IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 3, December 2021
Impact Factor: 5.731

Blockchain and Distributed Ledger Technology-Survey

Dr. S. Sobana[1], Nibin M S[2], Soorya K P[3], Muhammed Rufaid A[4], Silpa A K[5]
Sree Saraswathi Thyagaraja College, Pollachi, Tamil Nadu, India[1]
Students, Department of Computer Science & Engineering[2,3,4]
Assistant Professor, Department of Computer Science & Engineering[5]
Vedavyasa Institute of Technology, Malappuram, Kerala, India

Abstract: *Block chain technology is a form of distributed ledger technology. A block chain is a distributed ledger to transfer ownership, record transactions, track assets, and ensure transparency, secure and value exchanges in various types of transactions with digital assets. Distributed ledgers such as block chain are exceedingly useful for financial transactions because they cut down on operational inefficiencies. They also provide greater security due to their decentralized nature, as well as the fact that the ledgers are immutable. Distributed ledger technology has attracted significant attention with the tremendous development of crypto currencies.*

Keywords: Block chain

I. INTRODUCTION

A distributed ledger is essentially a consensus of replicated, Block chain is a continuously growing list of records, called blocks, linked and secured using cryptography. Block chain is a set of protocols/mechanisms that can help to verify and recognize each transaction by enabling all of the untrusted participants to come to a distributed consensus. Block chain has the potential to revolutionize the World, especially the digital world, by realizing distributed transactions, or a set of transactions, between unknown persons.

II. VIRTUALIZATION FOR DISTRIBUTED LEDGER TECHNOLOGY

Since ancient times, ledgers have been at the heart of economic activities. Although the invention of computers and the Internet provides the process of record keeping with great convenience, the basic principle has not been changed - ledgers are usually centralized. Recently, with the tremendous development of crypto-currencies (e.g., Bitcoin), the underlying distributed ledger technology (DLT) has attracted significant attention. A distributed ledger is a consensus of replicated, shared and synchronized data geographically spread across a network of multiple nodes. Here, there is no centralized data storage. Using a consensus algorithm, any changes to the ledger are reflected in the cop Block chain is considered the heart of Bitcoin. Block chain is a continuously growing list of records, called blocks, linked and secured using cryptography. Nevertheless, not all distributed ledgers have to necessarily employ a chain of blocks to

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 3, December 2021
Impact Factor: 5.731

successfully provide secure achievement of distributed consensus: a block chain is only one type of data structure considered to be a distributed ledger. Besides block chain, there are other data structures to implement DLT, such as directed acyclic graph (DAG), which is at the heart of IOTA. The transactions issued by nodes constitute the site set of the DAG, which is the distributed ledger for storing transactions.DLT has great potential to create new foundations for our economic and social system .DLT is making waves in industries such as finance; music and entertainment; diamond and precious assets; artwork; supply chains of various commodities; and more. While DLT has many advantages, it is in a nascent stage and still being explored to adopt in the best possible ways.

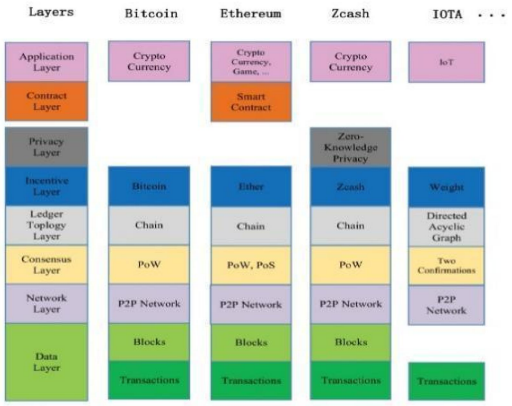


FIGURE 4. Different layers in some existing distributed ledger technology (DLT) systems.

In this paper, we present a novel virtualization attitude to address the challenges in the existing DLT systems. The contributions of this work are given below

- We survey the virtualization approaches in the IT landscape, including computing, OS, software, and networks. Then, we show that virtualization will be the next step to address the challenges in the existing DLT systems.
- We reviewed the layered model for the existing DLT systems, and presented the architecture of virtualization for DLT (vDLT). The application programming interface (API) of vDLT is described.

