Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol. 7, No. 4, December 2019, pp.1821-1832

The road to the blockchain technology: Concept and types

Sana Sabah Sabry[1], Nada Mahdi Kaittan[2], Israa Majeed Ali[3]
[1]College of Engineering, University of Information Technology and Communications, Iraq
[2]College of Business Informatics, University of Information Technology and Communications, Iraq
[3]College of Engineering, Al-Iraqia University, Iraq

ABSTRACT

As the Bitcoin keeps increasing in value compared to other cryptocurrencies, more attention has given to Blockchain Technology (BT), which is the infrastructure behind the Bitcoin, especially on its role in addressing the problems of the classical centralized system. As a digital currency, Bitcoin is dependent on the decentralized cryptographic tools and peer-to-peer system. The digital currency implements a distributed ledger using Blockchain when verifying any type of transaction. In this paper, the aim is to describe how digital currency networks such as Bitcoin provides a "trust-less" platform for users to embark on money transfers without necessarily depending on any central trusted establishments such as payment services or financial institutions. Furthermore, this work comprehensively overviewed the basic principle that underly BT, such as transaction, consensus algorithms, and hashing. This study also provided a novel classification for blockchain types according to their system architecture and consensus strategy. For each type, our contribution was provided with an example, which clearly describes the blockchain features and the transaction steps. Our classification intended to help researchers understand and choose the blockchain for their application. The paper ends with the discussion of the differences between each type

Keywords: Blockchain; Bitcoin; Ethereum; Hyperledger; Digital Currency

Corresponding Author:

Sana Sabah Sabry,
Universiti of Information Technology and Communications, Baghdad, Iraq
Email: Sana.Sabah@uoitc.du.iq

1. Introduction

Blockchain is the infrastructure behind the Bitcoin revolution. Bitcoin is a cryptocurrency that ensures trust and security via the implementation of programs for the verifying and validating transactions [1]. As a cryptocurrency, Bitcoin relies on decentralized cryptographic tools and peer-to-peer system to provide a "trust-less" platform for users to embark on money transfers without necessarily relying on any centralized trusted establishment such as payment services or banks [2]. With the non-dependence of the blockchain network on any centralized establishment, it cannot be controlled by such systems as with the conventional centralized payment and banking systems. Blockchain ensures trust (as an emergent property) from the internodal interactions within the network. there are two basic classifications of blockchains – private and public blockchains. The public or "permissionless" blockchain allows anyone to engage in financial transactions without necessarily having an identity. In public blockchains, a native cryptocurrency is mostly involved while consensus is often used based on economic incentives and "proof of work" (PoW). On the other hand, private or "permissioned" blockchains requires the identity of the participant to be known. In private blockchain, the interactions between a group of participants who share a common goal but do not have full trust on each other (for instance, transactions that involve the exchange of goods, information, or funds)

can still be secured. Being that private blockchain depends on the identities of the participants, it can be applied in the "traditional Byzantine-fault tolerant (BFT) consensus" [3].
Bitcoin is the most popular system that uses blockchain technology. There are several applications of blockchain technology [4], such as the music industry [5], healthcare [6], education [7], and cybersecurity [8]. Several blockchain researches have focused on Bitcoin only [9, 10] and have classified blockchain into private and public [11-14]. To overcome this, this paper described and categorized blockchains into three novel types based on their overall system and applications; a comparison was also made between these different types.

-Only Cryptocurrency blockchain (C2C): Type one deals with only cryptocurrency chain; it is totally reserved for payments or money decentralization (Bitcoin Blockchain).
-Business to Cryptocurrency blockchain (B2C)*:* In this type of blockchain, a logic tier is introduced into the ledger which serves as a multipurpose programmable infrastructure. Here, the public ledger does not only store financial transactions, but it also has facilities to deploy and execute programs on the blockchain system; a process known as smart contracts (Ethereum blockchain).
-Only business blockchain (B2B): The third type requires no currency; it supports the execution of software for business logic, such as Hyperledger project (Fabric blockchain).

This paper presents a comprehensive overview of Bitcoin and Ethereum transaction. The major aim of this study is to review the various types of blockchains to provide a better understanding of their important role in ensuring the security of digital data and in the next generation of internet and decentralize applications, as well as its role in businesses revolution and provision of state-of-the-art on digital currencies for today's techniques. A general overview on blockchain concepts, such as symmetric-key cryptography, hashing, transaction, and consensus algorithms was given in section 2 of this paper while section 3 described blockchain types with transaction scenarios and the comparison between these types. Finally, section 4 concluded the paper.

2. Blockchain overview

Blockchain implements a distributed ledger for the general verification of any kind of transaction [15]. Figure 1 illustrates the centralized and distributed system.

