

# Survey on Decentralized Payment System by using Blockchain

Ritesh Mohite<sup>1</sup>, Mousin Mulani<sup>2</sup>, Siddhant Basve<sup>3</sup>, Subhanshu Bansal<sup>4</sup>, Dr. Poonam Raskar<sup>2</sup>

U.G. Students, Department of Computer Engineering<sup>1,2,3,4</sup>

Professor, Department of Computer Engineering<sup>5</sup>

Smt.Kashibai Navale College of Engineering, Pune, Maharashtra, India

**Abstract:** Existing interbank payment systems are unable to offer cost-effective cross-border transactions because the correspondent banking process involves a large number of intermediaries operating in various time zones. They also experience lengthy transaction delays and a lack of transparency. These problems can be resolved by creating an auditable coin on a permissioned blockchain, which allows a set of administrators to control the network. Using an auditable cryptocurrency that supports unspent transaction output-based transactions in a consortium blockchain network, we suggest a low-cost, seamless cross-border payment system in this research. Participating nations perform the power-efficient proof of authority consensus method on the blockchain with equal privileges. Dynamic decentralized identifiers (DIDs), as opposed to traditional cryptocurrencies, are utilized as transacting addresses to enable self-manageable authentication.

**Keywords:** Blockchain, Smart Contract, Web 3.0, Meta Mask.

## I. INTRODUCTION

There is a pressing need to create a decentralized trust system. Distrustful parties have collaborated for ages to create societies, economies, and empires. But these alliances and exchanges have always been run by opaque, corruptible structures with huge power disparities. Think about the social contract that exists between a government and its people, for instance. It is challenging to return the system to a state that is agreeable to all parties since one party (the government) has an excessive amount of power.

In a decentralized trust system, numerous parties can work together digitally to complete a certain task without needing to have complete trust in one another. The administration of information is one duty that necessitates decentralized trust.

## II. RELATED WORK

### DCAP: A Secure and Efficient Decentralized Conditional Anonymous Payment System Based on Blockchain

The distributed ledger technology known as blockchain has a wide range of possible uses. Decentralized payment systems, like Bitcoin, have been one of the most developed and well-liked blockchain applications among them. Although early implementations (such as Bitcoin) are frequently the preferred mode of payment by cybercriminals (such as in ransomware instances), they only offer a semblance of anonymity because anybody can deanonymize Bitcoin transactions using information from the blockchain. Solutions like Monero and Zero Cash have been suggested to improve the privacy protection of decentralized payment systems. Completely decentralized anonymous payment (DAP) systems, however, can be misused for illegal purposes, such as online extortion and money laundering. We provide a fresh definition of "decentralized" in recognition of the significance of regulation.

### Blockchain-based Fair Payment Protocol for Deduplication Cloud Storage System

Nowadays, an increasing number of individuals and businesses are opting to outsource their data to cloud storage systems. To reduce the cost of cloud storage, data deduplication technology plays a crucial role. By using a cloud storage system with deduplication, a client can outsource data files to a cloud storage server and pay for them. The issue of fair payment is important in the context of cloud deduplication storage systems. While various secure deduplication

encryption schemes exist to ensure the privacy of client data, most of the current fair payment solutions rely on traditional electronic cash systems that necessitate a trusted authority to prevent double-spending, resulting in bottlenecks in the payment system. To address this issue, this paper proposes a novel decentralized fair payment protocol for cloud deduplication storage systems that leverages ethereum blockchain technology. By taking advantage of blockchain's decentralization, the new protocol enables direct transactions without the involvement of trusted third parties. In the event of a malicious attack, the smart contract stores penalty money to ensure fair payment. Our new protocol is demonstrated to be feasible based on safety and experimental analyses.