2.1 From the Internet of Things to the Internet of Value

The traditional internet was originally designed to handle the exchange of information, e.g., using websites and emails. It was not designed to handle the exchange of actual value. Anyone who transferring the money online is not actually moving the value directly. In order to successfully implement the Internet of value, we can take a look at the successful architecture of the Internet of information. Figure 1-(a) shows the hourglass architecture centering on the universal network layer (i.e., IP), which implements the basic functionality necessary for global interconnectivity.

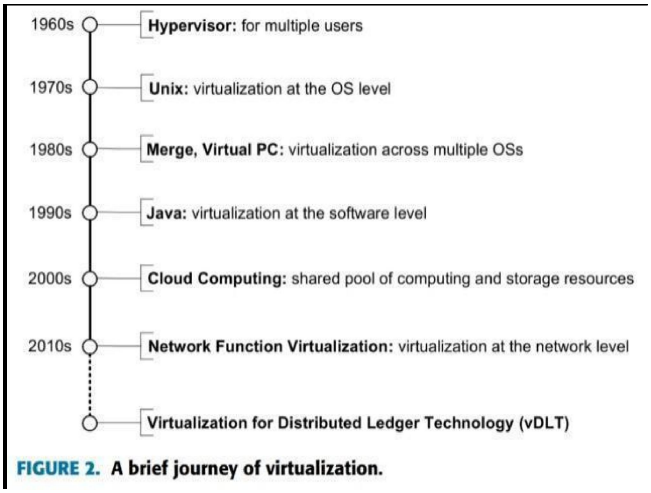


FIGURE 2. A brief journey of virtualization.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 3, December 2021
Impact Factor: 5.731

2.2 Virtualization for Computing and Storage

Virtualization has been revolutionizing the ways in which IT is developed, and traces its root all the way back to the 1960s. Hypervisor software, a term coined in 1966, was the original conceptualization of what would become virtualization. It is software that is used to create and runs virtual machines. The word is portmanteau of the prefix ‘‘hyper, ’meaning ‘‘above,’’ and ‘‘supervisor,’’ the primitive operating systems in use at the time. It had supported 14 machines simultaneously. The main advantages of using virtual machines vs a time-sharing operating system (OS) was a more efficient use of the system since virtual machines were able to share the overall resources of the mainframe, instead of having the resources split equally between all users. Figure 2 shows a brief journey of virtualization. We can see abstract the underlying resources, so that people can focus on the things they care the most. Now, we can have access to hardware, OS, software, storage, and network via virtualization (network virtualization will be described in the next subsection). Therefore, we believe that virtualization will be naturally the next step for DLT.

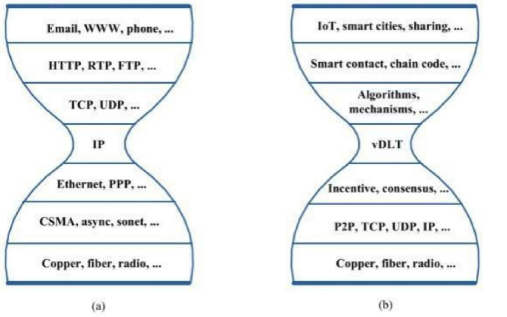


FIGURE 1. The architectures of (a) Internet of information and (b) Interne of value.

2.3 Virtualization for Networks

With the tremendous growth in the Internet traffic and services, it is quite natural to extend the success of virtualization from computing and storage to networks. Recently, network virtualization has been actively used in Internet research test beds, such as G-Lab [26] and 4WARD [27]. It aims to overcome the resistance of the current Internet to fundamental architecture changes. Network virtualization has been considered as one of the most promising technologies for the future Internet [28]. Particularly, the NFV concept was presented by a group of network service providers in 2012.These service providers wanted to simplify and speed up the process of adding new network functions or applications. Individual virtual network functions (VNFs), are an essential component of NFV architecture. Because NFV architecture virtualizes the network functions and eliminates specific hardware, network managers can add, move or change the network functions at the server level in a simplified provisioning process. Figure 3 show the comparison between the traditional network appliance approach and the NFV approach.