Figure 1. The centralized and distributed system

To have a better understanding of blockchain, it is necessary to be acquainted with the concept of a distributed ledger. By definition, a typically distributed ledger refers to a shared database, which is synchronized and

replicated among different network users in a decentralized manner. The participants' transaction data in a network is stored in the distributed ledger [16]. Hence, a blockchain relies on a "Distributed Ledger Technology (DLT)" which is distributed across several computing nodes or devices [17]. Before a transaction can be stored in the ledger, most of the blockchain network participants must give and record their consents. To ensure that each blockchain network user is updated, they are provided with a copy of the original ledger which must be updated and synchronized continuously when there are changes [18].
It is generally believed that blockchain is a system that creates a distributed consensus in the online digital space. This allows its participants to know for sure of the likelihood of a digital event to occur by simply creating a certain record in a public ledger, thereby creating a platform for the emergence of democratic space and a scalable digital economy from a centralized one. This disruptive technology presents several opportunities, and this is just the beginning of the revolution in this space.

Figure 2 illustrates the typical forms of a blockchain. A blockchain is comprised of data sets, which are made up of several blocks/data packages and each block is made up of several transactions. Each additional block extends the blockchain, hence, represents a complete ledger of the transaction record. The network can cryptographically validate the blocks. In each block, there is also a timestamp, the previous blocks' hash value ("parent"), as well as a nonce (a random number for the hash verification). With this concept, the integrity of the whole blockchain (down to the first or genesis block) is ensured. Owing to the unique nature of the hash values, it would be easy to prevent fraud since the manipulation of any block in the chain would instantly alter the value of the related hash. Before a block can be added to the chain, most of the nodes must agree on the validity of the transactions in the related block, as well as on the blocks' validity [11].

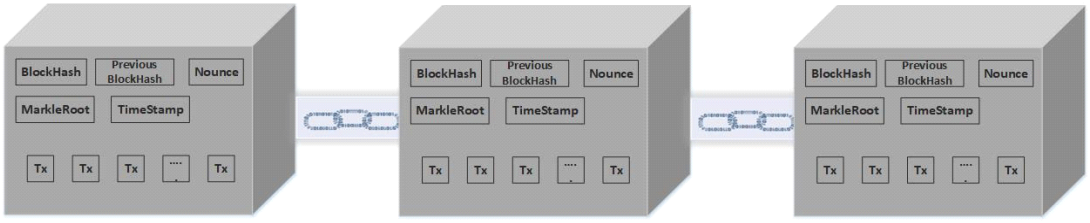

Figure 2. Typical forms of blockchain

Special peer nodes called miners are responsible for the whole validation and consensus process. These miners are robust computational software which is defined by the blockchain protocol.

3. Core blockchain concept

The blockchain network operates on some basic concepts which must be fully understood to be conversant with blockchains. These concepts are:

3.1 Asymmetric key cryptography

The blockchain network secures the operation of the blockchain using public-key cryptography. The execution of any transaction, except those on the same platform, requires the participants to have a digital wallet which is secured with the private key of the participant and can only be accessed using only the signatures generated by the corresponding private key. Each transaction is accompanied by a digital signature, which is sent to the receivers' public key after being digitally authenticated by the senders' private key. To spend any cryptocurrency, the owner of such currency must demonstrate that he is the owner of the "private key". Then, the recipient of the cryptocurrency using the public key in order to authenticate the ownership of the associated "private key" will verify the digital signature appended by the sender.

3.2 Transaction

Transaction in a blockchain network could be defined as a small unit of task stored in public records. The execution and storage of these records in the blockchain require prior approval by most of the participants involved in the network. Any previous transaction can be subjected to a review at any time; however, it cannot be updated. The transactions which are steadily generated by the nodes and congregated in blocks represent the current state of the blockchain [19].

3.3 Consensus algorithms

Upon the commencement of data propagation by the nodes via a blockchain network, the nodes have no centralized party that will be responsible for regulating and resolving disputes or protects against intrusions. Therefore, there is a need for a mechanism that will track the movement of funds and guarantee an incontrovertible fund exchange to prevent fraud (such as double spending attacks). All the nodes must consent to a common content updating protocol for this ledger to maintain a consistent state, and blocks should not simply be accepted to be a part of the blockchain without majority consent. This is called a consensus mechanism by which blocks are created and added to the existing ledger for future use.
There are a number of consensus mechanisms; however, the most common blockchain consensus mechanisms are Proof of Stake (PoS), Proof of Work (PoW)[20], Practical Byzantine Fault Tolerance (PBFT)[21], and Delegated Byzantine Fault Tolerance (dBFT). The key difference between various consensus mechanisms is the way they delegate and reward the verification of transactions [22]. The PoW protocol is one of the first utilized consensus protocols that is based on computational load, requiring miners to find a solution to a puzzle. Several cryptocurrencies utilize a variant of this protocol. Performance is quite low and found to be not suitable for very large ecosystems. To reduce the high resource cost of mining, PoS was proposed which assigns a difficulty value to a puzzle based on how much stake the miner has in the network. Some consensus protocols such dBFT and PBFT are based on the communication between different nodes, and they are mostly used in private chains that have authenticated nodes.

