IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

BLOCKCHAIN 4.0 TECHNOLOGY

Pavan Joshi, Aachal Dadhe, Suyog Hole, Bhavika Shinde, Prof. Sudesh Bachwani
Department of computer engineering, Government college of engineering, Yavatmal, India

Abstract— Blockchain is a cutting-edge technology that has had a huge impact on modern civilization because to its transparency, decentralisation, and security aspects. The initial Blockchain application, which received a lot of interest, was to record financial transactions of bitcoin. Blockchain technology has the potential to significantly alter how we interact, conduct business, and live in the near future. Previously, transtion took a long time, making the process of resolving these issues slow. Blockchain introduced the lightning network, DOPS, and DDPOS to improve the transaction processing time of blockchain. With Blockchain 2.0 began the era of smart contracts, which enabled Blockchain to go beyond its basic functionality of powering cryptocurrencies. Smart contracts enabled firms to automate their cross-organizational contracts. The rise of dApps has been essential to Blockchain 3.0. dApps allow several powerful blockchain use-cases like as DeFi platforms, Crypto loan platforms, NFT marketplaces, P2P lending, and others through a frontend user interface that calls to its backend smart contracts maintained on decentralised storages. Blockchain 4.0 promises to expand Blockchain into a business-useable platform for developing and running more advanced and mainstream decentralised apps. The primary focus areas for Blockchain 4.0, which includes Web 3.0, Metaverse, and others, will be speed, user experience, and use by a broader and more diverse population. This study finishes with a consideration of key future opportunities, new use cases, and outstanding research questions that scientists may pursue in order to advance Blockchain 4.0 as a discipline.

Keywords—Blockchain, Bitcoin, Lightning Network, LNURL, WebLN.

I. INTRODUCTION

Blockchain technology enables the existence of cryptocurrencies. Bitcoin, for which blockchain technology was first developed, is the cryptocurrency with the most widespread acceptance. A cryptocurrency is a digital currency similar to the US dollar that employs cryptography to regulate the creation of new units of currency and to confirm the flow of funds.

Blockchain is used because it is one of the most secure data protection methods. The rapid development of digital technology has also brought new challenges in data security.

Organizations must develop strong authentication and key vaulting procedures to secure their data. Blockchain, as one of the most significant technological innovations of this century, enables businesses to remain competitive without relying on the trust of third parties. Blockchain is the most effective approach for safeguarding the data of the shared community. Anyone using the blockchain's capabilities cannot access or tamper with any preserved sensitive data.

Despite being a widely used technology, blockchain still has a number of issues. The main challenge with its implementation is scalability. Blockchain is unsuitable for large-scale applications because, while transaction networks can handle hundreds of transactions per second without issue, processing transactions for Bitcoin (approximately 3-7 transactions per second) and Ethereum (about 15-20 transactions per second) takes a long time. Despite the fact that blockchain-based apps, networks, and businesses are more secure than traditional computer systems, hackers may still gain access to them. The solution is not simply having the government defend our privacy. We will be able to collect and govern our data thanks to blockchain self-sovereign IDs.

In this review paper, we will discuss a number of technologies that will make blockchain applications more interesting, dependable, and safe.

Scaling techniques for Bitcoin and Ethereum, such as Lightning Network and Plasma, enable fast, low-cost transactions. If blockchain is to be widely used, it must accelerate. Although the Lightning network is critical to bitcoin's future, the user experience leaves much to be desired.

The Lnurl standard is quietly gaining traction as a solution to this problem. It has been quietly integrated into dozens of additional programmes, as well as some of the most well-known Lightning wallets, with little notice. Zap, Phoenix, Breez, Blue Wallet, and Satoshi Wallet are a few examples.

Lightning payments are commonly paid or received after a brief setup and a series of eight stages. Lnurl aims to simplify a variety of common chores so that they only require a click or a QR scan.

WebLN, a library and set of specifications, can be used by Lightning apps and client providers to offer secure

communication between apps and users' or custodial Lightning nodes. Among other things, it provides a programmatic, permissioned interface that allows programmes to sign into websites using LN-Auth and generate Lightning invoices for payment.

II. BEGINNINGS OF BLOCKCHAIN

A. BLOCKCHAIN INVENTION

The notion of blockchain technology was first presented in 1991 by Stuart Haber and W. Scott Stornetta, two mathematicians interested in establishing a system where document timestamps could not be changed. Blockchain technology was first developed in 1991 to store and safeguard digital data.

