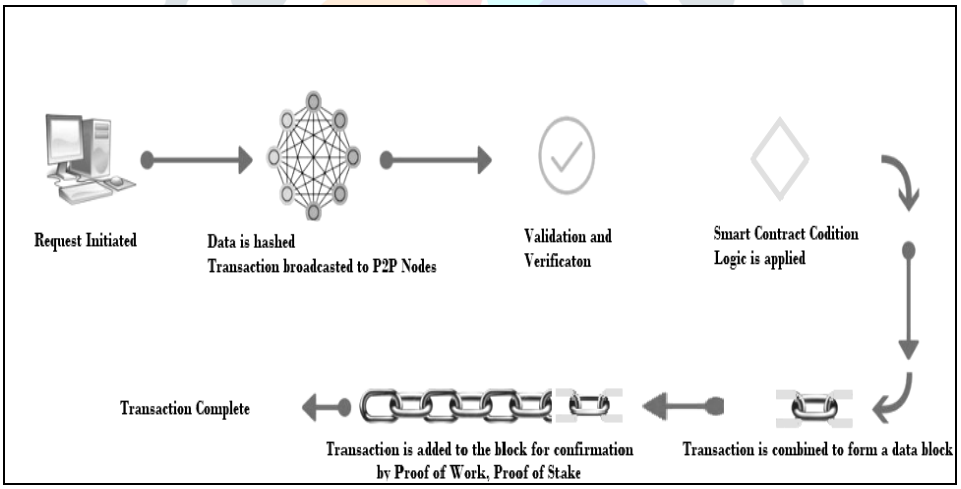
Application layer

The application layer contains service and application platforms. This will be discussed in details in Section 4.

The main working processes of blockchain are as follows:

1. Someone requests a transaction via something called a wallet.
2. The transaction is send (broadcast) to all participating computers in the specific blockchain network.
3. Every computer in the network checks (validate) the transaction against some validation rules that are set by the creators of the specific blockchain network.
4. Validated transactions are stored into a block and are sealt with a lock (hash).
5. This block becomes part of the blockchain when other computers in the network validate if the lock on the block is correct. Using Proof of Work and Proof Stake
6. Now the transaction is part of the blockchain and cannot be altered in any way.

Figure 4: Blockchain flow.



III. PRINCIPLE AND TYPES OF BLOCKCHAIN

Decentralization: Blockchain technology does not rely on involvement by third parties or hardware, nor does it have any central control. All blockchain regular users can partake in the authentication of their data. As discussed previously, Blockchain technology forms a network through a P2P protocol. Unlike the centralized network, nodes in a P2P network have the same network power, and there is no centralized server **[28].**

Openness and Transparency: Blockchain technology is an open source, data is open to everyone. Anyone can query blockchain data and develop applications through a common interface. Blockchain data resources and management belong to all nodes joining the blockchain system, while entities outside the blockchain system are blocked. As a distributed general ledger technology, all data records and operations within the system are transparent to all nodes in the network. The blockchain ensures high transparency of data information through a combination of asymmetric encryption and hash encryption. The procedures, rules, and access methods of the blockchain network are public **[29], [30].**

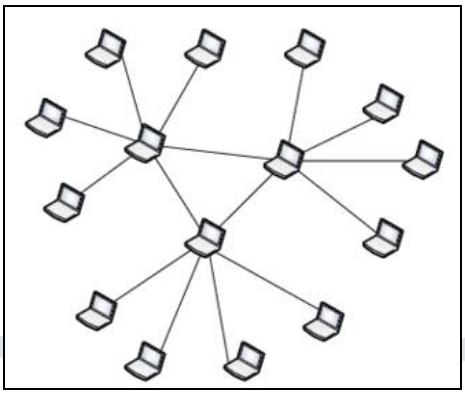
Independence: The blockchain is maintained by its own system node, and its data proof mechanism is implemented by the computer through a protocol without manual intervention **[31].**

Unforgeable: Each node added to the blockchain is distributed to record blockchain data, which guarantees irreversible modification of the data. Once the data information is verified and added into the blockchain, it will not be tampered.