3.4 Hashing

A hash function is used to map the original data (message) to a collection of data of fixed size (i.e., hash value). The features of the cryptographic hash function include collision resistance, pre-image resistance, second pre-image resistance, and puzzle friendliness. Because of these features, hash functions can be applied to verify the integrity of the original message, or as hash pointers, in which the pointer contains the hash of the message that it points to. In the blockchain, each data block contains the hash value of the previous block so that the integrity of all previous data can be verified, as well as to keep the transaction records from being altered [23].
Blockchain technology has over the past few years evolved from the earlier Bitcoin foundation to other generation platforms. Three major types of blockchains are available today as illustrated in Figure 3.

4. Blockchain types

4.1 Only cryptocurrency blockchain (C2C)

This type deals **only with cryptocurrency** chain and is wholly reserved for money or payments decentralization. Bitcoin was introduced in 2009 and since then, has become the most used cryptocurrency [24]. Bitcoin represents the first implementation of a DLT as it supports Bitcoins mining. The sole reason for Bitcoin blockchain development was to address the issue of double digital money spending. There are two types of nodes in the Bitcoin network; users that request transaction and miners that compete to add new blocks to the main blockchain. There are other

cryptocurrencies other than Bitcoin in this type of blockchain. Please refer to [15] and [25] for more information about the existing cryptocurrencies.

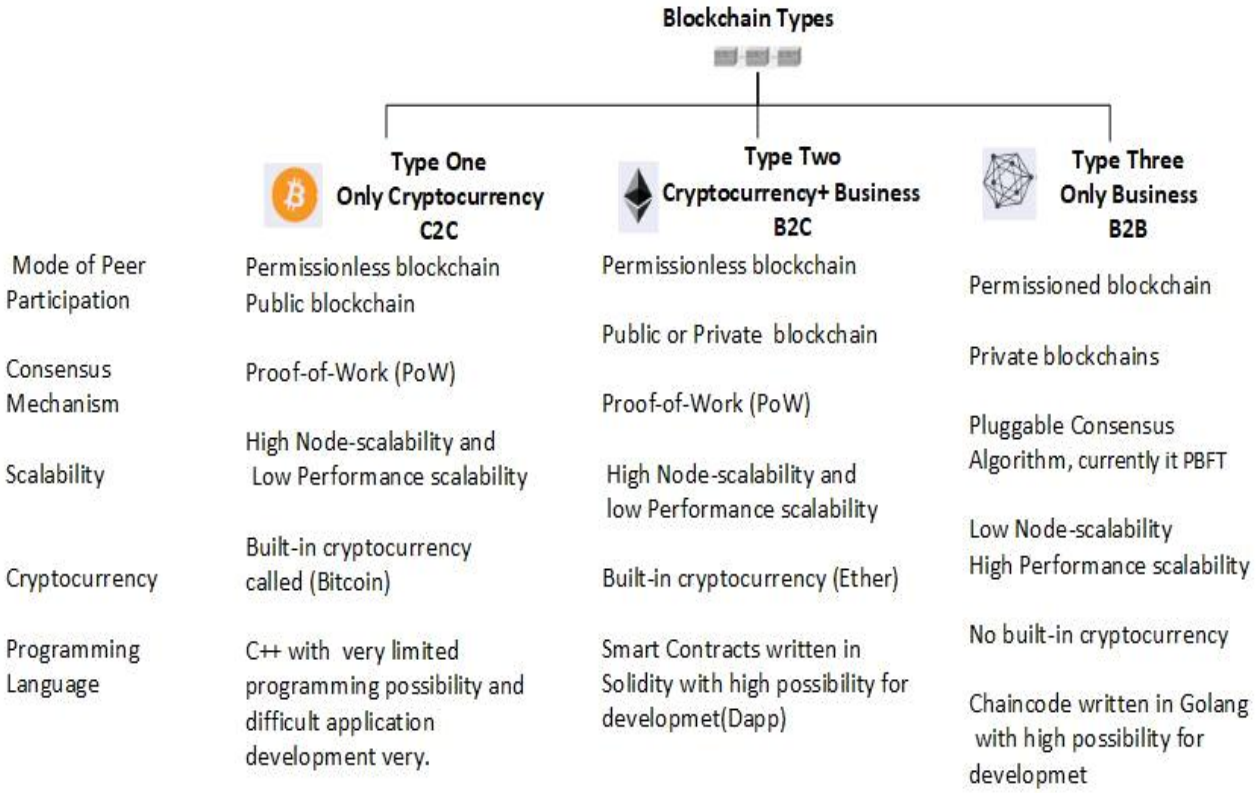

Figure 3. Blockchain types

Transaction steps in bitcoin

To understand the transaction process in Bitcoin, consider the following scenario where Bob requested to transfer 3 BTC to Allice to buy one of her apple pies.