B. AHEAD OF BLOCKCHAIN

Many of the technology on which blockchain is based were already in development before bitcoin existed. One of these methods is the Merkle tree, named after computer scientist Ralph Merkle. Merkle created a system for public key distribution and digital signatures known as "tree authentication" in his 1979 Ph.D. thesis for Stanford University. The Merkle tree provides a data structure for inspecting individual records.

David Chaum developed a vault system for developing, maintaining, and trusting computer systems by mutually suspicious groups in his Ph.D. dissertation for the University of California, Berkeley in 1982. This system displayed several hallmarks of a blockchain. Haber and Stornetta integrated Merkle trees into the design in 1992, allowing different document certifications to coexist on a same block.

C. EVOLUTION OF BLOCKCHAIN

Over the course of its existence, blockchain technology has advanced from one spectacular milestone to the next. Blockchain technology has progressed from blockchain 1.0 to blockchain 4.0, which includes a slew of new and better features.

Blockchain is currently separated into three versions based on applications: Blockchain 1.0, 2.0, and 3.0 and blockchain 4.0 is on its way to evolve.

III. BLOCKCHAIN AT ITS PINNACLE

Blockchain 1.0, 2.0, and 3.0 are stages in the evolution of blockchain technology. Each new level seeks to improve on the inadequacies of the preceding one.

Blockchain 1.0 started with the first iteration of Bitcoin, the world's first and most popular cryptocurrency. Blockchain 2.0 concentrated on Ethereum, whereas Blockchain 3.0 introduced Cardano to the market.

Blockchain 2.0 built on the premise of blockchain 1.0 to create a better and more advanced version.

The combination of these versions has enabled the industry to make better use of cryptocurrencies, smart contracts, and dApps.

A. BLOCKCHAIN 1.0

Throughout the blockchain 1.0 era, which was solely focused on the development of cryptocurrencies, decentralisation as a whole experienced iteration. The launch of the first cryptocurrency, Bitcoin, signalled the start of blockchain development (BTC).

This arose as a result of the Cypherpunks team of professionals' concerns about the stability of the banking system and the internet. The organisation believed that surveillance and censorship would be a part of the future of the internet. They attempted to develop an electronic cash system that would guarantee privacy in order to economically safeguard the open internet.

The system was built on the ECash (electronic cash) designs that were introduced in the 1980s and 1990s. During this time, blockchains were focused on highly secure, anonymous, peer-to-peer transactions of a completely decentralised digital currency.

Blockchain 1.0 technology includes components such as a Blockchain Core for the applicable cryptocurrency, wallet software, mining rigs, and mining software. Every cryptocurrency has a Blockchain Core, which allows any computer to start a node.

According to some sources, blockchain 1.0 refers to the technology's first iteration, which focused primarily on decentralisation and cryptocurrency.

B. BLOCKCHAIN 2.O

Blockchain 2.0, the next iteration of blockchain technology following Blockchain 1.0, is ostensibly a better version of Blockchain 1.0, which is represented by Ethereum (ETH).

The development of Ethereum and the implementation of smart contracts are the primary goals of Blockchain 2.0.

Ethereum was established as a platform for developing decentralised applications. As a result, Blockchain 2.0 is based on it, as it has provided programmers with more alternatives for deploying smart contracts to the Ethereum blockchain in a permissionless and open-source manner.

As a result of this technology, initial coin offers (ICOs), decentralised autonomous organisations (DAOs), decentralised financing (DeFi), and non-fungible tokens have all emerged (NFTs).

C. BLOCKCHAIN 3.0

This level of blockchain development attempts to improve scalability while also enabling blockchain interoperability. Blockchain 3.0 has introduced Cardano (ADA). Though there are no specific definitions or agreed-upon concepts about what the blockchain promises the internet, a Proof-of-Stake (PoS) method is assumed.

However, its promise is centred on finding solutions for organisations and areas other than economics. Blockchain 3.0 is regarded as an institutional and commercial blockchain. It intends to increase the blockchain's security while simultaneously lowering the hefty gas fees associated with the previous version.

D. NEW GENERATION TECHNOLOGY: BLOCKCHAIN 4.0

Blockchain 3.0 appears to be the precursor to Blockchain 4.0, the next generation of blockchain technology. It intends to fully mainstream blockchain technology by making it usable in commercial settings for developing and running apps.

Previous generations of blockchain technology have already proved potential benefits for enterprises, such as security, automatic record-keeping, immutability, and the ability to pay bills, wages, and invoices in an entirely secure environment.

However, there is still room for development in terms of speed and the limited ease with which blockchain innovations may now be made. Blockchain 4.0 promises to improve user experience in the sector.