Types of Blockchain

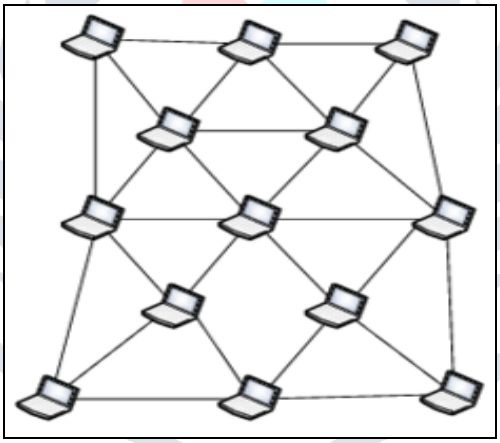
Private Blockchain: A blockchain that serves organizations or simple businesses. Private blockchain is basically closed and exclusive. It is usually implemented in a small range. Due to its single goal, the structure is relatively simple **[32] [33].**

Figure 5: Private Blockchain.



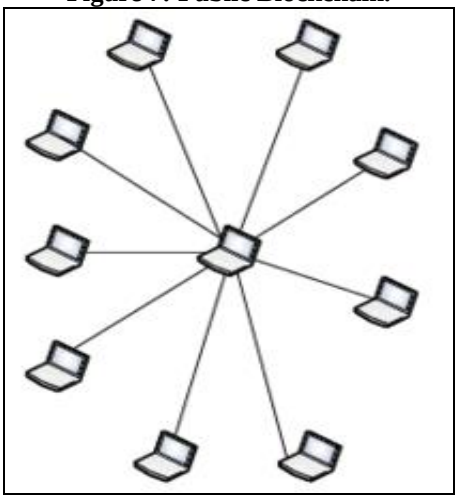
Consortium Blockchain: A blockchain consisting of multiple organizations serves as a common goal, and some related organizations can join the consortium blockchain through common agreements. This blockchain will become the mainstream of future blockchains **[34], [35], [36].**

Figure 6: Consortium Blockchain.



Public Blockchain: Any organization or individual can apply to join the blockchain. This blockchain has no restrictions on scalability and may be difficult to maintain in the future **[37].**

Figure 7: Public Blockchain.



IV. APPLICATION AREAS

Cryptocurrency: Cryptocurrencies are medium of exchange that uses cryptography to secure transactions. They have a poor store of value compared to traditional currencies and have lower price stability due to lack of government intervention. However, cryptocurrencies are a more efficient medium of exchange as blockchain technology is uniquely positioned to tackle speed and cost. There are many cryptocurrencies being created and used for specific purposes. It may be noted that the value of the cryptocurrency is measured using the fiat currency.

Private Data Storage: In some proposed system, the transactions are used to carry instructions for storing, queuing and sharing data. With increased number of mobile applications seeking complete access to user data such as contacts, messages, photos and a variety of other personal data, **[38]** has provided the implementation architecture of a system which uses blockchain along with an offline storage mechanism in order to manage permissions explicitly for each line item, rather than giving complete access permission indefinitely. Offline storage such as LevelDB or any cloud storage can be used to limit the amount of data stored in the blockchain.

Education: Blockchain can be the transformational force in education as well, researchers have suggested the use of blockchain to provide a verifiable, easily shareable and permanent record of such educational records and rewards. It also talks about the possibility of having an 'Educational Reputation Currency', which is initially distributed to participating institutes based on any existing metric. A successful implementation of blockchain to award educational certificates has been done by Sony and University of Nicosia.

