Blockchain: Trends and Future

Wenli Yang, Saurabh Garg,Ali Raza, David Herbert and Byeong Kang[1]

Discipline of ICT, School of TED, University of Tasmania, Sandy bay, Australia
yang.wenli@utas.edu.au,saurabh.garg@utas.edu.au,ali.raza@utas.edu.au,
david.herbert@utas.edu.au,byeong.kang@utas.edu.au

Abstract. Blockchain has attracted a great deal of attention due to its secure way of distributing transactions between different nodes without a trust entity, and tracking the validity of data. Although many experts argue the solutions to several problems in today's inherently insecure Internet lies with blockchain technology because of its security and privacy features, there is no systemic survey to analyze and summarize blockchain technology from different perspectives. In this paper, we present the current trends in blockchain technology from both technical and application viewpoints and highlight the key challenges and future work required that will help in determining what is possible when blockchain is applied to existing and future problems.

Keywords: Blockchain · Scalability · Crypto-currency

1 Introduction

For the last few decades there has been massive volumes of digital information produced due to the growth of computing technologies such as storage, processing power and networking. On one side, we can see how the maintenance of data has been transformed from purely private information on isolated desktops to completely public data in the form of social networks. On the other side, every IT service is becoming outsourced to third parties in the form of Cloud computing [4]. Moreover, we can see the digital data growth has been so enormous that it is called "Big Data" and it brings more opportunities to innovate and optimize our decisions [13]. However, such growth has also led to grave issues in terms of trust, privacy and security [6]. The problems such as 'Fake News' are also coming into focus [1]. The recent third-party distribution of millions of Facebook user's data has compounded the problem further and it increased public awareness of the issues. Given all of our data is public and maintained in a decentralised manner, it is almost impossible to keep track of such issues. In the real world we find the installment of CCTV cameras to trace criminal activity has not only reduced crime but it has also put fear in the mind of criminals that are being watched. We postulate the question as to whether we have something analogous to CCTV cameras for all of our internet activities that can give some sense of protection for of our data.

Recent development and applications of distributed ledgers such as blockchain has given a glimpse as to how to alleviate such issues [19]. One of the key examples is Bitcoin, which is a decentralized currency that is maintained in an autonomous manner. All transactions processed in Bitcoin are tracked through a "blockchain", where each transaction is verified in a decentraliased manner before it is recorded, preventing any chance of illegitimate transactions occurring. Due to the potential use of blockchain and related technologies to maintain tamper-proof systems that can be maintained in a distributed and autonomous manner, blockchain seems to be the perfect match to make various sectors that operate through a public network such as the Internet accountable. With this aim in mind, this paper will review the various trends in blockchain to understand how it can play an important role in protecting digital data and its usage. Based on the review, we also give a roadmap for future research that is required to make this vision possible.

In summary, the contributions of our research are:

- we provide a detailed evolution of blockchain systems, and discuss technical resources and typical characteristics of different stages of development.
- We describe and categorize trends in blockchain from three criteria: data structure, consensus method and the overall system.
- We introduce several blockchain platforms and compare them using criteria related to usability, limitation, flexibility and performance, and this summary can serve to guide the future blockchain research and development.
- We discuss future challenges in the design of blockchain-based Internet ecosystems, and how the application of AI can guide future implementations.

This paper is organized as following: Section 2 introduces the basic concepts of blockchain. Section 3 outlines the existing data structures used and Section 4 describes blockchain's most common consensus algorithms. In Section 5 we discuss trends in blockchain systems.

2 Blockchain Basics

To understand blockchain, we need to understand the meaning of a distributed ledger. A typical distributed ledger is a shared database that is replicated, and synchronized in a decentralised manner among the different members of a network. The distributed ledger stores the transactional data of the participants in the network. A blockchain is based on Distributed Ledger Technology (DLT) that is spread across several nodes or computing devices [14].