IV. BITCOIN: FIRST SUCCESSFUL USE CASE OF BLOCKCHAIN

In 2008, a person using the moniker Satoshi Nakamoto proposed the principles behind bitcoin, describing how encryption and an open distributed ledger could be utilised to construct a digital currency application (Nakamoto 2008). Initially, bitcoin's development was hampered by its extremely high volatility and many nations' opposition to its complexity, but the merits of blockchain—the technology that supports bitcoin—attracted increasing attention. Blockchain's distributed ledger, decentralisation, information transparency, tamper-proof design, and openness are some of its advantages.

The ideas underlying bitcoin and the blockchain were introduced in a white paper written by Satoshi Nakamoto in 2008. According to the white paper, blockchain infrastructure will enable secure peer-to-peer transactions without the need for dependable third parties like banks or governments.

Jan. 3, 2009. By mining the initial Bitcoin block, Nakamoto established the legitimacy of the blockchain. The Genesis block, also known as block 0, was made up of 50 bitcoins.

A. BLOCKCHAIN: WHY SATHOSHI USED IT?

1) A transaction cannot be modified after it has been recorded since it is an immutable public digital ledger.

2) Because of its encryption characteristic, blockchain is always secure.

3) Transactions are done fast and transparently since the ledger is automatically updated.

4) Because the system is decentralised, no intermediate costs are required.

5) A transaction's participants authenticate and certify its legitimacy.

B. BITCOIN: SCALABILITY ISSUE

To reach its goal of becoming a worldwide currency, Bitcoin employs the proof-of-work consensus process (POW).

Proof of work is the consensus algorithm employed by the most well-known cryptocurrency networks, such as bitcoin and litecoin (PoW). Any participating node that wishes to add new transactions to the blockchain must demonstrate that the work they have completed and submitted fits the necessary criteria.

The obsolete POW consensus method and bitcoin's top transaction processing speed of 7 transactions per second As more businesses strive to integrate blockchain to improve their existing systems, blockchain that uses old consensus techniques and has scalability difficulties will not give the best benefits.

C. LIGHTNING NETWORK FOR FASTER PROCESSING TIME

To address these issues, modern approaches such as the lightning protocol, sharding, super quadratic sharding, and DPoS were introduced. The lightning protocol, which distributes transactions on-chain once the lightning channel between the two users is closed and takes Bitcoin transactions off-chain in peer-to-peer channels to enable quick micropayments, is one of the most popular second layer alternatives.

The Lightning network has enabled bitcoin transactions to be scaled from 7 transactions per second to millions of transactions per second without any downtime. When compared to VISA payments, which can handle up to 65000 transactions per second, these figures are much higher but still fall short of improved UX interactivity.

V. IMPROVING BITCOIN USER EXPERIENCES AND SECURITY OVER THE INTERNET BY USING BLOCKCHAIN 4.0 BASED TECHNOLOGIES

Blockchain 4.0 is the next generation of blockchain technology, following Blockchain 3.0. Its goal is to eventually make blockchain useful in commercial environments for designing and running apps, bringing the technology fully mainstream.

One shortcoming of the lightning network is its poor user experience (UX) when accessed via a web browser or the internet, which creates discomfort and encourages consumers to stick with the currency. This disadvantage can be overcome by utilising various technologies and interfaces that focus on giving UX to the user, resulting in widespread adoption of cryptocurrencies over the internet as well as the provision of various new methods of online security.

A. PERMISSIONED INTERFACES

Users can interact with cryptocurrency blockchains such as bitcoin directly from their browsers by employing permissioned interfaces to communicate with their lightning nodes from web apps, i.e., browsers.

Permissioned interfaces improve security when using blockchain over the internet in a decentralised manner without the involvement of a third party.

B. WebLN AS A PERMISSIONED INTERFACE

WebLN is a set of specifications for Lightning apps and client providers that enables safe communication between web apps and users' Lightning nodes while also providing a better UX for accessing bitcoin over the internet.

WebLN provides a programmatic, permissioned interface through which apps can request payments from users, generate invoices to receive payments, and much more.

WebLN is based on web3.js, a library collection that allows you to interface with a local or remote Ethereum node via HTTP, IPC, or WebSocket.

The WebLN specs were published in 2018 and have been regularly developed since then. In the interim, this standard has been used to build various Lightning applications and client providers.

The following is what WebLN brings to the table:

1. **Better UX**: WebLN allows for programmatic interactions and reduces friction between a Lapp and the user's wallet. Users don't have to switch contexts for scanning a QR code to make a payment anymore. Additionally, they can sign a message with one click to prove ownership of a wallet. If a WebLN client supports autopayments, no prompt is needed and the user is just one click away from sending a payment.