Banking: The impact of blockchain as a technology was first felt by the banking and trading sector. Blockchain, was initially seen as the biggest threat to banking businesses worldwide. However, in past few years it has been seen that banks have deep dived to make this technology work for them in a favorable manner and are experimenting various ways to use blockchain in their business. In Philippines several banks have embraced blockchain ie Union Bank, some experts however still do believe that blockchain will lead to the end of several long standing businesses and professions. Typical banking processes like approval of a loan or derivative is a time consuming process due to multiple back end steps involving contract negotiations with multiple parties. Blockchain provides the necessary transparency and speed via smart contracts, to this requirement. Multiple banks are already experimenting Blockchain-as-a-Service offering from technology companies such as R3, IBM and Microsoft.

Taxation: As indicated in **[39],** taxation is one area where blockchain can potentially make a big contribution. The report relates the key attributes of blockchain namely provenance, transparency and traceability to the exact needs of a modern taxation system. A huge advantage of cutting on administrative cost can result from the use of blockchain especially in transaction taxes such as VAT, withholding Tax, stamp duties, etc. In a sharing economy, blockchain could be used to achieve compliance and transparency for tax payments, thus shifting the responsibility of collecting tax from tax authorities to participants of the sharing economy. In countries like India which are moving towards uniform taxation via GST (Goods and Services Tax), blockchain can help in tracking the end-to-end collection and expenditure of taxes by the government. While the tax provenance aspect is very important and so also is the utilization of tax earnings.

Healthcare**:** Over the past decade, healthcare is turning digital with more and more doctors, hospitals, healthcare machineries going cloud bassed to store their patient records. Digitization of medical data enables easy retrieval, sharing on need basis for better decision making based on historic cases and is also very crucial for legal purpose record keeping. A blockchain based Healthcare Data Gateway (HDG) is proposed by **[40].**They propose the use of a private blockchain cloud to guarantee that the medical data cannot be changed by anybody including the patient himself and/or the physicians. Medical data is diverse in kind, i.e. it could be numeric, textual, image data (scans, x-rays, photos, etc.), video data (transcripts, recordings, etc.), etc. **[41].** Have also proposed a blockchain based system MeDShare, for sharing medical data among cloud service providers. MeDShare would provide data access control, provenance and auditing.

Voting: In the year 2014, a Danish political party was the first to use blockchain technology for voting. Online voting platforms such as 'Followmyvote', which enable digitally secure blockchain based voting have also been created.

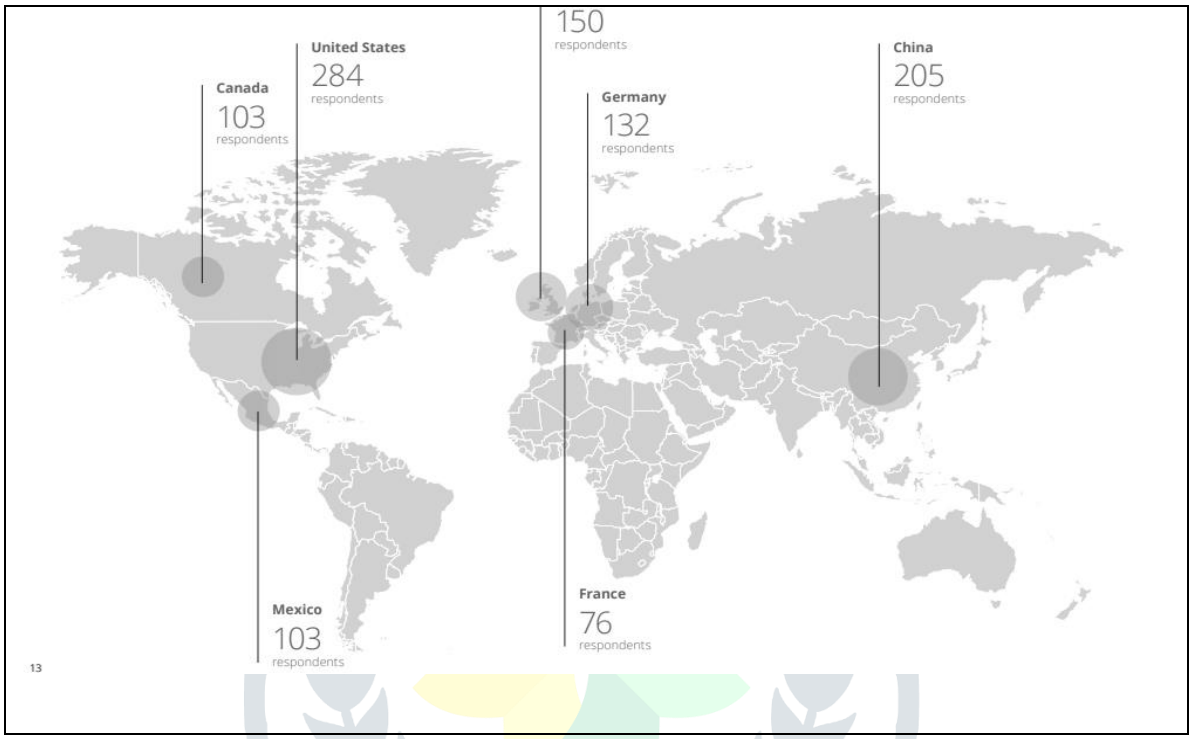
Internet of Things: IoT has gradually become a popular technology for enterprises and users. Many centralized IoT infrastructures and IoT devices interact with each other through centralized control methods. However, this method is not proper for anonymous communication. Blockchain technology offers the possibility to build such a decentralized IoT platform. Due to P2P transmission and high security, blockchain technology can be the underlying infrastructure of IoT. Scholars have different views on the IoT infrastructure, but security is a common recognition. Compared to traditional networks, IoT can be embedded with a variety of devices, hardware, software, and blockchain-based technologies **[42].**

