IMPLEMENTATION OF BLOCKCHAIN IN FINANCIAL SECTOR TO IMPROVE SCALABILITY

L. Manikandan[1], B. Keerthi[2], M. Vijayalakshmi[3], M. Harisha[4]

Article History: **Received:** 13.02.2023 **Revised:** 28.03.2023 **Accepted:** 15.05.2023

Abstract

Cryptocurrencies open transaction ledger was first powered by blockchain technology. Blockchain technology is already being investigated for a broad range of additional uses outside of cryptocurrencies because to its distinctive mix of security, decentralization, anti-tampering properties, transparency. These are the qualities that are especially beneficial for most of the major issues which are happening in the financial sector encounters. So, blockchain technology has the capability to completely transform the financial industry by altering how various financial services are provided. We describe five major financial industry use cases that the implementation of blockchain technology is expected to significantly affect in this post.

Keywords: include blockchain applications, blockchain benefits, blockchain features and blockchain security.

[1]Assistant Professor, Department of Computer Science & Engineering, Sridevi Women's Engineering College, Hyderabad, Telangana, India
[2,3,4]B.Tech Final Year, Department of Computer Science & Engineering, Sridevi Women's Engineering College , Hyderabad, Telangana, India

Email: [1]swecmanicse90@gmail.com, [2]budurukeerthireddy@gmail.com, [3]honeyvijayalaxmi369@gmail.com, [4]harisha.maddela@gmail.com

DOI: 10.31838/ecb/2023.12.s3.337

1. INTRODUCTION

After the launch of well-known cryptocurrencies like Ethereum and Bitcoin, which are only two major uses of this technology, blockchain technology rose to prominence. The financial services sector has shown interest in Bit Coin and Ethereum, and other cryptocurrencies Alt Coins including Prime Coin, Light Coin, Z cash and Name Coin, have also been created. Additionally, they played a major role in the creation of Initial Coin Offering mechanism, a novel idea for innovative funding projects and products. From the past few years, there have been an increase in interest in blockchain based applications outside of cryptocurrencies, particularly those that attempt to make use of the decentralized nature of distributed ledger technologies as well as their anti-tampering features, transparency and security. These characteristics are utilized by many applications in the context of permission blockchain infrastructures, which provides fine grained authorization and authentication while also doing away with the requirement for challenging and time taking Proof of Work procedures. Latter is necessary to support applications that need transaction completion speeds that are quicker than those provided by older, more established public blockchains like Bitcoin and Ethereum As a response, solutions to handle permissioned blockchains have evolved, including Hyperledger Fabric and R3/Corda, both, which support hundreds of transactions per second. Numerous sectors, including energy, business, supply chain management, and healthcare, are currently looking into applications based on permissioned blockchains for non-cryptocurrencies. Financial institutions are taking a look at a few of these apps as part of the wave of FinTech advancements. Financial institutions may solve a number of persistent, significant issues by utilizing blockchain technology. One of the biggest problems with bank credit is the lack of understanding of credit scoring, which makes it difficult for individuals and SMEs to get loans from financial institutions [2].

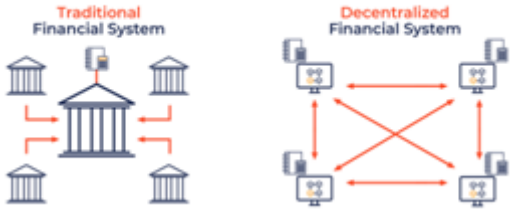

Fig.1: Example figure

Due to a lack of comprehensive and correct data, financial businesses have difficulty doing trustworthy customer profiling so they may successfully distinguish and tailor their goods [3]. Similar to this, the insurance policies sold by financial institutions cover a complex claims process that includes several parties before a claim is eventually settled and paid.