2. **Ready and secure:** WebLN is a specification that only describes how to interact with a Bitcoin Lightning wallet. There is no need to trust and integrate a third-party library. Over the years WebLN has developed and has been recognized as a standard within the community.
3. **Simple:** implementation Initialization and execution of WebLN requires not more than some lines of code of JavaScript — a language that is commonly used for creating web apps.
4. **Complementary to LNURL**: WebLN works well together with LNURL, another, more manual standard to make interactions with Lighting easier. If implemented correctly WebLN provides a great enhancement of the UX. For users without a WebLN provider installed, LNURL can serve as a fallback option.

C. WEBBTC AS A PERMISSIONED INTERFACE

WebBTC is a common convention in the Bitcoin web application ecosystem for key management software ("wallets") to expose their API via a JavaScript object on the web page. This object is called the common web wallet interface.

Historically, Provider implementations have exhibited conflicting interfaces and behaviors between wallets. This working group formalizes a Bitcoin extension API to promote wallet interoperability. The API is designed to be minimal, event-driven, and agnostic of transport and RPC protocols. Its functionality is easily extended by defining new RPC methods and message event types.

Historically, providers have been made available as window.bitcoin or window.we bln in web browsers, but this convention is not part of the specification.

D. WebLN and WebBTC

WebLN is an implementation of the WebBTC specification that focuses only on off-chain Lightning Network functionality, allowing web apps and client providers to communicate with user wallets.

WebBTC was created to empower everyone to send and receive money on the web. Coupled with the Lightning Network's ability to send bitcoin instantly and with (almost) no fees, we're ushering in a new standard for how value moves across the web.

Integrating WebBTC into the web application is straightforward. Set up support for this new standard and join the era of total Bitcoin Lightning interoperability!

E. MAGIC OF WebLN COMMUNICATING WITH BITCOIN BLOCKCHAIN VIA LIGHTNING NETWORK

WebLN is a standard, and any developer can programme the following function without the assistance of a third party.

WebLN API Methods-

First, enable the provider by calling as it is a permissioned interface.

webln.enable()

Then, use the APIs

webln.getInfo() - Get information about the connected node: node alias, public key and color

webln.keysend() - Request the user to send a keysend payment. This is a spontaneous payment that does not require an invoice and only needs a destination public key and and amount

webln.makeInvoice() - Request that the user creates an invoice to be used by the web app.

webln.sendPayment() - Request that the user sends a payment for an invoice

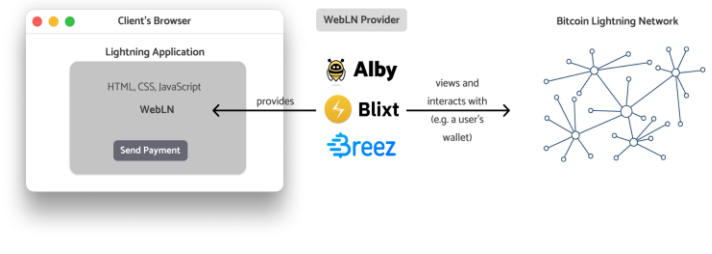
webln.signMessage() - Request that the user signs an arbitrary string message.

webln.verifyMessage() - Opens an external view where the user's client verifies the signature against the raw message, and lets the user know if it was valid.

Fig. 1. WebLN provider functionality.

F. WebLN USE CASES

1. Use your browser to make bitcoin payments over the internet.



2. Have your decentralised identity accessible via the internet.
3. WebLN allows for blockchain authentication over the internet.

VI. BLOCKCHAIN 4.0 USE CASES

A. WEB3.0

We are approaching the third generation of internet services, which will be powered by technological developments such as IoT, Blockchain, and AI. The Internet is always changing. Blockchain is critical to the development of Web 3.0 since it emphasises decentralisation.

Web 2.0 has revolutionised social interaction by opening up new avenues for interaction. However, in order to take advantage of these opportunities, we as consumers have moved all of our data into centralised systems, compromising our privacy and exposing ourselves to all of the usual internet threats. Web 2.0 platforms are managed by centralised entities that manage user data and establish transactional rules.

B. METAVERSE

Metaverses, pet projects of tech behemoths like Facebook, Nvidia, and others, will be the next big thing for us to experience in the coming years.

We are connected to virtual worlds through a variety of touchpoints, including social contact, gaming, employment, networking, and many others. Because of the metaverse, these experiences will become more real and vivid. Metaverse's virtual reality worlds will be created with cutting-edge AI, IoT, AR, VR, cloud computing, and Blockchain technology. Through lifelike experiences, users

will engage with other users and the computer-generated world.

The more we discuss about Metaverse, the more wonderful it appears to us, especially when we consider games, enormous art displays, concerts, virtual boardrooms for businesses, and other possibilities.

