

A Peek into the Blockchain Technology Developments

Editorial

Dr. Justin Y. Shi | justinshi@ieee.org (EIC)

Editors: Dr. Boleslaw Szymanski, boleslaw.szymanski@gmail.com

Dr. Lakshmi Shankar Ramachandran, rlshankar@emory.edu

Mr. Imran Bashir, drequinox@gmail.com

IEEE Blockchain Technical Briefs (BCTB) 2023

August 2023

1. Introduction

Known as Distributed Ledger Technology or DLT, blockchain can store transaction ledgers on networked, geographically dispersed computers securely and reliably in perpetuity. It is best known for its role in cryptocurrency systems, but it is also desirable in a wide range of other applications, such as health records, supply-chain management, elections, and many others.

Distributed databases are a type of centralized DLT that have failed to scale. Eliminating database service downtimes and arbitrary transaction losses has been proven to be very difficult if not impossible to accomplish [1].

Blockchain is a new type of decentralized DLT that is also difficult to scale. Blockchain technology enables decentralized ledger processing without central authority using step-locked cryptographic proofs [2]. Since transactions are approved by anonymous computers, authenticating them correctly and processing them securely are the two top priorities while performance is of secondary concern. Indeed, finding a balance between these priorities – decentralization, security, and stability – is inherently difficult and is often referred to as the “Blockchain trilemma”.

The successes of the blockchain technology in cryptocurrencies inspired many other applications, including NFT (non-fungible tokens) and DeFi (decentralized finance) applications. However, broad applications of blockchain technology still require a scalable solution that is tamper resistant and energy efficient. Not all DLT applications can be decentralized with anonymous users. Many DLT applications still require centralized authentication, such as KYC (know your customer) for fraud prevention and for regulatory compliance in financial services [3]. The practical DLT requirements are very basic: delivering incrementally better transactional processing security, reliability, and performance by simply adding hardware components: networks, processors and storage without exponentially growing software complexity and maintenance expenses [4].

2. Four Blockchain Challenges

The very first blockchain challenge is scalability, a term that needs careful definitions. For blockchain DLT applications, the protocols need to offer (a) immutability of all transaction records [2], (b) infinite storage scaling, and (c) energy efficiency for the consensus algorithms to secure the transaction processing network .

Blockchain partition or “sharding” was proposed to address the blockchain scalability challenges [5]. Since each partitioned chain requires a specific management protocol to communicate with other partitions, the overall protocol complexity grows in $O(N^2)$ order as the number of partitions N grows. It seems not plausible to achieve truly infinite storage scaling with finite hardware.. Experimental

implementations also have not demonstrated such potential.

A “chain of chains” idea was also proposed to tackle the blockchain scaling challenges [6, 7]. Since each chain offers limited scaling, the sum of all chains is also still scaling limited. It can only postpone the network saturation point.

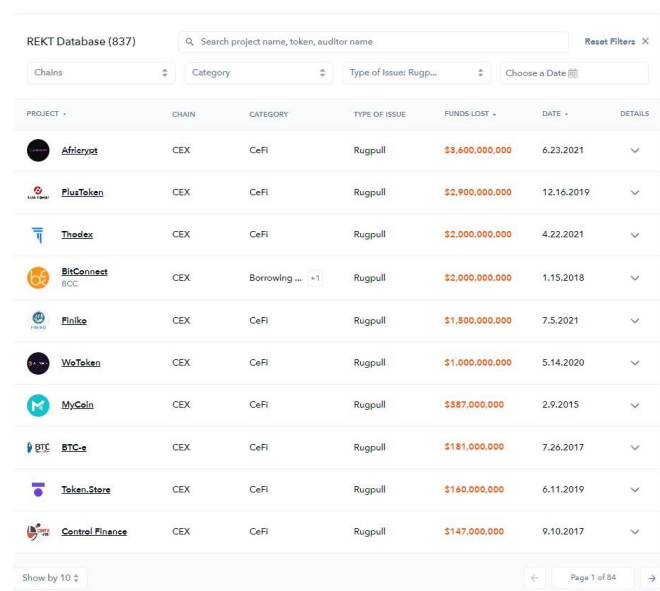
At IEEE BCTB, we will focus on the latest developments in innovative blockchain applications and technical breakthroughs. We are interested in soliciting innovative proposals for solving the blockchain scaling challenges.

The second blockchain challenge is preventing users from tampering with resistance of Open-Source programs. Unlike the closed-source database programs, most blockchain protocols are Open-Source. This means that anyone can download the source code, modify, compile, and run it against a running chain or system. It is well-known that for simple transactions, the blockchain consensus algorithm and cryptographic locks can prevent tampered code attacks by failing the ill-formed transactions unless there are more than 51% compromised nodes [8].

For smart contract implementations, however, contract malleability becomes possible in poorly designed smart contracts or processors, where transaction atomicity and isolation are not enforced. The REKT database records the latest smart contract exploits.

For 2023 IEEE BCTB, we will be interested in new cryptographic tamper-resistant transaction processing techniques for smart contract applications.

The third blockchain challenge is fraud prevention. This is the most important concern for financial DLT applications where the most vibrant innovations have occurred in the recent past. Currently, there are more than 22,000 cryptocurrencies in the world. Due to the lack of regulation and anonymous users and hosts, fraudulent activities, such as “rugpull”, are commonplace, putting investors at high risk.