### **A Secure Blockchain Lightweight Wallet based on Trustzone**

As the total value of digital currency continues to rise, the security of encryption wallets has become increasingly important. While hardware-based wallets are safe, they are inconvenient due to the need for an additional physical device. Software-based wallets, on the other hand, are convenient but cannot guarantee security. Furthermore, all wallets require blockchain synchronization, which is challenging for most mobile devices that lack sufficient storage capacity. Simplified Payment Verification (SPV) can address this issue, but existing methods fail to protect the transaction verification process effectively. In this study, we propose a Secure Blockchain Lightweight Wallet based on Trustzone (SBLWT) that addresses these challenges. The SBLWT is more portable than hardware wallets and safer than software-based alternatives. It ensures the protection of private keys and wallet addresses from attackers, regardless of whether the Rich OS is malicious. Moreover, it employs the Secure Execution Environment (SEE) to protect the verification process by verifying transactions while keeping local block headers encrypted and unreadable from the Rich OS. We test the SBLWT on a RASPBERRY PI 3 MODEL B development board and find that it has minimal impact on system performance.

### **Digitizing Invoice and Managing VAT Payment Using Blockchain Smart Contract**

Currently, the process for authenticating transactions is complex, and the centralized server-based Value-Added Tax (VAT) administration system is vulnerable to high-risk attacks from hackers. Consequently, only a small number of countries have adopted digital technologies to calculate and manage VAT payments, despite their benefits. In this study, we propose a new model based on blockchain technology that combines a decentralized storage network (DSN) with a smart contract (SC) to authenticate transactions, calculate VAT, and approve VAT payments. The system operates on a host computer (host PC) that encrypts and decrypts data. The smart contract is developed using the Remix Integrated Development Environment (IDE) on the Ethereum platform. Our experimental results indicate that the proposed model not only reduces the cost of authenticating transactions but also provides protection against hacker attacks due to the consensus property of blockchain technology.

### **Blockchain-Based Payment Channel Networks: Challenges and Recent Advances**

Blockchain technology was developed with the aim of facilitating secure collaboration among untrusted parties, without the need for a central authority. However, the technology has encountered a scalability challenge despite its numerous promising applications. To increase transaction throughput and reduce transaction confirmation latency, payment channel networks have been proposed. These networks introduce a layer on top of the main chain, enabling safe transactions to occur solely between the transacting parties without impacting the entire network. In this article, we explore the numerous research aspects presented by this new type of network. We begin by explaining how payment channel networks operate, followed by an overview of various research problems that arise in this context, such as routing, scheduling, rebalancing, network design and topology analysis, and fee optimization. This work is relevant to both the networking and network economics communities.

### **Blockchain and Smart Contract Payment for Electric Vehicle Charging**

Our study focuses on developing an electronic payment system for electric vehicle (EV) charging, leveraging blockchain and smart contract technologies. By using these technologies, we aim to streamline and decentralize the payment process, allowing for automatic payments between devices. Moreover, our proposed system addresses the issue of inadequate charging stations for EVs during long-distance travel. EV owners who have charging facilities at

their homes can share them and receive automatic payments. We set up a blockchain node at the charging station, which is controlled by an application for EV owners. The application displays charging information and automates the payment and charging process. We also simulated data transmission between the charging station and the EV

### **Blockchain Anonymous Trading System based on Multi-Hop Payment**

The emergence of blockchain technology and its benefits, including decentralized trust, not tampered, traceable, and consensus features, have attracted attention from academia and industry. However, the transaction processing speed of the bitcoin network is limited to 7 transactions per second, which makes it unsuitable for many e-commerce applications. The scalability of transaction consensus on blockchain is a challenge issue. The lightning network has been proposed to improve the scalability of the bitcoin transaction through cross-chain consensus. However, anonymity between the seller and buyer remains a privacy challenge for fast blockchain payments. In this paper, we propose a blockchain anonymous trading framework based on multi-hop payment to solve the scalability problem of blockchain transactions and improve efficiency among nodes. Three-session encryption is used to build multiple encryption transaction channels between nodes, and Dijkstra is used to find a minimal anonymous service fee path. Experimental results demonstrate that the lightning network with encryption transaction channels can improve use efficiency, reduce the extra cost of transactions, and guarantee user privacy information.