2. LITERATURE REVIEW

Outlook and Blockchain application in the banking industry

The financial industry has great potential for using blockchain technology, which is a basic, underlying technology. On the one hand, the consequences of interest rate liberalization and a decline in earnings brought on by the shrinking interest-rate difference are being felt by China's

banking sector. On the other side, it is also influenced by the financial revolution, the expansion of the Internet, and the economy. As a result, the banking industry must urgently modernize and is searching for fresh chances for growth. Blockchains may thus modernize and rethink the technology that underlies banks' credit information and payment clearing operations. Blockchain applications also support "multi-center, weakly intermediated" scenarios, which will boost the financial sector's effectiveness. Blockchains are permissionless and self-governing, but there are still issues with legislation and decentralized system implementation that need to be overcome. As a result, we advocate for the rapid creation of a "regulatory sandbox" `and creation of industry standards

.

Blockchain Beyond Cryptocurrencies: 21st-Century FinTech and Strategy

Blockchain technology is thought to have the power to completely change how financial services companies operate. The present research on the potential impacts of blockchain adoption for four important financial activities payments and remittance, credit and, trading, lending and settlement is outlined in this chapter. It also introduces the key properties of blockchain technology. In order to pinpoint potential directions for future study, the literature's current gaps are explored.

Towards a universal standard against falsifying financial data integrity

The global financial crisis of 2007 showed how crucial confidence is to the functioning of the system and how fragile it may be. A new danger to financial stability and the unprecedented scope of the risk that malevolent cyber actors represent to financial institutions were made clear by the 2016 Bangladesh central bank cyber crisis. More so than other types of financial coercion, utilizing cyber operations to influence the integrity of data in particular offers a unique and elevated set of systemic vulnerabilities. Because of the financial system's complexity, interdependence, and transcendence of geographical and national boundaries, altering the integrity of financial institutions' data may endanger both the stability of the financial system and the global economy. Importantly, unlike the global financial crisis of 2007–2008, this danger is unrelated to core economic fundamentals and will only grow as more and more governments explicitly want to create cashless economies. It is commendable that the G20 finance ministers and central bank governors called for strengthening the financial system's resilience in their communiqué from March 2017. The G20 member nations might expressly promise not to use offensive cybertools to tamper with the integrity of data in the financial system and to work together in the event that such assaults do happen.

Blockchain for RES Financial Investments Services Facilitation

The interest in blockchain technology has grown over the past few years. This technology is unique in that it provides several important properties like decentralization, transparency, and dependability by the design. Application field was mostly the financial one at first, but many others have since looked into. In this essay, We provide a real world case study from finance industry that was applied to a neighborhood's renewable energy exchange. This describes the development of a finance platform, based on q private implementation of the Ethereum blockchain, that offers a range of services for investments in renewable energy sources RES Platform implements price-based, peer-to-peer reliable energy market, serving both district energy prosumers and RES Financial investors. Participants automatically trade certain "tokens" to monitor and record transactions, ensuring auditability, and to

show the amount of energy traded and its monetary counter values. Financial services provided for investors range from simple models of shared profits and equity to more complicated models of investment performance monitoring. The microgrid's market and each of its users are nodes in the blockchain. Utilizing Ethereum smart contracts, all platform capabilities were deployed, assuring dependability and transparency.

Difficulty control for blockchain-based consensus systems:

Recently, interest in cryptocurrencies like Bitcoin has increased significantly. The creation of a Nakamoto blockchain through "mining" is an essential component of these systems. We employ a Poisson process model of mining to get predictions regarding block timings for a variety of hash-rate situations, with exponentially growing hash rate being the most crucial. We also look at how Bitcoin updates the "network difficulty" as a way to maintain consistent block timings. We suggest a novel approach to updating difficulty since the current technique routinely produces too many blocks too quickly for exponential hash-rate increase. We demonstrate both in simulations of contrived growth situations and with real-world data that our suggested strategy works significantly better at assuring consistent average block durations over extended periods of time. In addition to Bitcoin itself, this offers useful advantages, especially for platforms like Name coin. It may be used to increase the predictability of name expiration timings, reducing unintentional name loss.