- A Bitcoin typically is not physically stored anywhere, instead, it must utilize digital storage. A private key is used to access the Bitcoin's public address. This requires the use of a software program that provides access to multiple Bitcoin addresses known as a wallet.
- Both Bob and Allice must already have a wallet (or create one).
- A Bitcoin wallet generates cryptographic key pairs (private +public key) which map to a unique address. To ensure privacy, a different address is used per transaction for the same wallet.
- Allice indicates her Bitcoin balance.
- Bob transfers the 3 BTC to Allice's address and signs the transaction with his private key which was created for this transaction using his own address. Bob's public key is also added to the transaction for ownership validation.
- The network must verify the payment ownership (Bob owns the 3 BTC?). The possession of Bitcoin blockchain is determined by
- Bob signs the transaction with his private key (transaction provided by Bobs' signature).
- Anyone in the network can verify Bobs' transaction by his public key.

Note: money can be sent by anybody with a public key to a Bitcoin address; however, the money can be sent by only a private key-generated signature.

- Bobs' verified transaction is bundled with other unrecorded transactions in a new block, waiting for miners to validate the new block and add it to the chain. The process of finding the right block is called mining and the nodes executing the search are called miners. The nodes can capture the PoW through mining and this is a form of establishing an agreement between the distrusted nodes.
- The wallet software informs Bitcoin miners around the world of the proposed transaction; the miners verify that Bob has enough Bitcoin to buy the delicious apple pie. Then, the miners' computers race to group the data of Bobs' proposed (pending) transaction with other unrecorded transections, plus the last block of transactions recorded in the public ledger, as well as a random number called nonce.
- Miners calculate the hash function as PoW

For every new hash tried, the mining software utilizes a different nonce as the block headers' random element and based on the nonce and whatever is left in the block, the hash will be generated by the hashing function.

F (Previous block hash + groped data + nonce) = hash for the new block; where F = cryptographic hash function (double hashing using SHA256).

Miners are unable to predict the nonce that produces a hash value with the required number of zeros.

To ensure that blocks are found roughly every ten minutes, there exists a "difficulty target". The creation of a valid block requires miners to find a hash which is below this "difficulty target".

- The winning miner gets his prize in BTC for his effort and resources; some hardware resources include CPU, GPU, FPGA, and ASIC. Most miners choose to mine in a pool to increase the chances of finding the right hash.
- Finally, the new block is added to the blockchain and Bob enjoys his delicious apple pie while Allice gets her money. All these steps are summarized in Figure 4.

4.2 Cryptocurrency to business blockchain (C2B)

This type of blockchains has a logic tier in the ledger, which provides a multi-purpose programmable infrastructure. The public ledger does not only store financial transactions in C2B, but it also has facilities to deploy and execute programs on the blockchain system (known as smart contracts). Smart contracts refer to small computing programs, which are automatically executed upon meeting certain conditions [26] [27]. Owing to the tamper-proof nature of smart contracts, the costs for the verification, execution, and prevention of fraud are reduced. An example of this type of blockchain is Ethereum, the second-largest permission-less network which was introduced by [28] as a platform for implementing smart contracts. Ethereum addresses several limitations of the Bitcoins' scripting language, such as the issue of long delays of Bitcoin transactions, where the time interval between blocks averages is around 10 min while it is 13-15 sec in Ethereum. The major advantage of Ethereum is full Turing-completeness, suggesting its support to all forms of computations, including loops.

Ethereum also supports state-of-the-art transactions and presents several improvements to the blockchain structure [29].