It is assumed that these nodes do not fully trust each other as some may exhibit Byzantine (dishonest) behaviour. These nodes maintain a long chain of cryptographic hash-linked blocks where each modification or addition of a transaction is validated by the consensus of all nodes in the system. In one sense blockchain is similar to a traditional database requiring ACID properties to be satisfied. The key difference is the 'distributed consensus' algorithm which decides whether a new block is valid and legitimate before any insertion can be

done. Based on the membership of the nodes, the blockchain can be either public, private or hybrid [2]. Public blockchains are fully decentralized where any node can join and leave the system. The other two types enforce some restrictions on membership in regard to system access. Hybrid blockchains tries to combine the characteristics of both private and public blockchains – every transaction is private, however it can be verified in the public state. Figure 1 shows the data structure of a blockchain whose basic concepts include:

1. **Transaction:** an operation that caused a change of the block.
2. **Block:** a container data structure, and a block is composed of a header and a long list of transactions.
3. **Chain:** is a continuously growing list of blocks, which are linked and secured using cryptography.

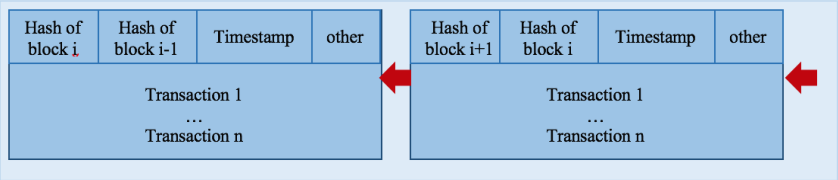

Fig. 1. Blockchain Datastructure

3 Trends in Blockchain Type Data Structure

As stated before, blockchain technology originated from Distributed Ledger Technology (DLT) proposed in the 1990s[18]. Even though DLT was proposed almost 20 years ago, it became prominent with the implementation of Bitcoin and its usage as a crypto-currency in 2008[14]. The initial data structure for blockchain was based on a hash-table, however with its significant growth of usage, it became apparent that new data structures are required for the efficient storage and transmission of information in order to maintain a rapidly growing number of transactions in the ledger. Due to these requirements, several new data structures were proposed for solving the limitations of the traditional blockchain. Some authors [9] suggested the usage of Directed Acyclic Graph (DAG) for maintaining transaction information as it is scalable, light-weight and decentralised. However, this alternative also has similar problems to blockchain at very high scales. Tempo Ledger proposed by RadixDLT aims to scale linearly in an unbounded and efficient manner [16]. In the Tempo ledger, each node can maintain a shard of the whole ledger in comparison to the traditional blockchain implementation where the whole ledger is maintained at each node. We summarised these trends from different perspectives in Table 1.

Table 1. Trends in Blockchain Type Data Structure

Year	1995	2008	2017	2018
DS	MDL	Blockchain	Directed Acyclic Graph or DAG	Tempo ledger
Applications	Sharing Economy Broker and Reinsurance Claim Payment Data Sharing	Cyrptocurrencies eg. Bitcoin, Litecoin, Ripple, Namecoin, etc.	Iota, Raiblocks, Hashgraph, etc.	RadixDLT
TF	High	High	Low	Low
TCT	Several minutes	Several minutes	Minutes	< 5 seconds
Popularity	Launched in 1995, used by a few systems now.	Launched in 2008. Very well known.	Launched in 2017. Not well known yet.	Will be Launched in Q3 2018.

MDL=*Mutual distributed ledger*: a record of transactions shared in common and stored in multiple locations.
DS=key data structure
TF=Transaction fee
TCT=Transaction confirmation time

4 Trends in Consensus Algorithms

Consensus algorithms are designed to achieve reliability in a network involving multiple unreliable nodes. They ensure that the next block in a blockchain is the one and only version of the truth, and it keeps adversarial groups from derailing the system and successfully forking the chain. The most common consensus algorithms include Proof of Work(PoW), Proof of Stake(PoS) [11], Delegated Proof of Stake(DPoS) [11], Ripple [17], Practical Byzantine Fault Tolerance(PBFT) [5] and Delegated Byzantine Fault Tolerance (dBFT). A summary based on different application scenarios and features of the consensus mechanism by the following criteria is presented in Table 2.

- **Data management:** support for whole network nodes and data supervision by privilege nodes.
- **Performance and efficiency:** confirmed efficiency of consensus between transactions.
- **Resource consumption:** high CPU load, storage, network capacity, etc. during consensus processing.
- **Tolerance power:** anti-attacking and cheat-proof capacity.