Bitcoining: A scalable blockchain protocol:

Cryptocurrencies, which are based on and led by Bitcoin, have the potential to provide the basis for trustless digital asset exchange, smart contracts, low-cost transfer, anonymous online payments, and remittance. The inherent scalability constraints of blockchain protocols developed from Bitcoin which trade offs latency throughput preclude the fulfilment of this promise. The scalable Bitcoin Next Generation blockchain technology is presented in this paper. Bitcoin-NG is a Byzantine fault-tolerant blockchain system with the same trust architecture as Bitcoin and is resilient to high churn. We also offer a number of additional measures that are useful for measuring the efficiency and security of blockchain protocols similar to Bitcoin, in addition to Bitcoin-NG. Using the same clients for both protocols, we create Bitcoin-NG and conduct extensive tests 15% to the size of the live Bitcoin system. These tests show that Bitcoin-NG grows well, with latency and bandwidth both constrained by the network's propagation time and the capacity of the individual nodes.

Mix coin: Anonymity for bitcoin with accountable mixesl:

We suggest Mix coin as a mechanism to help with Bitcoin and other cryptocurrency anonymous payments. We extend the phenomena of money mixtures by including a method for holding people accountable in order to reveal theft. We show that incentives of mixes and customers may be matched to prevent theft by logical mixes. Our plan is effective and completely Bitcoin compatible. Our technique offers an anonymity set of all concurrent coin-mixing users to protect against a passive attacker. There is no obvious analogue for this intriguing new feature in more well researched communication mixtures. Our method provides comparable anonymity to conventional communication mixes when facing active attackers.

Implementation

All currently used applications are run by a single, centralized server, and if this server is compromised or crashes as a result of a heavy load of requests, the services will not be available.

Disadvantages:

- No services are available
- Request overload problems

We can utilize decentralized Blockchain technology to solve this issue since it maintains data across numerous servers or nodes, ensuring that consumers can still access services even if one node goes down.

Advantages:

1. Provide a safe and trusted transactions
2. High security

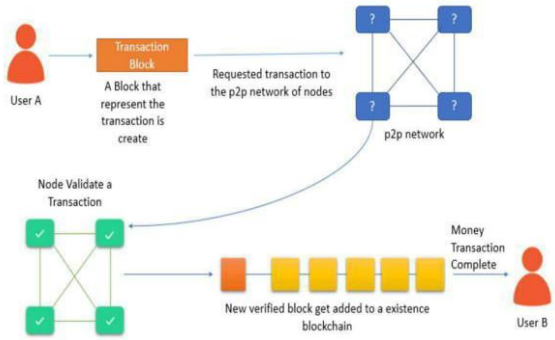

Fig.2: System architecture

ALGORITHMS

As every current application relies on a single centralized server and if this server is hacked or crashes due to a heavy load of requests, the services will not be provided, we are using Blockchain technology in financial applications in this project. We can utilize decentralized Blockchain technology to solve this issue since it maintains data across numerous servers or nodes, ensuring that consumers can still access services even if one node goes down.

Blockchain stores data as blocks or transactions and assigns each block an distinct hash code. Ahead storing any new block, Blockchain verifies the hash codes of all existing blocks to ensure that no blocks have been attacked or altered. If this verification is successful, Blockchain will only then store a new block. Blockchain is said to be immutable since it cannot be attacked or have its data changed from the backend if the verification process fails because it won't store any new data. Verification will fail if altered.

The aforementioned benefits of blockchain are driving businesses to move from centralized servers to decentralized networks.

Customers and service providers are the two types of users we are creating for this project.

1) Service Providers: The service provider may register, log in, add new items, and view customer orders after doing so.
2) Users: The user may register and log in to the application, examine all information about the service providers, add money to their wallet, and explore product descriptions to make purchases.