Cloud: A blockchain is a database. As time goes by, the blockchain database capacity will soon reach the order of big data, so the blockchain system is inseparable from cloud computing. The combination of blockchain and cloud computing is recreated in the storage, calculation, and management of blockchain data on the cloud platform. Blockchain systems, on the other hand, provide the hardware/software resources and other network devices for cloud computing. The amount of data involved is very large. Hence, the computing power of a stand-alone system does not meet the operational requirements of the blockchain system. Big data management requires cloud storage implementation. Without cloud platform and cloud processing, it is difficult for blockchain big data management to break through the bottleneck.

V. USERS FORECAST

In the survey conducted by **[43]** blockchain survey which is of more than 1,000 blockchain-savvy executives globally is a leading indicator of the future of blockchain. While blockchain is not quite ready for primetime, it is getting closer to its breakout moment every day. The academic hypotheses of five years ago are steadily becoming a reality. Momentum is shifting from a focus on learning and exploring the potential of the technology to identifying and building practical business applications. The executives that was surveyed hold pragmatic views and look poised to make some major moves over the next year. As seen below, those surveyed see great value in blockchain's potential to reinvent processes across the business value chain as more investment is made in identifying and developing a wider range of use cases.
To summarize, the survey was fielded across seven countries (Total number of respondents = 1,053)

Figure 8: Survey participants.



The attitude towards blockchain was one of the initial question and respondents are extremely strong on blockchain's potential, namely its ability to broadly scale and reach mainstream adoption. A majority also agreed that blockchain technology will disrupt their industry. Despite these high expectations, 39 percent of respondents agreed that blockchain technology is overhyped, suggesting that even blockchain believers think some of the rhetoric on the technology's potential is overly optimistic.

As mentioned that blockchain will be a disruptive technology the most significant advantage of blockchain over existing systems suggests that companies are interested in leveraging blockchain's real-time information exchange capabilities to speed up business processes and gain operational efficiencies. Additionally, 28 percent of respondents believe that blockchain can help them unlock new revenue sources and business models, underscoring the technology's disruptive potential.

When it comes to security they were asked if blockchain-based solution is currently more secure or less secure than systems built from more conventional information technologies and the overwhelming majority of respondents believe that blockchain is more secure than conventional IT systems.

As discussed previously, we have three types of blockchain from the survey, most of the respondent choose Permissioned blockchain mainly because they have clearly defined governance structures compared to public blockchain networks. Public blockchains operate like public forums where any individual operating a full node would have a say in the governance and the rules of the network.