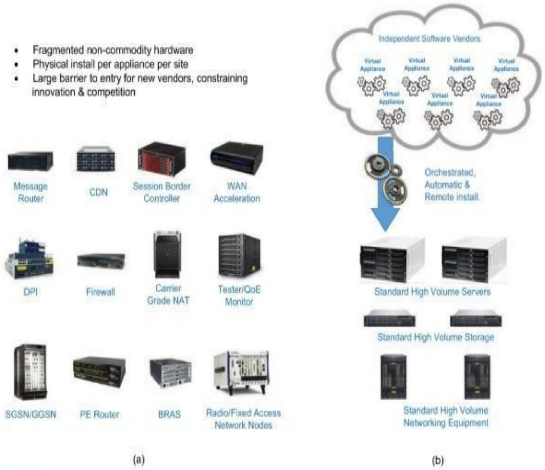


FIGURE 3. Comparison between (a) classical network appliance approach and (b) network function virtualization (NFV) approach.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 3, December 2021
Impact Factor: 5.731

2.4 Virtualization for Distributed Ledger Technology

The existing DLT systems can be divided into several layers, including data layer, network layer, consensus layer, ledger topology layer, incentive layer, privacy layer, contract layer, and application layer, as shown in Fig. 4.The data layer in the DLT architecture encapsulates the data generated from different applications. In the blockchain form of DLT, each block contains a number of transactions, and is ‘‘chained’’ back to the previous block, resulting in an ordered list of blocks. There are mainly two parts in each block: the block header and the block body. The block header specifies the metadata, including hash of previous block, hash of current block, timestamp, Nonce and Merkle root. The block body stores the verified transactions. In the DAG form of DLT, instead of blocks, data are added directly to a graph of transactions, which reference previous transactions.DLT has a great potential to create new foundations for our economic and social systems by efficiently establishing trust among people and machines, reducing cost, and increasing utilization of resources.

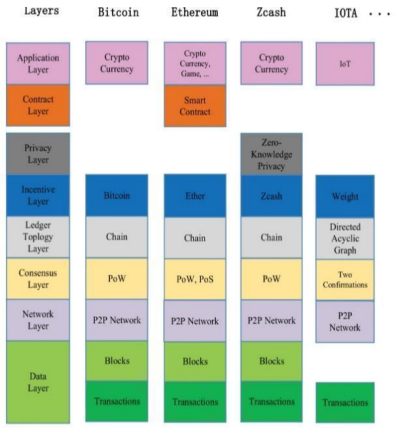
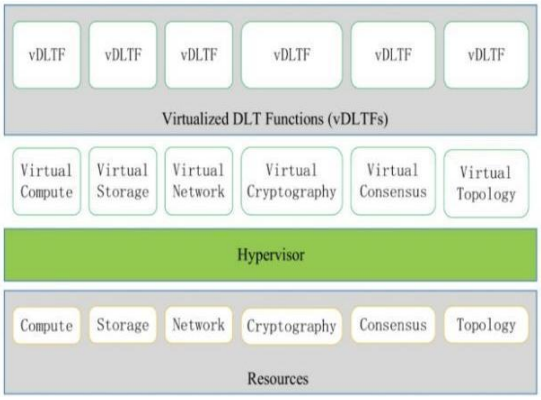


FIGURE 4. Different layers in some existing distributed ledger technology (DLT) systems.

2.5 The Architecture of Virtualization for Distributed Ledger Technology

Fig. 5 shows the architecture of vDLT. The resources consist of networking, compute, and, storage, cryptography, consensus and topology resources. Virtual resources are abstractions of the physical resources. The abstraction is achieved using a virtualization layer (based on a hypervisor), which decouples the virtual resources from the underlying physical resources.



2.6 Application Programming Interface of vDLT

Open interfaces and clearly defined reference points are key to accelerate the deployment of vDLT. This approach allows multiple parties to independently develop the building blocks of the vDLT architecture and enables different application to pick the solutions and implementations best suited to their application needs. At the same time, the use of established standards, protocols and interface technologies, e.g. from OpenStack, is highly desirable to shorten time to

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 3, December 2021
Impact Factor: 5.731

develop the vDLT framework on a broad basis. For the software implementation, an open framework based on open-source software is the most flexible approach and avoids a lock-in with any particular component.