Blockchain uses smart contracts to store data, and SOLIDITY programming is used to define these contracts. Truffle allows SOLIDITY code to be deployed on the Ethereum blockchain. Once deployed, the contract will produce an ADDRESS, which can be used in a Python program to access the contract and save and receive data from the blockchain.

BLOCKCHAIN

Blockchain is a decentralized, rigid ledger that makes managing assets and transaction data in business networks simpler. Money, property, auto mobiles. and other tangible goods are examples of tangible assets. Almost every value might be recorded and traded on the blockchain network, which lowers risk and

boosts efficiency for all parties. Without the information the firm cannot function. It is better to recognize soon and accurately. Because it provides real-time, shareable, and completely transparent data that is stored on an fixed ledger and only accessible to members of a permissioned network, blockchain is the appropriate technology for delivering this kind of information. Among other things, a blockchain network might be used to payments, track orders, manufacturing and accounts. So the fact that everyone have access to similar version of truth, you may observe a transaction from starting to end. It increases your self-confidence and opens up new possibilities.

An individual or bunch of people going by the moniker Satoshi Nakamoto created a blockchain in 2008 to serve as the public distributed record for bitcoin cryptocurrency transactions, building on prior work by Stuart Haber, W. Scott Stornetta, and Dave Bayer.[6] Blockchain technology was initially used by Bitcoin to prevent double spending without the need of a central server or other reliable authority.

Alternative uses [3]. The bitcoin design has an impact on [2] and blockchains, which are widely used by cryptocurrencies and accessible to the general public. The blockchain is one type of payment rail that can be considered. Private blockchains have been offered for business use. Some have asserted that well-built permissioned blockchains may more decentralized and, as result, more secure in use than permissionless ones. According to Computerworld, selling such private blockchains without an effective security system is like selling "snake oil"[8].