VI. CHALLENGES

Initial Costs: Though the adoption of blockchain technology promises long-term benefits with regard to productivity, efficiency, timeliness and reduced costs, it is expensive to initially put it in place. The software required to run blockchain technology in organizations must typically be developed for the specific firm and is therefore expensive to purchase, acquire or develop in-house. Moreover, organizations may have to obtain specialized hardware for use with the software.In addition to the software costs, organizations must also find qualified personnel to work in tandem with the technology. The blockchain technology space is relatively new and is growing at such a fast rate that professionals proficient in the field are few and far between. Due to the large demand and limited supply, organizations must be willing to pay large salaries to the individuals who are qualified for these positions.This means that a move to a complete or even partial blockchain-based system is out of reach for most small- and medium-sized business due to the high setup costs involved **[44].**

Integration with current systems: In order to make the move to a blockchain-based system, an organization must either completely overhaul their previous system or find a way to integrate their existing system with the blockchain solution. However, it may be difficult for blockchain solutions to handle all functions needed by organizations, initially making it difficult to completely eradicate legacy systems. Therefore, considerable changes must be made to the existing systems in order to facilitate a smooth transition. This process may take a significant amount of time, funds and human expertise. Many organizations are reluctant to make the move to blockchain solutions because of the meticulous planning, time and money that would be required in order to achieve successful company-wide implementation**.**

Energy Consumption: Ethereum network use the proof-of-work mechanism to validate transactions made on the blockchains. This mechanism requires the computation of complex mathematical problems to verify and process transactions and to secure the network. These calculations require large amounts of energy to power the computers solving the problems. In addition to the energy used to run the computers, a sizable amount of energy is also required to cool down the computers. The large amount of energy required to keep the most well-known blockchains in operation is a deterrent to many corporations that are now focusing on sustainable methods of doing business. With climate change being a major concern, such massive use of energy does not seem justifiable.

Public Perception: The majority of the public is still oblivious to the existence and potential uses of this technology. In order for blockchain technology to make the move to the mainstream, there must first be a public buy-in to its benefits. Though the technology is revolutionizing many different industries, knowledge of the benefits of distributed ledger technology is still limited to those who are involved in the technology space and those whose industries are adopting blockchain solutions.Before the adoption can be achieved, members of the public must understand the difference between bitcoin, other cryptocurrencies and the blockchain**.**

Decentralized storage. Existing cloud storage solutions often face security, privacy and data control challenges. Users only perform cloud storage on their confidentialdential files when they trust the cloud storage company's service plan. Storj20 provides a P2P distributed cloud storage platform based on blockchain, providing users with data transmission and sharing services **[45].**

VII. CONCLUSION

The blockchain is highly appraised and endorsed for its decentralized infrastructure and peer-to-peer nature. However, many researches about the blockchain are shielded by Bitcoin, but blockchain could be applied to a variety of fields far beyond Bitcoin. Blockchain has shown its potential for transforming the traditional industry with its key characteristics: decentralization, persistency, anonymity and auditability. In this paper, we present a comprehensive survey on the blockchain. We first give an overview of the blockchain technologies including blockchain architecture and key principles of the blockchain. We then discuss the typical consensus algorithms used in the blockchain. We analyse and compare these protocols in different respects. We also investigate typical blockchain applications. Furthermore, we list some challenges and problems that would hinder blockchain development. Some possible future application directions are also discussed. Due to the advancement of Information Technology, security of data became an important topic of the field. Information Security professionals proposed different solutions to overcome the security challenges, among these one of the solutions is blockchain technology. We plan to take an in-depth investigation on how Blockchain can act as security measure for Internet of Things (IoT) in the future.

REFERENCES

[1]. Swan, M (2015). Blockchain: Blueprint for a new economy. \O'Reilly Media, Inc.". Tarasiewicz, M and A Newman (2015). Cryptocurrencies as distributed community experiments. In Handbook of Digital Currency, DLK Chuen (ed.), pp. 201–222. Academic Press, London.