PROJECT	CHAIN	CATEGORY	TYPE OF ISSUE	FUNDS LOST	DATE	DETAILS
Alfricrypt	CEX	CeFi	Rugpull	\$3,400,000,000	6.23.2021	▼
PlusToken	CEX	CeFi	Rugpull	\$2,900,000,000	12.16.2019	▼
Theindex	CEX	CeFi	Rugpull	\$2,000,000,000	4.22.2021	▼
BitConnect	CEX	Borrowing ... +1	Rugpull	\$2,000,000,000	1.15.2018	▼
Finlike	CEX	CeFi	Rugpull	\$1,800,000,000	7.5.2021	▼
WeToken	CEX	CeFi	Rugpull	\$1,000,000,000	5.14.2020	▼
MyGain	CEX	CeFi	Rugpull	\$387,000,000	2.9.2015	▼
BTC-e	CEX	CeFi	Rugpull	\$181,000,000	7.26.2017	▼
Token.Store	CEX	CeFi	Rugpull	\$160,000,000	6.11.2019	▼
Central Finance	CEX	CeFi	Rugpull	\$147,000,000	9.10.2017	▼

Figure 1. Blockchain “Rugpull” exploits

Regardless of these risks, total transaction volume across all cryptocurrencies (as tracked by Chainalysis), grew to \$15.8 trillion in 2021, up 567% from 2020’s totals [11]. Many of these

transactions are illicit. Due to the potentially high impact on overall economic conditions, regulators are slow in imposing regulatory constraints. Since all non-financial applications also require fraud prevention, this need elevates the importance of the centralized KYC (know your customer) approach to the front and center of decentralized blockchain research [3].

At IEEE BCTB, we will be interested in accepting proposals targeting fraud prevention and elimination on blockchain networks.

The fourth blockchain challenge is Interoperability between DLT systems. Since the global economy requires the participation of all technologies and stakeholders, interoperability between DLT systems is a necessary requirement. The situation becomes worse when each DLT system has its own currency symbol and value. This complicates the development of transaction gateways and exchanges. These challenges have in turn fostered projects like Cosmos[6] and Polkadots [7], which allow multiple chains to interact at a chain of chains using protocols such as Tendermint [13] and Parachains [14]. As discussed earlier, since all chains have storage scaling limits, the sum of all chains still cannot promise infinite storage as required by the blockchain protocols. It is worth emphasizing that financial innovations also happen quickly in this space. The most noticeable is AMM (automated market maker) which has not only witnessed significant growth in volume over the past few years but has also attracted several innovative ideas [12].

At IEEE BCTB, we are interested in publishing open discussions on these subjects.

3. Summary

Peer-to-peer or decentralized computing has captured the public's attention ever since the BitTorrent and Bitcoin projects emerged. As these technologies differ fundamentally from the centralized web services and legacy transaction processing methods, web3.0 was proposed to name these efforts [15]. At the time of this editorial, it is still not clear if all web3.0 applications should be decentralized. Although the blockchain immutability, transaction transparency and end-to-end encryption provide great measures for data privacy and security, the centralized authentication for fraud prevention still seems unavoidable in many applications before the technologies could be widely adopted. To date, progress has been slow. We proposed to focus on the four foundational blockchain challenges for the 2023 IEEE BCTB issues. This IEEE Blockchain Technology Brief quarter will be dedicated to publishing the latest blockchain scalability solution developments in industry, academic and government agencies.

References

1. J. Gray, P. Helland, P. O'Neil, D. Shasha, "The Dangers of Replication and A Solution," ACM SIGMOD Record, v25,2, June 1996.
2. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," <https://bitcoin.org/bitcoin.pdf> , 2008.
3. Dow Jones, "Risk and Compliance Glossary," <https://www.dowjones.com/professional/risk/glossary/know-your-customer/> , Retrieved 2023.
4. Investopedia, "Distributed Ledger Technology(DLT): Definition and How It Works," <https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp> , Retrieved 2023.
5. Consensus, "The Ethereum 2.0 Beacon Chain is Here. Now What?," <https://consensus.net/blog/blockchain-explained/the-ethereum-2-0-beacon-chain-is-here-now-what/> , Retrieved 2023.
6. Cosmos.network, "Build on the Interchain," <https://cosmos.network/> , Retrieved 2023.
7. Polkadot.network, "The multichain vision for Web3," <https://polkadot.network/> , Retrieved

- 2023.
8. Investopedia, "51% Attack: Definition, Who is at Risk, Example and Cost," <https://www.investopedia.com/terms/1/51-attack.asp#:~:text=A%2051%25%20attack%20is%20an%20attack%20on%20a%20blockchain%20by,other%20miners%20from%20completing%20blocks>, Retrieved 2023.
 9. SolidityLanguage.org, "Expressions and Control Structures," <https://docs.soliditylang.org/en/v0.8.19/control-structures.html> , Retrieved 2023.
 10. REKT database, "Cumulative Lost & Recovered Funds," <https://de.fi/rekt-database> , Retrieved 2023.
 11. Chainanalysis.com, "Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in value, All-Time Low in Share of All Cryptocurrency Activity," <https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/#:~:text=Across%20all%20cryptocurrencies%20tracked%20by,more%20cybercriminals%20are%20using%20cryptocurrency>, Retrieved 2023.
 12. Mcdex.medium.com, "Proposing New AMM Pricing Formula," <https://mcdex.medium.com/proposing-new-amm-pricing-formula-bdd40d31ebd9> , Retrieved 2023.
 13. Tendermint.com, "Powerful & Secure Software for the Decentralized Future," <https://tendermint.com/> , Retrieved 2023.
 14. Polkadot.network, "Parachains' Protocol Overview," <https://wiki.polkadot.network/docs/learn-parachains-protocol> , Retrieved 2023.
 15. Investopedia, "Web3.0 Explained, Plus the History of Web1.0 and Web2.0," <https://www.investopedia.com/web-20-web-30-5208698>, Retrieved 2023.