3. EXPERIMENTAL RESULTS

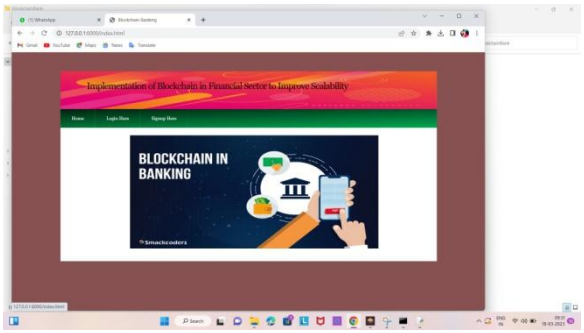

Fig.3: Home screen

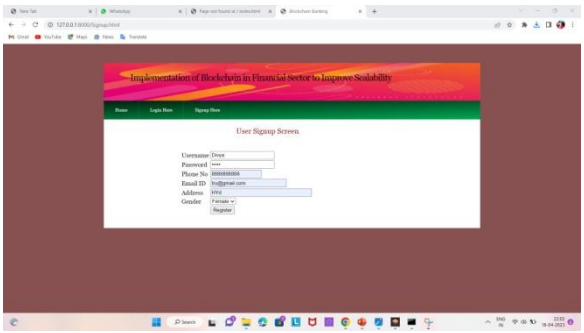

Fig.4: New user signup

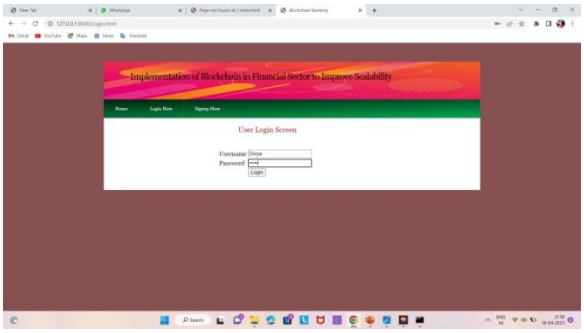

Fig.5: User login

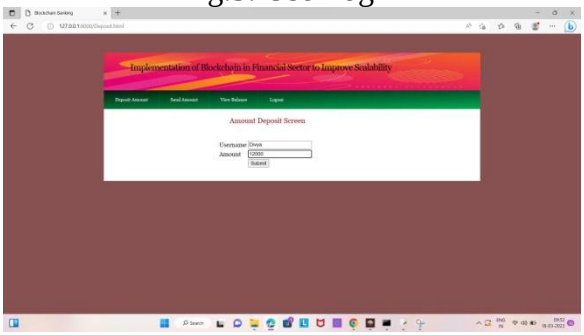

Fig.6: Deposit Amount

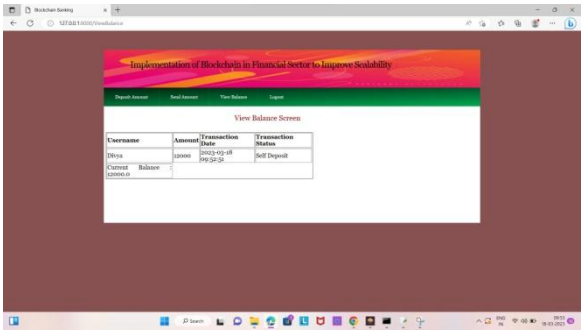

Fig.7: Balance

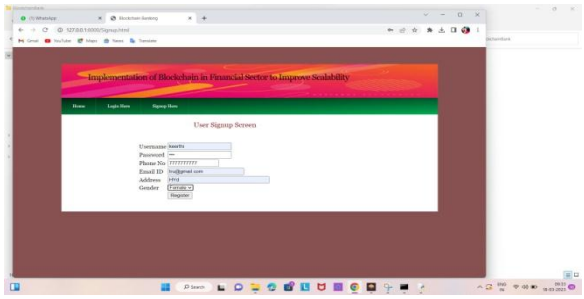

Fig.8: Another user signup

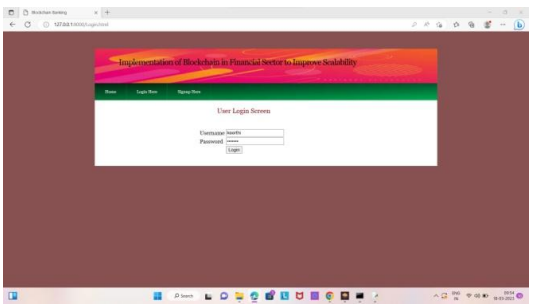

Fig.9: User login

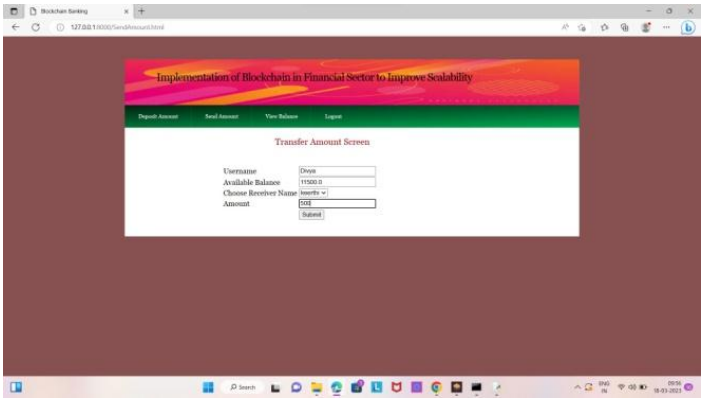

Fig.10 : Send amount

Fig .11: Total balance

4. CONCLUSION

Blockchain technology supporters predicts these use cases will become ubiquitous in financial sector over next 10 years. Additionally, they demonstrate new applications for the Corda/R3 platform in the areas of securities and investment banking, both of which are currently very benefited by it. Conservative voices, on the other hand, caution us against overestimating technology and the fact that the only now popular blockchain applications are cryptocurrencies like Bitcoin. It is unclear what will occur in the medium and long terms. The stated blockchain use cases offer fertile ground for FinTech and InsurTech businesses, among other financial sector innovators.