### **Decentralized Freelancing using Ethereum Blockchain**

The proposed decentralized system based on the public Blockchain Ethereum aims to resolve the issues generated by third-party intermediaries in the freelancing market. The current centralized freelancing websites are prone to manipulation and rely on third-party intermediaries for payment contracts, leading to potential issues in security, trust and transparency.

The proposed system will enable peer-to-peer transactions using cryptocurrency, providing a secure and decentralized payment system that allows for increased trust between freelancers and employers. Additionally, the system will incorporate peer-to-peer reviews on the distributed ledger of Ethereum, enhancing transparency and accountability in the freelancing industry.

By leveraging the capabilities of blockchain technology, the proposed system has the potential to revolutionise the freelancing industry, providing an efficient and secure platform for freelancers and employers to transact without the need for intermediaries. The decentralized nature of the system ensures that all parties involved have greater control over their transactions, leading to increased trust and transparency in the industry

## **III. EXISTING SYSTEM**

### **3.1 Traditional Payment**

The primary contrast between traditional banking and online banking lies in their physical presence. Traditional banks typically have headquarters, regional offices, and branches dispersed across countries where they operate, often with their own ATMs. Some smaller traditional banks may collaborate to operate a larger network of ATMs to manage costs. The local branches of traditional banks were originally selected for their convenience and personalized customer service through face-to-face interactions. On the other hand, online banking lacks physical branches and relies on digital platforms for banking services.

### **3.2 Online System**

To remain competitive and meet customer satisfaction, many traditional banks have integrated internet banking into their services. Online portals enable customers to access features such as viewing balances, transferring funds, opening new accounts, and applying for mortgages, all available round-the-clock, unlike physical branches. Online customer service, including email, chat, and video calls, is increasingly becoming more prominent compared to phone calls or in-person visits to a bank branch

#### **IV.CONCLUSION**

The Decentralized Conditional Anonymous Payment System (DCAP) that you describe sounds like an interesting and innovative approach to improving anonymity and governance in payment systems. Your use of a formal semantics and security model for defining a conditional anonymous payment (CAP) scheme is commendable, as it provides a solid foundation for the design of the DCAP.

It is also encouraging to see that you have tested the performance of your prototype and compared it to that of Zerocash, another popular privacy-focused cryptocurrency. The fact that your proposal is practical for real deployments is a promising sign for future adoption.

Working with a real organization to adapt and implement your proposal in a real environment is a wise next step, as it will allow you to identify additional features or properties that may be necessary for success. Overall, your research appears to have valuable contributions to the field of anonymous payment systems and blockchain technology.

#### **REFERENCES**

- [1]. DCAP: A Secure and Efficient Decentralized Conditional Anonymous Payment System Based on Blockchain. 2020 [Chao Lin]
- [2]. Blockchain-based fair payment protocol for deduplication cloud storage system. 2019 [Yuying Wang]
- [3]. A Secure Blockchain Lightweight Wallet based on Trustzone. 2018 [Weiqi Dai, Jun Deng]
- [4]. Digitizing Invoice and Managing VAT Payment Using Blockchain Smart Contract. 2020 [Van-Cam Ngyugen, Hoai-Luan Pham]
- [5]. Blockchain-Based Payment Channel Networks: Challenges and Recent Advances. 2020 [Nikoloas Papadis]
- [6]. Blockchain and Smart Contract Payment for Electric Vehicle Charging. 2020 [Nathanan Chanthong,Thitiwat Ruangsakorn,Sorayut Glomglome]
- [7]. Blockchain anonymous trading system based on multi-hop payment. 2020 [Weiwei Zhang]
- [8]. Decentralized Freelancing using Ethereum Blockchain. 2020 [Prathmesh Deshmukh, Shreyas Kalwaghe, Ajinkya Appa and Aprupa Pawar]
- [9]. Risk Management in Payment System Architectures. 2016 [Boullier Dominique]
- [10]. A Low-Cost Cross-Border Payment System Based on Auditable Cryptocurrency with Consortium Blockchain: Joint Digital Currency . 2022 [Md. Mainul Islam,Md. Kamrul Islam, Md. Shahjalal , Mostafa Zaman Chowdhury , Yeong Min Jang ]