The PoW protocol is one of the first utilised consensus protocols that is based on computational load, requiring *miners* to find a solution to a puzzle. Several cyrpto-currencies utilise 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 that assigns a difficulty value to a puzzle based on how much *stake* the miner has in the network. Delegated

Proof of Stake (DPoS) is a newer consensus structure where users select some delegate nodes that confirm the validity of a block. Some consensus protocols such dBFT and PBFT are based on communication between different nodes and they are mostly used in private chains having authenticated nodes. Tendermint [12] improves the performance of PBFT by making small modification allowing different nodes with different voting power. The voting power is determined by the stake a user owns in the network. Despite the many modifications to the original consensus protocol, they still fail to scale well. To overcome this, federated protocols such as Ripple were proposed. In these protocols, the whole network is partitioned into smaller units; and each unit runs a local consensus.

Table 2. Consensus algorithm summary

Consensus	PoW	PoS	DPoS	Ripple	Tendermint	PBFT	dBFT
Year	2008	2012	2014	2014	2014	2015	2016
Data management	O	O/P	O/P	O/P	P	P	P
Performance	L	M	M	H	H	H	H
High Resource	yes	partial	partial	no	no	no	no
Tolerance	<= 25%	<= 51%	<= 51%	<= 20%	<= 33.3%	<= 33.3%	<= 33.3%
Application	Bitcoin	Tezos	Lisk	Ripple	Tenderminty	Hyperledger Fabric	Neo

O=Open,P=Permission
L=Low,M=Medium,H=High

5 Trends in Blockchain Systems

Over the past few years, blockchain technology has been evolving rapidly – from the original Bitcoin protocol to the second generation Ethereum platform[15], and today we are in the process of building what is informally termed blockchain 3.0 and future-generational blockchain 4.0 (see Table 3). This evolutionary change shows how the technology is evolving from its initial form as essentially just a database, to becoming a fully-fledged globally distributed system. The applications of blockchain have evolved to much wider scopes than crypto-currency and asset management. Applications from different industries including healthcare and energy sectors are being designed with blockchain as an underlying technology. These application's requirements have also led to structural changes in blockchain itself, which is evolving from linear chains to DAG, with emerging future types of chains such as Relational and Divisible chains.

Blockchain 1.0 is completely dedicated to the decentralization of money and payments, although this was the first implementation of a distributed ledger technology (DLT). It supports the mining of Bitcoins. The network is peer to peer and transactions take place between users directly without the involvement

of any third party. Other crypto-currencies that are recently supported are Litecoin, Dogecoin etc. The technology stack of bitcoin consists of the blockchain platform, and a protocol which is used to describe how assets are transferred. The concensus algorithm utilised is Proof of Work (PoW). Blockchain 1.0 guarantees distributed storage, enables data sharing between nodes, and enables transparency in transaction processing.

In Blockchain 2.0, a logic tier was added into the ledger and which supported what is termed smart contracts. Smart contracts are small computer programs that execute automatically when certain conditions are met. Since smart contracts are in essence tamper-proof, it reduces the cost of verification, execution and fraud prevention. The most prominent system in this version of blockchain is Ethereum. It is a platform for implementing smart contracts. It was proposed in 2013 and the initial release of its first blockchain was in July 2015. This version enables the creation and transfer of digital assets.

After the initial successes of Blockchain 1.0 and 2.0, several limitations were revealed. The most important ones are:

- **Energy consumption:** Since mining requires significant energy (electricity) costing billions of dollars per year, it is not scalable to mass adoption.
- **Volume of transactions:** The number of transactions is increasing every 10-12 seconds with each new block creation. Bitcoin can theoretically process 7 transactions per second while Ethereum processes 15 transactions per second. If we compare the number of transactions to Visas network, which processes 24000 transactions per second, we still need to improve volume of transactions.
- **Cost:** Since a small fee is required to pay miners for maintaining the ledger, this scheme is only suitable for a limited number of large transactions but not for micro-transactions as it would become prohibitively expensive.

In order to tackle the limitations in blockchain 1.0 and 2.0, a third generation of blockchain platforms are currently under development such as Dfinity [10], NEO [8], IOTA [7] and Ethereum [15], using different approaches. They aim to support multiple programming languages and the development of various mobile based applications.