FUTURE SCOPE

We will keep researching ways to provides off chain settlement to banks that are not mentioned on platform, one possibility is to obtain permission to approach its database, which would permit additional transactions to be made between listed and non-listed banks and support the equal ledger for both.

5. REFERENCES

Tejal Saha and Shalilak Jani, "Applications of Blockchain Technology in Banking and Finance", Parul College, Vadodara, India, February 2018, DOI: 10.13140/RG.2.2.35237.96489

DUSKO KNEZEVIC, “Impact of blockchain technology platform in changing the financial sector and other industries., University Union Belgrade, Serbia, Montenegrin Journal Of Economics, Vol. 14, No. 1(2018), p.p(109-120).

Cong Zhiguo He Working Paper 24399 byLinWilliamhttp://www.nber.org/ papers/w24 399 1050

Massachusetts Avenue Cambridge, MA 02138, National Bureau of Economic Research March 2018, April 2018

In the Asia Pacific Journal of Innovation and Entrepreneurship, Vol. 11 Issue: 3, pp. 312-321, Soonduck Yoo discussed a blockchain-based financial case study and impacts.

C. Miguel and L. Barbara, "Practical byzantine fault tolerance," in Proceedings of the Third Symposium on Operating Systems Design and Implementation, vol. 99, New Orleans, USA, 1999, pp. 173–186.

Underwood, S. (2016), Blockchain beyond Bitcoin, Commun. ACM, Vol. 59,No.11,pp.15–17. https://doi.org/10.1145/2994581

Digital currencies", IEEE Commun. Surv. Tutorials, Vol. 18, No. 3, pp. 20842123.https://doi.org/10.1109/ COMST.2016.2535718.

Greenspan, G. (2015), "Multi Chain Private Blockchain",White Paper Founder and CEO, Coin Sciences Ltd, https://www.multichain.com

M. Vukoli´c, "The quest for scalable blockchain fabric: Proof-of work vs. bft replication," in International Workshop on Open Problems in Network Security, Zurich, Switzerland, 2015, pp. 112– 125.

D. Kraft, "Difficulty control for blockchain-based consensus systems," Peer-to-Peer Networking and Applications, vol. 9, no. 2, pp. 397–413,2016.

I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoinng: A scalable blockchain protocol," in Proceedings of 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), Santa Clara, CA, USA, 2016, pp. 45–59.

I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A scalable blockchain protocol," in Proceedings of 13th USENIXSymposium on Networked Systems Design and Implementation (NSDI16), Santa Clara, CA, USA, 2016, pp. 45–59.

J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W.Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 486–504.

T. Ruffing, P. Moreno-Sanchez, and A. Kate, "Coinshuffle: Practical decentralized coin mixing for bitcoin," in Proceedings of EuropeanSymposium on Research in Computer Security, Cham, 2014, pp. 345–364.

I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous

A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in CRYPTO '86, vol. 263 of LNCS, 1986, pp. 186–194.

A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in Proceedings of the 2014 ACMSIGSAC Conference on Computer and Communications Security, NewYork, NY, USA, 2014, pp. 15–29.

S. Barber, X. Boyen, E. Shi, and E. Uzun, "Bitter to better – how to make bitcoin a better currency," in Financial Cryptography 2012, vol. 7397 of LNCS, 2012, pp. 399–414. digital currencies", IEEE Commun. Surv. Tutorials, Vol. 18, No. 3, pp.2084–2123.

CryptoCurrency Market Capitalizations, Coinmarketcap.com,Available: https://coinmarketcap.com

R. Narendula, T.G. Papaioannou, K. Aberer, A decentralized online

social network with efficient user-driven replication, in: Proceedings of Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom), IEEE, 2012, pp. 166–175.

S. Jahid, P. Mittal, N. Borisov, Easier: encryption-based access control in social networks with efficient revocation, in: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ACM, 2011, pp. 411–415.