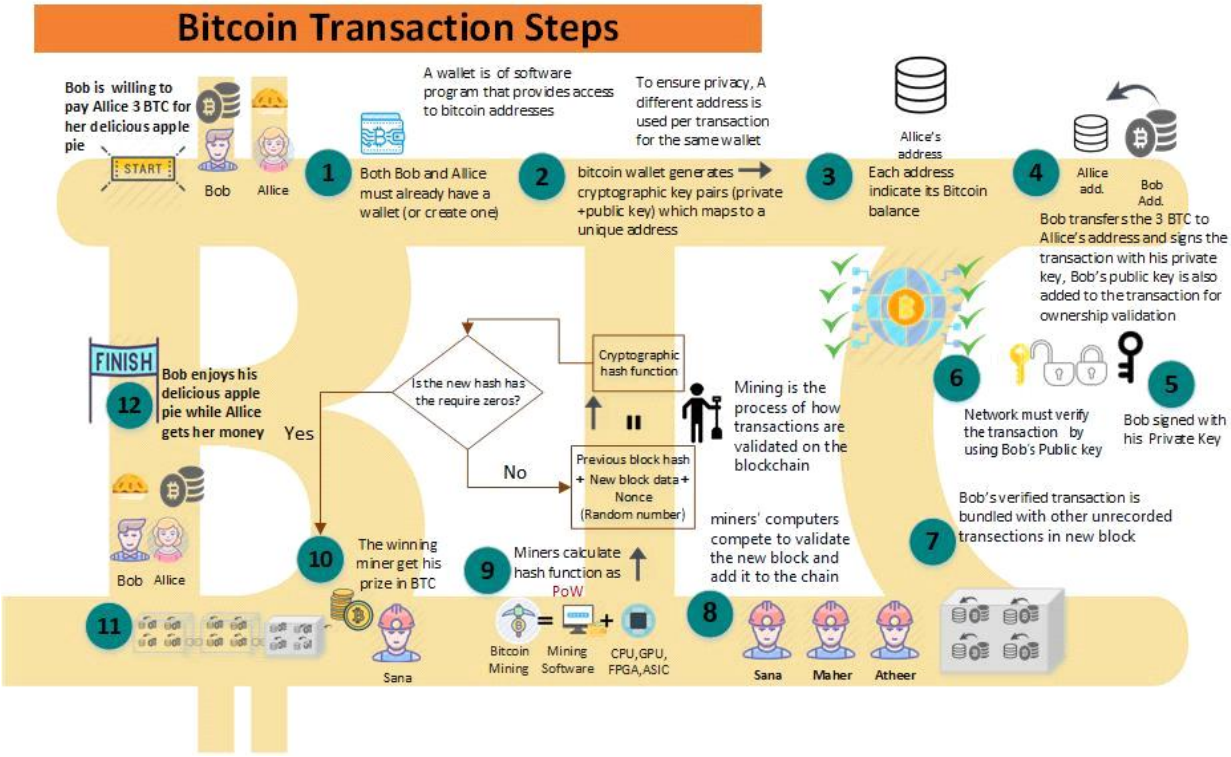

Figure 4. Bitcoin transaction steps

The programmable platform capabilities of Ethereum has made it attractive to users as it allows the creation of individual cryptocurrency by the users which can be used to launch and pay for smart contracts while having its own cryptocurrency (ether) for service payments. Ethereum has already found application in several fields, such as keyless access, Governance, crowdfunding, autonomous banks, financial derivatives trading & settlement; these applications depend on the use of the smart contract

Ethereum blockchain executes the smart contracts Etherum end-user (miners) locally; as a result, miners' computational resources were consumed. For resource usage limitation and reaping miners for that usage, gas concept was used, as a fee.

Based on a user-defined gas price, the gas cost is converted to Ether, i.e. the amount of Ether-per-gas that the initiator of a transaction is prepared to pay. Normally, the gas price is set by default to a market rate by the users (this is often the average of the previously considered transactions).

There is another concept related to the smart contract which is the decentralized applications (DApp). It is an open source software that leverage on the blockchain technology and built partly with Ethereum smart contracts. Decentralized apps connect users and providers directly without the need for the third party. The backend of a DApp is executed in a decentralized environment. This is different from the backend of normal apps which are executed on a centralized server. A DApp, like a normal app, can have frontend code and user interfaces that interact with its backend through an API. The frontend can be hosted as a website on a centralized server.

To fully understand Ethereum, the same scenario with Bob and Allice was considered as in the following steps:

- Allice builds her DApp on Ethereum platform to sell her delicious apple pies.
- Bob accesses Allices' DApp through his mobile or computer and orders one of her pies.
- Bobs' request is distributed to a network of independent nodes instead of one server; these nodes (Ethereum end users) are owned by people like Allice and Bob and each one contributes to the work; they are called "Mist".
- Every node receives a reward (in Ether) for effort and computational recourses.

- Bob then pays the apple pies' price (in Ether) in almost the same steps as in a Bitcoin transaction with miners and PoW.
- The Ethereum transactions cost (called Gas) is set according to the bandwidth used, computational complexity, and storage space.
- Bob enjoys his delicious apple pie while Allice gets her money.

All these steps are summarized in Figure 5.