As the usage of blockchain is continuing to increase, a fourth generation of blockchain platforms is being proposed by Seele whose aim is to innovate the new era of Value Internet. Blockchain 4.0 (aka Seele [3]) proposed new consensus algorithms based on Neural Networks that improves the fault tolerance of the system. The proposal also includes a new network architecture, low latency internet connection protocol to enable integration with Internet resources and the development of blockchain-based services.

6 Blockchain-based Internet and Its Challenges

In the previous section, it was observed in the different trends of blockchain development new systems are trying to address the problem of scalability and performance without sacrificing the security of the information maintained by the

Table 3. Comparison of Different Generations of Blockchain.

Evolution	Blockchain 1.0	Blockchain 2.0	Blockchain 3.0	Blockchain 4.0
Year	2008	2013	2015	2018
Apps	Digital currency	Smart contract	Decentralized applications (DApp)	Usable in wider industrial applications
CS	Meta chain	Meta chain	a)Meta chain and side chain, b)Directed graph data structure	a)Relational chains b)Divisible chains
SL	very limited	FFPL	FFPL	FFPL
Consensus	PoW	PoW, PoS	PoW,PoS,DPoS, PBFT,Ripple, PoET	Consensus algorithm based on AI
ID	Mining	Initial Coin Offering (ICO)	ICO,ZCASH, EOS	Seele and others
Features	guaranteed transaction authenticity; reduced server costs; transactions transparency	Guarantee of distributed computation; creating and transferring digital assets	Completely open-source; autonomous operation; arbitrary protocol language support	Faster consensus and transaction confirmation; complete ecosystem of bottom-up technologies and applications

CS=Chain Structure
SL=Scripting Language
ID=Initial Distribution FFPL=Fully Featured Programming Language

network. Keeping these trends in mind, we envision that blockchain technology will significantly advance and become the basis for building totally autonomous security systems that solve the privacy and trust issues faced in today's web era. However, for this realisation to occur there are several challenges that need to be addressed before the current blockchain technologies can simultaneously ensure scalability, privacy and reliability at scales with billions of transactions every second. Here, we note the key challenges:

- **Scalability:** The current blockchain requires all transactions to be stored and be available for validating any new transaction. Due to this, cryptocurrencies such as Bitcoin can only process a few transactions every second. Newer systems fail to scale after some threshold of record and network sizes. There are several sub-problems that must be solved to address the issues, for example the optimisation of storage for transactions requiring intelligent means to maintain only a minimal amount of data to validate transactions. This also involves the challenge of when data can be archived and deleted. In addition, how data should be distributed between different nodes to ensure the best efficiency and scalability is another challenge in this context. When considering the scalability of blockchain networks, the consensus protocol also plays an important role. Therefore, load-balancing in terms of how many and which nodes should be used to validate every transaction among participating nodes is another important question to answer.
- **Interoperability of Multiple Blockchains:** Given the highly distributed and heterogeneous nature of the Internet, we can envisage there will be several private and public blockchains co-existing in the ecosystem. To maintain a global state of the information, these different blockchains should be able to communicate in a secure and transparent manner without affecting security. For example, to know the exact identity of a user, several blockchains may be queried before a blockchain validates the transaction of that user.
- **Blockchain and AI:** Current blockchain protocols are effective in securing and validating the information stored within the network, however most of these are simple and they require long verification times even though the number of nodes in the network is relatively small – the efficency of current consensus protocols need to improve. However, at greater scales, we can expect millions of nodes and this increases the risk of malign nodes trying to break the system. Several AI algorithms can help solve this and many other problems by making different parts of the blockchain 'smarter'. For example, the behaviour of nodes can be learned through their different actions and communication interactions, enabling smart decision-making on whether a particular node is trust-worthy or not. Thus, if some nodes are not trustworthy, they can be automatically pruned from decision making and this reduces the cost of adding new block.
- **Energy:** The maintenance of a secure system also comes at a cost. In particular, it can be very energy intensive. The current Bitcoin ecosystem has been estimated to consume the electrical equivalent of some small cities. When we consider Internet-scale networks with heterogeneity of connection types

and devices such as mobile phones, energy usage becomes a key factor. This requires intelligent management of data and computation depending on the device's capacity in terms of computation and battery power.