The underlying distributed ledger technology of crypto-currencies has great potential to create new foundations for our economic and social systems. However, the existing DLT has a number of drawbacks, including scalability, ossification and specialization, etc. In this paper, we are presenting a novel virtualization approach to address the challenges in the existing DLT systems. Specifically, in the proposed virtualization for DLT (vDLT), the underlying resources (e.g., hardware, compute, storage, network, and so on) are abstracted.

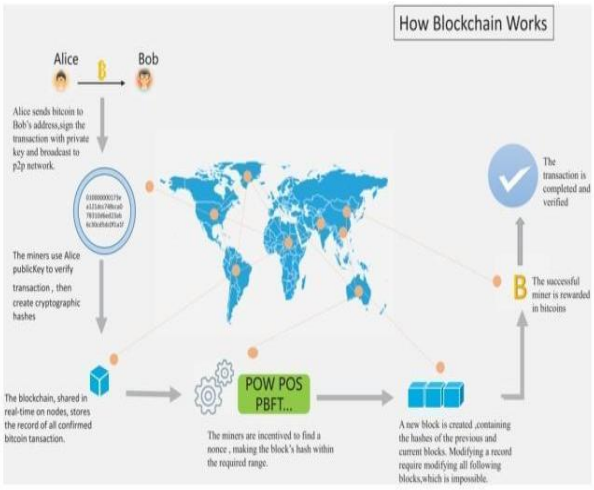
III. Literature Survey

3.1 A Low Storage Room Requirement Framework for Distributed Ledger in Blockchain

Traditional centralized commerce on the Internet relies on trusted third parties to process electronic payments. A pure decentralized mechanism called block chain tackles the above problem and has become a hot research area. However, since each node in a block chain system needs to store all transactions of the other nodes, as time continues, the storage room required to store the entire block chain will be huge. Commerce on the Internet has come to rely relatively exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust-based model. The block chain technique, which is a distributed solution of the trust problem without any third party, is a promising substitution. In the following sections, we briefly illustrate the history of the technique development.

A. Brief Introduction to Block Chain

In general, block chain is a set of protocols/mechanisms that can help to verify and recognize each transaction by enabling all of the untrusted participants to come to a distributed consensus. Block chain has the potential to revolutionize the world, especially the digital world, by realizing distributed transactions, or a set of transactions, between unknown participants.



The basic idea of block chain can be explained by its two typical applications as follows.

Mechanism of block chain in Bitcoin: Each transaction is broadcast to every node in the Bitcoin network and is then recorded in a public ledger after verification. Every single transaction is needed to be verified for validity before it is recorded in the public ledger. A verifying node needs to ensure the following two things before recording any transaction [1]: (1) The spender owns the cryptocurrency-digital signature verification on the transaction.

B. Bloat Problem in Blockchain

As described in the previous subsection, block chain requires that each node stores all the transactions generated by all the nodes. Therefore, the volume of data stored at each node increases linearly with respect to n 2, where n denotes the number of nodes in the system. Moreover, it also increases linearly with time. The above two factors may cause the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 3, December 2021
Impact Factor: 5.731

following problems: (1) a lack of storage room at each node, especially for portable devices [4], and (2) non-sustainable development of the system size, which may require much bandwidth for the initial synchronization of the new participant. The above two problems can be called the storage bloating problem. For example, currently, one entire block chain in a Bitcoin network takes up 66 GB, and this number is continually increasing by 0.1 GB per day.

C. Proposed NC-DS Framework for Blockchain

In this section, we propose a network coding-based distributed storage (NC-DS) framework for block chain. This part is embedded into the existing block chain system. Compared to Fig. 1, only the process of the inserted part is shown, and the remaining part is the same as that shown in Fig. 1 and hence are not drawn in this figure.

For the example in Fig. 2, we may adopt the (6, 3) code illustrated in Fig. 3. In this example, the new generated block is partitioned into 3 equal-length sub-blocks, namely A, B,C as shown in blue color. These three sub-blocks are then encoded into 6 sub-blocks as shown in red color according to a particular (6, 3) combination property (CP) code illustrated in Fig. 3. Detailed illustration of the (6, 3) code may refer to sub sec. II-A. Correspondingly, when the system fetches these encoded blocks, they need to perform decoding before normal block chain procedure.