[2]. Nguyen, QK (2016). Blockchain-A ¯nancial technology for future sustainable development. In Green Technology and Sustainable Development (GTSD), Int. Conf., pp. 51–54, IEEE

[3]. Lu, Y (2017). Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, 1

[4]. Pilkington, M (2016). Chapter 11. Blockchain technology: Principles and applications. In Research Handbook on Digital Transformations, FX Olleros and M Zhegu (eds.), p. 225. Edward Elgar Publishing, Cheltenham, UK.

[5]. Liang, X, S Shetty, D Tosh, C Kamhoua, K Kwiat and L Njilla (2017). Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud and Grid Computing, pp. 468–477, IEEE Press.

[6]. Liu, L and B Xu (2018). Research on information security technology based on blockchain. In 2018 IEEE 3rd Int. Conf. Cloud Computing and Big Data Analysis (ICCCBDA), pp. 380–384, IEEE.

[7]. Kiran Vaidya, Bitcoin's implementation of Blockchain. Dec 8, 2016 (https://medium.com/all-things-ledger/bitcoins-implementation-of-blockchain-2be713f662c2)

[8]. Huobi 2017 - Blockchain 101 (*timestamp*) https://blog.hbg.com/category/education/

[9]. Shaan Ray 2017. Merkle Trees.

[10]. Alketbi, A, Q Nasir and MA Talib (2018). Blockchain for government services — cases, security bene¯ts and challenges. In Learning and Technology Conf. (L&T), pp. 112–119, IEEE.)

[11]. Lisk Academy 2019. https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/blockchain-cryptography-explained

[12]. David Xiao. 2016. The Four Layers of the Blockchain. https://medium.com/@coriacetic/the-four-layers-of-the-blockchain-dc1376efa10f

[13]. Tech Terms. 2019. https://techterms.com/definition/p2p

[14]. Tschorsch and Scheuermann, 2016. Tschorsch, F and B Scheuermann (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084–2123

[15]. Saghiri, AM, M Vahdati, K Gholizadeh, MR Meybodi, M Dehghan and H Rashidi (2018). A framework for cognitive Internet of Things based on blockchain. In 2018 4th Int. Conf. Web Research (ICWR), pp. 138–143, IEEE.

[16]. Kaushik, A, A Choudhary, C Ektare, D Thomas and S Akram (2017). Blockchain — Literature survey. In Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017 2nd IEEE Int. Conf. IEEE, pp. 2145–2148.

[17]. Mattila, J (2016). The blockchain phenomenon — the disruptive potential of distributed consensus architectures (No. 38). The Research Institute of the Finnish Economy

[18]. Lamport, L, R Shostak and M Pease (1982). The Byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS), 4(3), 382–401.

[19]. Kroll, JA, IC Davey and EW Felten (2013). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In Proc. WEIS, Vol. 2013, p. 11.

[20]. Pilkington, M (2016). Chapter 11. Blockchain technology: Principles and applications. In Research Handbook on Digital Transformations, FX Olleros and M Zhegu (eds.), p. 225. Edward Elgar Publishing, Cheltenham, UK.

[21]. King, S and S Nadal (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. Selfpublished paper, 19 August.

[22]. Courtois, NT (2014). On the longest chain rule and programmed self-destruction of crypto currencies. arXiv preprint arXiv:1405.0534.

[23]. Larimer, D (2014). Delegated proof-of-stake (dpos). Bitshare Whitepaper. Lei, A, H Cruickshank, Y Cao, P Asuquo, CPA Ogah and Z Sun (2017). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal, 4(6), 1832–1843.

[24]. Puthal, D, N Malik, SP Mohanty, E Kougianos and C Yang (2018a). The blockchain as a decentralized security framework. IEEE Consumer Electronics Magazine, 7(2), 18–21.