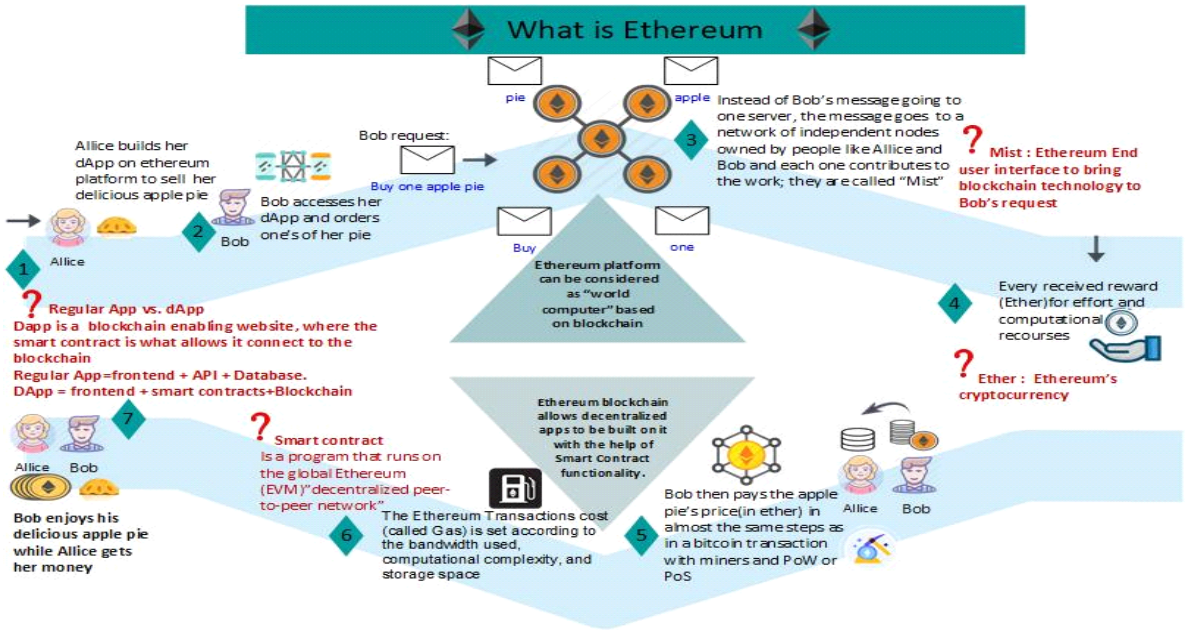

Figure 5. Different steps in the execution of smart Ethereum network

4.3. Business to business blockchains (B2B)

Here, no currency is supported, but software execution is supported for business logic, such as Hyperledger project. With the distinctive nature of each industry or business in their own way, their respective needs must be served with personized applications as well. The Ethereum blockchain network deploys a highly generalized protocol for everything that runs on its network. For instance, Hyperledger can be considered as software that helps people to develop personalized blockchains which will tend to their specific business needs. Organizations have started deploying blockchain technologies which are specifically developed for their specific needs in order to overcome some of the challenges with other types of blockchain, issues like privacy, scalability, and lack of governance [30, 31].

Unlike the other two blockchain types which rely on cryptocurrency, Hyperledger benefits from DLT without depending on any cryptocurrency [32]. Hyperledger is an umbrella project which has been hosted as a global partnership (of open-source blockchains and related tools) by the Linux Foundation since December 2015. Its membership cuts across several sectors, including finance, Internet of Things[33], banking, manufacturing, supply chain, and technology. Hyperledger system does not require the embedding of cryptocurrency or any form of mining operation [34]; it only allows users to develop the personalized private blockchain applications. Several blockchain projects like Sawtooth, Iroha, Fabric, Burrow, Indy, Caliper, and Cello are offered by Hyperledger system.

Hyperledger specification has several implementations from different vendors, such as Fabric, Sawtooth Lake, Corda, Iroha, Geid, and Burrow. Further discussions will focus on a specific blockchain platform, which is Hyperledger fabric. Figure 6 illustrates an overview about the hyperledger.

Fabric is a "modular and extensible open-source system for deploying and operating permissioned blockchain". It is the first truly extensible blockchain system for executing distributed applications. As it supports modular consensus protocols, it allows the building of a system based on the specific use cases and trust models. Fabric remains the first blockchain system to execute distributed applications which are written in multi-purpose standard programming languages without necessarily depending on any cryptocurrency [3].