C. BUSINESSES WITH BLOCKCHAIN 4.0

We are all familiar with how businesses function or seek to operate in the Industry 4.0 environment. Smart factories, smart supply chains, digitised service offerings, innovative digitally enabled business models, and consumer transparency characterise Industry 4.0 organisations in industries such as healthcare, manufacturing, finance, logistics, education, and government.

D. INDUSTRIAL REVOLUTION 4.0

We can consider Blockchain 4.0 to be a concept that drives all development activities targeted at making Blockchain viable in Industry 4.0. The world has always needed industrial revolutions to shake up prejudices and introduce new ideas. Blockchain is fueling the fourth industrial revolution's upheavals in the same way that the steam engine and the Internet did in previous industrial revolutions. Blockchain is the fourth industrial revolution's pillar, according to World Bank experts, since technology has the ability to minimise corruption by improving openness in business operations, government processes, and supplier networks.

VII. CONCLUSION

In this article, we claimed that blockchain technology is transformative, particularly in the financial and logistical sectors. Blockchain is a distributed ledger that keeps a permanent, tamper-proof record of transactional data.

Blockchain 1.0 is the initial iteration of blockchain technology, emphasising bitcoin and decentralisation.

Blockchain 2.0 is a significant upgrade to the Ethereum network, transitioning it from the proof-of-work (PoW) paradigm to the proof-of-stake (PoS) model. The goal of blockchain 2.0 is to increase the network's scalability, accessibility, and security.

The key goals of Blockchain 2.0 are the development of Ethereum and the implementation of smart contracts.

Ethereum was established as a platform for developing decentralised applications. As a result, Blockchain 2.0 is based on it, as it has provided programmers with more alternatives for deploying smart contracts to the Ethereum blockchain in a permissionless and open-source manner.

Web 3.0 enables an increasing number of innovative apps and services. Blockchain 3.0 focuses on developing solutions for services and sectors other than economics.

Essentially, blockchain 4.0 focuses on tackling UX challenges, where webln and lnurl come in handy for accessing the power of bitcoin and blockchain through an internet browser.

WebLN is a permissioned interface that allows programmes to request payments from users, generate invoices to receive payments, and much more. WebBTC was established to let anyone to send and receive money via the internet. We're ushering in a new standard for how value moves throughout the web by combining it with the Lightning Network's capacity to transport bitcoin immediately and with (nearly) no costs.

Blockchain is still in its infancy and has a lot of room to grow in the future.

REFERENCES

[1] TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains, Sidra Malik;Volkan Dedeoglu;Salil S. Kanhere;Raja Jurdak 2019 IEEE International Conference on Blockchain (Blockchain) Year: 2019 | Conference Paper | Publisher: IEEE)

[2] A Survey on Safety Regulation Technology of Blockchain Application and Blockchain Ecology, Pengxu Shen;Suozai Li;Ming Huang;Haoyu Gao;Leixiao Li;Jun Li;Hong Lei 2022 IEEE International Conference on Blockchain (Blockchain) Year: 2022 | Conference Paper | Publisher: IEEE

[3] Research and Implementation on the Operation and Transaction System Based on Blockchain Technology for Virtual Power Plant Da Li; Qinglei Guo; Desheng Bai;Wei Zhang 2022 International Conference on Blockchain Technology and Information Security (ICBC TIPS) Year: 2022 | Conference Paper | Publisher: IEEE

[4] Muhammad Nasir Mumtaz Bhutta, Amir A. Khwaja, Adnan Nadeem, Hafiz Farooq Ahmad, Muhammad Khurram Khan, Moataz A. Hanif, Houbing Song, Majed Alshamari, Yue Cao, "A Survey on Blockchain Technology: Evolution, Architecture and Security", in: IEEE Access (Volume: 9).

[5] Hyojung Lee, Kiwoon Sung, Kyusang Lee, Jaeseok Lee, Seung Jae Min, "Economic Analysis of Blockchain Technology on Digital Platform Market", in year 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), Conference Paper, Publisher: IEEE.

[6] Yang Cheng, Han Shaoqin, 2020 International Conference on Big Data & Artificial Intelligence & Software Engineering (ICBASE), "Research on blockchain technology in cryptographic exploration"Year: 2020, Conference Paper, Publisher: IEEE

[7] Zhan Su, Hejian Wang, Huanjuan Wang, Xin Shi, 2020 IEEE 3rd International Conference of Safe Production and Informatization (IICSPI), "A Financial data security sharing solution based on blockchain technology and proxy re-encryption technology", Year: 2020, Conference Paper, Publisher: IEE