[25]. Atzei, N, M Bartoletti and T Cimoli (2017). A survey of attacks on ethereum smart contracts (sok). In Principles of Security and Trust, pp. 164–186. Berlin, Heidelberg: Springer.

[26]. Wright, C and A Serguieva (2017). Sustainable blockchain-enabled services: Smart contracts. In Big Data (Big Data), 2017 IEEE Int. Conf., pp. 4255–4264, IEEE.

[27]. Gupta, Y, R Shorey, D Kulkarni and J Tew (2018). The applicability of blockchain in the internet of things. In Communication Systems & Networks (COMSNETS), 2018 10th Int. Conf., pp. 561–564, IEEE.

[28]. Crosby, M, P Pattanayak, S Verma and V Kalyanaraman (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2, 6

[29]. Zheng, Z, S Xie, H Dai, X Chen and H Wang (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In Big Data (BigData Congress), 2017 IEEE Int. Congress, pp. 557–564, IEEE.

[30]. Lin, IC and TC Liao (2017). A survey of blockchain security issues and challenges. IJ Network Security, 19(5), 653–659

[31]. Iansiti, M and KR Lakhani (2017). The truth about blockchain. Harvard Business Review, 95(1), 118–127.

[32]. Dinh, TTA, J Wang, G Chen, R Liu, BC Ooi and KL Tan (2017). Blockbench: A framework for analyzing private blockchains. In Proc. 2017 ACM Int. Conf. Management of Data, pp. 1085–1100, ACM.

[33]. Sato, T and Y Himura (2018). Smart-contract based system operations for permissioned blockchain. In New Technologies, Mobility and Security (NTMS), 2018 9th IFIP Int. Conf., pp. 1–6, IEEE.

[34]. Zhou, L, G Wang, T Cui and X Xing (2017). Cssp: The consortium blockchain model for improving the trustworthiness of network software services. In Ubiquitous Computing and Communications (ISPA/IUCC), 2017 IEEE Int. Symp. Parallel and Distributed Processing with Applications and 2017 IEEE Int. Conf., pp. 101–107, IEEE.

[35]. Gu, J, B Sun, X Du, J Wang, Y Zhuang and Z Wang (2018). Consortium blockchain-based malware detection in mobile devices. IEEE Access, 6, 12118–12128

[36]. Brousmiche, KL, T Heno, C Poulain, A Dalmieres and EB Hamida (2018). Digitizing, securing and sharing vehicles life-cycle over a consortium blockchain: Lessons learned. In New Technologies, Mobility and Security (NTMS), 2018 9th IFIP Int. Conf., pp. 1–5, IEEE.

[37]. Anoaica, A and H Levard (2018). Quantitative description of internal activity on the ethereum public blockchain. In New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conf., pp. 1–5, IEEE.

[38]. Zyskind, G and O Nathan (2015). Decentralizing privacy: Using blockchain to protect personal data. In Security and Privacy Workshops (SPW), pp. 180–184, IEEE

[39]. Annual Report 2018 - PwC UK. https://www.pwc.co.uk/issues/futuretax/how-blockchain-technology-could-improve-tax-system.html

[40]. Xiao Yue, Huiju Wang, Dawei Jin, Mingqiang Li, Wei Jian (2016) Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control

[41]. Qi Xia. 2017. MeDShare: Trust-less Medical Data Sharing Among Cloud Service Providers Via Blockchain

[42]. Seyoung Huh ; Sangrae Cho ; Soohyung Kim.2017. Managing IoT devices using blockchain platform

[43]. Deloitte's 2018 global blockchain survey. https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-2018-deloitte-global-blockchain-survey.pdf

[44]. Bitcoin Magazine 2018)https://www.nasdaq.com/article/five-challenges-blockchain-technology-must-overcome-before-mainstream-adoption-cm899472

[45]. Renner, T, J Müller and O Kao (2018). Endolith: A blockchain-based framework to enhance data retention in cloud storages. In Parallel, Distributed and Network-based Processing (PDP), 2018 26th Euromicro Int. Conf., pp. 627–634, IEEE.