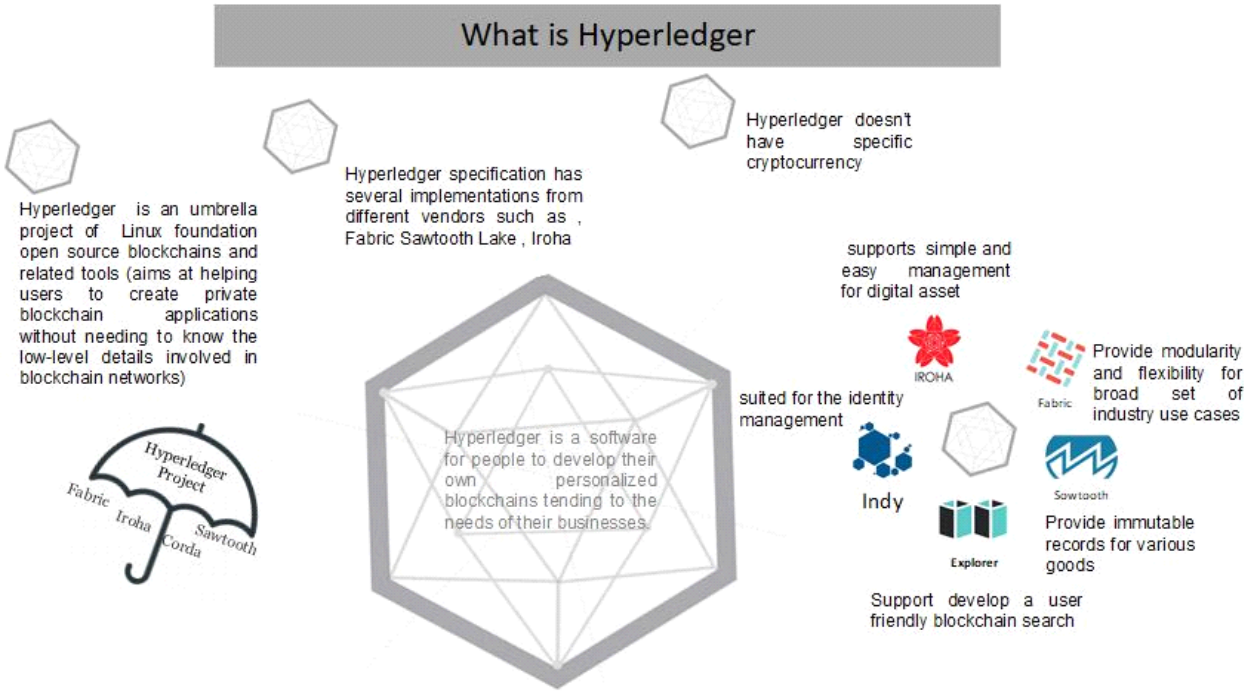

Figure. 6. Hyperledger fabric

Fabric overview

As a permission-based blockchain, Hyperledger demands all potential users to register and obtain a unique identity before trying to access the platform and submit transactions.

Both the registration process and the management of users' identity is the sole responsibility of Fabrics' Membership Services. The system is comprised of both clients, validating and non-validating peers. The validating peers perform the consensus agreement; they validate and execute the transactions via smart contracts (or chain codes); they also update the ledger. Non-validating peers are also supported in Fabric; as their name implies, they perform the non-consensus-related network tasks. Evidently, the core element of this framework is the validating peers. However, the scalability of network can be hindered by placing key functionalities chain code and consensus execution" within the same blockchain node. For instance, different transactions should not be parallelly validated since all the validators must sequentially execute them by summoning the chain codes and running consensus on each of them. Plans for the release of Fabric version 1.0 which comes with significant architectural changes to improve its scalability and modularity are on the way [35]. Table 1 summarized the differences between Bitcoin, Ethereum and Hyperledger Fabric.

Table 1. Differences between bitcoin, ethereum, and hyperledger fabric

	Bitcoin	**Ethereum**	**Hyperledger Fabric**
Currency	Bitcoin	Ether	No currency
Scalability	Low	Low	High
Legal status	Some countries like	Some countries like	Legal

	Bitcoin	Ethereum	Hyperledger Fabric
	the European Union allow the use of Bitcoin while others such as Canada have legal restrictions. Countries like Iran prohibit their usage.	the European Union allow the use of Bitcoin while others such as Canada have legal restrictions. Countries like Iran prohibit their usage.	
minor	Yes (ASIC)	Yes (GPUs)	No minors
Latency	10 min	12-14 sec	< 1 sec
Data Confidentiality	No	No	yes
Throughput	7 Tx/s	9-10 Tx/s	Can achieve thousand Tx/s
Programming Language	C++	Solidity	Written in general purpose programming languages (e.g., Go, Java, Node.js).
Applications	Only cryptocurrency (financial)	Smart contract Cryptocurrency (multiple applications)	Smart contract (chaincode) (multiple applications)
User authentication	Digital signature (public + private keys)	Digital signature (public + private keys)	Membership certificate
Future research opportunities	Low	High	High

5. Conclusion

The blockchain is highly appraised for its decentralized infrastructure and P2P nature. However, many blockchain researchers have focused on Bitcoin only and have classified blockchain into private and public. However, blockchain could be applied to many fields beyond only cryptocurrency. Blockchain realizes trust and security by using software programs to verify and validate consensus in new infrastructure. We first provided an overview of the blockchain concept, including transaction, consensus algorithms, and hashing. Then, we categorized blockchains into three novel types (Cryptocurrency blockchain C2C, Business to Cryptocurrency blockchain B2C and business to business blockchain B2B) based on their overall system and applications; we also made a comparison between these different types of blockchain. Furthermore, we presented detailed scenarios for Bitcoin and Ethereum transaction to give a complete overview of these blockchain types. Finally, we provided the differences between Bitcoin, Ethereum and Hyperledger Fabric. This paper's main goal is to provide a roadmap to blockchain developers and researchers when choosing the right type of blockchain that suits their needs. With the advancements in blockchain-based application, our future plan is to comprehensively investigate blockchain technology based on application and smart contract.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, *et al.*, "A taxonomy of blockchain-based systems for architecture design," in *2017 IEEE International Conference on Software Architecture (ICSA)*, 2017, pp. 243-252.