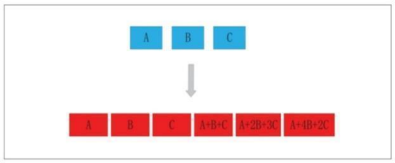


FIGURE 3. An optional (6, 3) code for the red sub-blocks in Fig. 2.

D. Analysis of Proposed Scheme

We analyze the proposed framework from the viewpoint of storage room, bandwidth, consensus speed, and scalability.

E. Storage Room

As previously described, our proposed NC-DRDS uses 1/k of the storage room used by existing block chain systems. With respect to our proposed NC-RLDS, especially the random shift method, the utilization of storage room is slightly larger than 1/k due to storage room overhead induced by shift.

F. Bandwidth Consumption for Data Dissemination Within the Network

After the first user finishes his computation, he needs to disseminate his data to all nodes in the system. In the traditional block chain system, the bandwidth consumption is n times that of the data volume of the disseminated data. For our proposed framework, the volume of data to be disseminated is 1/n of the original.

G. Consensus Speed

The processing order is as follows: After each new block reaches consensus, this block is then network coded and appended in each block chain and stored using our proposed storage framework. Therefore, our proposed storage framework has no effect on consensus speed. For the case when there are multiple parallel sub-chains, we need to first perform decoding from those coded blocks and then perform a consensus process. There is only certain additional decoding procedure.

H. Scalability

Our proposed NC-DRDS and NC-RLDS can scale with respect to network size automatically. Firstly, for NC-DRDS, the encoded packets are output sequentially which suits scalability. Secondly, for NC-RLDS, the random shift also suits scalability since the scope of the number of shifts can be adjusted and properly designed. In this paper, we adopt a network coded (NC) distributed storage (DS) framework to store the block chain to save storage room. Trivial application of NC-DS to block chain is difficult because the parameter is difficult to set. We propose two solutions to tackle this problem. Analysis shows that the proposed scheme indeed achieves significant improvement in saving storage room.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 3, December 2021
Impact Factor: 5.731

3.2 Decrypting Distributed Ledger Design-Taxonomy, Classification And Blockchain Community Evaluation

Over 1000 systems have emerged in recent years from distributed ledger technology (DLT), raising $600 billion in investment in 2016. They power a large scale of novel distributed applications making use of changelessness, integrity, and fair access, and transparency, rejection of dealings4 and crypto currencies. These applications include improving supply-chains, IoT, creating self-sovereign identity, establishing peer-to-peer energy markets, and securing digital voting, e-health and enabling international financial transactions. The most well-known DLT system is Bitcoin, featuring a novel consensus mechanism and a crypto economic design (CED), which enables untrusted parties to reach consensus. Bitcoin is the first public DLT system that prevents double-spending4 and Sybil attacks.

These crypto economies rely on digital currencies referred to as tokens and cryptographic techniques to regulate how value is exchanged between the participating actors. The options and choices of a crypto wealth are referred to as crypto economic design (CED) and this plays a major role in the stability of a DLT system in terms of convergence, liveness, and fairness. This paper derives a useful6 anatomy of DLT systems from a novel conceptual architecture. This anatomy is then exploited to classify 50 viable and actively keep going DLT systems. In contrast to earlier work, a novel evaluation methodology is employed that solicits feedback from the block chain community and constructively uses it to validate and further improve the proposed taxonomy and classification. Moreover, the classification data are utilized to quantitatively reason about key design choices in the observed DLT systems, which then, in turn, determine a design guideline for DLT systems. To make this design guideline objective, this paper relies on systematic methods that combine in a novel way (i) literature review, (ii) novel data collection and (iii) ML-based data analysis. In particular, the data-driven approach results in a guideline that structures the modeling complexity of DLT systems and thus accelerates and simplifies the design phase by grouping together system design configurations derived from the attribute values of the taxonomy. The contributions of this paper are outlined as follows:

1. A conceptual architecture that models DLT systems with four components. The architecture (Fig. 1) defines minimal and insightful design elements to illustrate the inner mechanics of distributed ledgers and the interrelationships of their components.
2. A taxonomy (Fig. 2) of distributed ledgers that formalizes a set of 19 descriptive and qualitative attributes, including a set of possible values for each attribute.
3. A classification of fifty DLT systems, including Bitcoin and Ethereal, backed by an extensive literature review.
4. A taxonomy evaluation criterion referred to as ‘expressiveness’ derived from earlier theory on taxonomies.
5. Crowd sourced feedback from the block chain community to further assess and improve the taxonomy and classification.
6. A design guideline for DLT systems (Fig. 12), which is constructed using machine learning techniques to reason based on empirical data of viable, actively maintained and academically referenced DLT systems.
7. A methodology (Fig. 3) that utilizes a broad spectrum of interdisciplinary methods to derive system design guidelines by reasoning based on machine learning techniques, wisdom of the crowd and taxonomy theory.

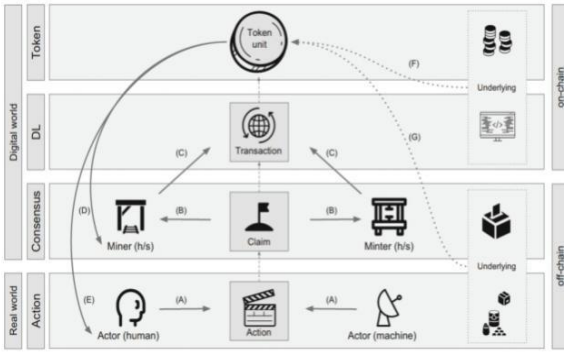


Fig. 1 An overview of the conceptual architecture containing the four key concepts of DLT systems and their relationship: action, consensu distributed ledger and token

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 3, December 2021
Impact Factor: 5.731

A. Distributed Ledger

A distributed ledger is established as a distributed data building, containing entries that serve as digital records of actions. In the Bitcoin system, an appearance in the data structure is called a block. An appearance contains a set of dealings (Fig. 1, DL component). In Bitcoin, these transactions represent the swapping of crypto currency worth. The assign of the distributed ledger are data building, origin, address trackable and Turing completeness. Data structure designates in which format data is set aside on the distributed ledger. It can be one of the following: Block chain, directed open-chain graph or other. The well-known data structure is a block chain; an changeable and append-only linked list that has a total order of elements. Several systems use block chains, such as Bitcoin, Reuther and Lite coin. When compared to Block chains, DA's trade off security against a higher dealings throughput by smooth fast entry confirmation times [28]. Ripple uses neither a block chain nor a directed open-chain graph but instead makes use of other agreement-based accounting appliances.

This paper concludes that the evolving complexity of distributed ledgers can be better understood via a proposed anatomy of DLT systems designed according to standards of state-of-the-art anatomy theory. To support such understanding, this paper contributes a systematic and rigorous classification of 50 viable and actively maintained DLT systems into the taxonomy using sagacity of the crowd and machine learning methods fed with real-world data.

IV. Conclusion

This paper concludes that the evolving complexity of distributed ledgers can be better understood via a proposed anatomy of DLT systems designed according to standards of state-of-the-art anatomy theory. To support such understanding, this paper contributes a systematic and meticulous classification of 50 viable and actively maintained DLT systems into the anatomy` using sagacity of the crowd and machine learning methods fed with real-world data. From that data a novel procedure is derived that identifies key design choices that govern the difficulty of distributed ledgers. The contributed guideline is a result of a novel data-driven methodology that structures the modeling difficulty of DLT systems at design phase and thus can support the business and distributed computing community to fabricate. Where there is room for innovation and which systems have ruthless features or shared designs.