– **Simulation and Testing:** Recently several types of blockchain-based systems have appeared. Each claim to offer advantages over the others. There is currently no standardised simulation environment or benchmarks that are available than can allow comparison between different proposed concensus and data structures in addition to testing security concerns. Simulation environments are not only essential for testing the currently proposed systems but also for future development. Moreover, simulation environments are cost-effective and allow repeatability of results.

7 Conclusion

In this paper, we survey blockchain technologies and applications from different perspectives. We first include an overview of blockchain concepts, and then categorize and compare data structures used in blockchains. We also compare the consensus protocols, and summarize blockchain implementations. Furthermore, we outline some challenges that need to overcome to improve the privacy and security of current internet services. It is becoming clear from developments over the last few years, that blockchain applications have increased and with them come necessary modifications to blockchain's features to make it more scalable and fault tolerant. However, when using blockchain in massive-scale systems, scalability limitations become prevalent leading to poor performance when millions of nodes participate. Evolving design considerations will enable blockchain to be able to communicate and interoperate on networks of enormous size, maintaining a global and reliable respository of information. AI can address some of the problems that need to be solved, however its applicability needs to be tested in different scenarios. We will consider in depth the modification and ramifications of a combined blockchain and AI approach in future research.

References

1. Allcott, H., Gentzkow, M.: Social media and fake news in the 2016 election. Journal of Economic Perspectives **31**(2), 211–36 (2017)
2. Anh, D.T.T., Zhang, M., Ooi, B.C., Chen, G.: Untangling blockchain: A data processing view of blockchain systems. IEEE Transactions on Knowledge and Data Engineering (2018)
3. Bi, W.: Seele project. https://seele.pro/ (2018)
4. Buyya, R., Garg, S.K., Calheiros, R.N.: Sla-oriented resource provisioning for cloud computing: Challenges, architecture, and solutions. In: Cloud and Service Computing (CSC), 2011 International Conference on. pp. 1–10. IEEE (2011)
5. Castro, M., Liskov, B., et al.: Practical byzantine fault tolerance. In: OSDI. vol. 99, pp. 173–186 (1999)
6. Culnan, M.J., McHugh, P.J., Zubillaga, J.I.: How large us companies can use twitter and other social media to gain business value. MIS Quarterly Executive **9**(4) (2010)

7. Divya, M., Biradar, N.B.: Iota-next generation block chain. International Journal Of Engineering And Computer Science **7**(04), 23823–23826 (2018)
8. Eisses, J., Verspeek, L., Dawe, C., Dijkstra, S.: Effect network: Decentralized network for artificial intelligence (2018)
9. Gramoli, V.: From blockchain consensus back to byzantine consensus. Future Generation Computer Systems (2017)
10. Hanke, T., Movahedi, M., Williams, D.: Dfinity technology overview series consensus system (2018)
11. Kiayias, A., Russell, A., David, B., Oliynykov, R.: Ouroboros: A provably secure proof-of-stake blockchain protocol. In: Annual International Cryptology Conference. pp. 357–388. Springer (2017)
12. Kwon, J.: Tendermint: Consensus without mining. Retrieved May **18**, 2017 (2014)
13. McAfee, A., Brynjolfsson, E., Davenport, T.H., Patil, D., Barton, D.: Big data: the management revolution. Harvard business review **90**(10), 60–68 (2012)
14. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)
15. Project, E.: Ethereum project. https://www.ethereum.org/ (2018)
16. Ridyard, P.: Tempo white paper. https://projects.radix.global/wiki/radix/wikis/Tempo-White-Paper (2018)
17. Schwartz, D.: The ripple protocol consensus algorithm. https://ripple.com/files/rippleconsensuswhitepaper.pdf (2018)
18. Walport, M.: Distributed ledger technology: Beyond blockchain. UK Government Office for Science (2016)
19. Zyskind, G., Nathan, O., et al.: Decentralizing privacy: Using blockchain to protect personal data. In: Security and Privacy Workshops (SPW), 2015 IEEE. pp. 180–184. IEEE (2015)