[3] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*, 2018, p. 30.

[4] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: current status, classification and open issues," *Telematics and Informatics*, 2018.

[5] M. C. Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: beyond Bitcoin," *Sutardja Center for Entrepreneurship&Technology*, 2015.

[6] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, p. 218, 2016.

[7] C. Holotescu, "Understanding blockchain technology and how to get involved," *The 14thInternational Scientific ConferenceeLearning and Software for EducationBucharest, April*, pp. 19-20, 2018.

[8] H. Atlam, R. Walters, and G. Wills, "Fog computing and the internet of things: a review," *big data and cognitive computing*, vol. 2, p. 10, 2018.

[9] N. Bozic, G. Pujolle, and S. Secci, "A tutorial on blockchain and applications to secure network control-planes," in *2016 3rd Smart Cloud Networks & Systems (SCNS)*, 2016, pp. 1-8.

[10] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond Bitcoin," *Applied Innovation*, vol. 2, p. 71, 2016.

[11] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, pp. 183-187, 2017.

[12] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, 2017, pp. 557-564.

[13] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, pp. 352-375, 2018.

[14] M. Niranjanamurthy, B. Nithya, and S. Jagannatha, "Analysis of Blockchain technology: pros, cons and SWOT," *Cluster Computing*, pp. 1-15, 2018.

[15] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, pp. 2084-2123, 2016.

[16] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, *et al.*, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable and Sustainable Energy Reviews*, vol. 100, pp. 143-174, 2019.

[17] W. Yang, S. Garg, A. Raza, D. Herbert, and B. Kang, "Blockchain: trends and future," in *Pacific Rim Knowledge Acquisition Workshop*, 2018, pp. 201-210.

[18] H. F. Atlam and G. B. Wills, "Technical aspects of blockchain and IoT," *Role of Blockchain Technology in IoT Applications*, vol. 115, p. 1, 2019.

[19] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in *Banking beyond banks and money*, ed: Springer, 2016, pp. 239-278.

[20] A. Kiayias, I. Konstantinou, A. Russell, B. David, and R. Oliynykov, "A Provably Secure Proof-of-Stake Blockchain Protocol," *IACR Cryptology ePrint Archive*, vol. 2016, p. 889, 2016.

[21] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *OSDI*, 1999, pp. 173-186.

[22] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," *Applied Energy*, vol. 195, pp. 234-246, 2017.

[23] W. Gao, W. G. Hatcher, and W. Yu, "A Survey of Blockchain: Techniques, Applications, and Challenges," in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, 2018, pp. 1-11.

[24] MoinMarketCap. (2019, May 10,2019). *Top 100 Cryptocurrencies by Market Capitalization*. Available: https://coinmarketcap.com/

[25] M. Morisse, "Cryptocurrencies and Bitcoin: Charting the research landscape," 2015.

[26] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *Ieee Access*, vol. 4, pp. 2292-2303, 2016.

[27] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 254-269.

[28] V. Buterin, "A next-generation smart contract and decentralized application platform," *white paper*, 2014.

[29] D. Vujičić, D. Jagodić, and S. Ranđić, "Blockchain technology, Bitcoin, and Ethereum: A brief overview," in *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*, 2018, pp. 1-6.

[30] T. Eguchi, H. Ohsaki, and M. Murata, "On control parameters tuning for active queue management mechanisms using multivariate analysis," in *Applications and the Internet, 2003. Proceedings. 2003 Symposium on*, 2003, pp. 120-127.

[31] W. Li, A. Sforzin, S. Fedorov, and G. O. Karame, "Towards scalable and private industrial blockchains," in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, 2017, pp. 9-14.

[32] M. Vukolić, "Rethinking permissioned blockchains," in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, 2017, pp. 3-7.

[33] S.S. Sabry, N.A. Qarabash, and H.S Obaid, "The Road to the Internet of Things: a Survey".In *2019 9th Annual Information Technology, Electromechanical Engineering and Microelectronics Conference (IEMECON)*, 2019, pp.290-296.

[34] Y. Lu, "The Blockchain: State-of-the-Art and Research Challenges," *Journal of Industrial Information Integration*, 2019.

[35] V. Dhillon, D. Metcalf, and M. Hooper, "The hyperledger project,"