References

[1]. S. Nakamoto. (Oct. 2018). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[2]. Distributed Ledger Technology: Beyond Block Chain, UK Government, Office Sci., London, U.K., 2016.
[3]. IOTA. Accessed: Apr. 26, 2018. [Online]. Available: https://iota.org
[4]. M. Iansiti and K. R. Lakhani, ‘‘The truth about blockchain,’’ Harvard Bus. Rev., vol. 95, pp. 118–127, Jan. 2017.
[5]. Ethereum. Accessed: Apr. 26, 2018. [Online]. Available:https://www.ethereum.org/
[6]. Ripple. Accessed: Apr. 26, 2018. [Online]. Available: https://ripple.com/
[7]. J. Pearson. Bitcoin Unlimited’ Hopes to Save Bitcoin from Itself. Mother- board. Accessed: Apr. 26, 2018. [Online]. Available: https://motherboard.vice.com/enus/article/wnx7vz/bitcoinunlimited-hopes-to-save-bitcoin-from-itself-block-size
[8]. SegWit. Accessed: Apr. 26, 2018. [Online]. Available: https://segwit.org/
[9]. Lighting Network. Accessed: Apr. 26, 2018. [Online]. Available: https://lightning.network/
[10]. Raiden Network. Accessed: Apr. 26, 2018. [Online]. Available: https://raiden.network/
[11]. Plasma. Accessed: Apr. 26, 2018. [Online]. Available: http://plasma.io/
[12]. Cardano. Accessed: Apr. 26, 2018. [Online]. Available: https://cardano.org
[13]. J. A. Cunningham, P. Meissner, and C. A. Kettering, ‘‘A computer for weather data acquisition,’’ in Proc. Int. Workshop Manag. Requirements Knowl., New York, NY, USA, Dec. 1960, pp. 57–66.
[14]. K. Flamm, Creating the Computer: Government, Industry, and High Technology. Washington, DC, USA: Brookings Institution, 1988.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 3, December 2021
Impact Factor: 5.731

[15]. S. T. King and S. W. Smith, ‘‘Virtualization and security: Back to the future,’’ IEEE Secur. Privacy, vol. 6, no. 5, p. 15, Sep. 2008.

[16]. V. Salapura, ‘‘Cloud computing: Virtualization and resiliency for data center computing,’’ in Proc. IEEE 30th Int. Conf. Comput. Design (ICCD), Sep. 2012, pp. 1–2.

[17]. S. Nakamoto. (Oct. 2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://www.cryptovest.co.uk/

[18]. C. Xu, K. Wang, and M. Guo, ‘‘Intelligent resource management in blockchain-based cloud datacenters,’’ IEEE Cloud Comput., vol. 4, no. 6, pp. 50–59, Nov. 2017.

[19]. M. Crosby, P. P. Nachiappan, S. Verma, and V. Kalyanaraman, ‘‘BlockChain technology—Beyond bitcoin,’’ SCET, Berkeley, CA, USA, Tech. Rep. Rev 2:6–19, Oct. 2015.

[20]. K. Wang, J. Mi, C. Xu, Q. Zhu, L. Shu, and D. J. Deng, ‘‘Real-time load reduction in multimedia big data for mobile Internet,’’ ACM Trans. Multimedia Comput., Commun. Appl., vol. 12, no. 5, Oct. 2016, Art. no. 76.

[21]. Null. (May 2017). Scalability: Bitcoinwiki. [Online]. Available: https://en.bitcoin.it/wiki/Scalability

[22]. R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, ‘‘Network information flow,’’ IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[23]. A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, ‘‘Network coding for distributed storage systems,’’ IEEE Trans. Inf. Theory, vol. 56, no. 9, pp. 4539–4551, Sep. 2010.

[24]. A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, ‘‘A survey on network codes for distributed storage,’’ Proc. IEEE, vol. 99, no. 3, pp. 476–489, Mar. 2011.

[25]. P. Vingelmann, P. Zanaty, F. H. P. Fitzek, and H. Charaf, ‘‘Implementation of random linear network coding on OpenGL-enabled graphics cards,’’ in Proc. IEEE EW, Aalborg, Denmark, May 2009, pp. 1–5.

[26]. [26] M. Shahabinejad, M. Khabbazian, and M. Ardakani, ‘‘An efficient binary locally repairable code for Hadoop distributed file system,’’ IEEE Commun. Lett., vol. 18, no. 8, pp. 1287–1290, Aug. 2014.

[27]. M. Dai, C. W. Sung, H. Wang, X. Gong, and Z. Lu, ‘‘A new zigzag-decodable code with efficient repair in wireless distributed storage,’’ IEEE Trans. Mobile Comput., vol. 16, no. 5, pp. 1218–1230, May 2017.