AN ENHANCED BLOCKCHAIN-BASED DIGITAL MONEY TRANSACTION USING STRONG ENCRYPTION DISTRIBUTED LEDGER TECHNOLOGY

Mrs.Jeyapriya Assistant Professor, Department of Computer Science, Sri Krishna Arts and Science College (Autonomous), Coimbatore

Abstract

In recent times, blockchain currencies have seen increased usage over traditional fiat currencies by consumers who value anonymity and security. Currencies that use a blockchain, such as cryptographic currencies ("cryptocurrencies"), offer consumers a currency that is decentralized and relatively anonymous and secure in its use. A transaction that is posted to a blockchain may not require any information regarding the sender or recipient of the currency, and thus may enable the payer and payee of a transaction to retain anonymity. Such an aspect of blockchain transactions may be highly desirable for consumers that wish to maintain their privacy, and may help reduce the likelihood of fraud due to theft of their information. However, while blockchain currencies can often provide such safety and security for the payer's information, such security may be limited for payees, particularly due to the limitations of the blockchain. It often takes a significant amount of time, around ten minutes, for a blockchain-based transaction to be processed, due to the computer processing time and resources required to verify and update the blockchain.

Bitcoin is an open source, decentralized, peer-to-peer payment network maintained by users, with no central authority. Bitcoin provides completely digital money for transactions on the Internet/web.

Introduction

The nature of blockchain currencies is that the access to any given address to which credentials, often referred to as an electronic wallet, e-wallet, or simply "wallet." As such, if the wallet is lost, discarded, or stolen, the associated currency often cannot be recovered by the rightful owner and may be used without their knowledge and permission. Furthermore, because of the anonymous nature of the blockchain, the consumer may be unable to prove their identity and ownership of a wallet, and thereby have little recourse if their wallet and/or associated currency is stolen. Thus, there is a need to improve on the storage and processing of transactions that utilize blockchain currencies. Existing payment networks and payment processing systems that utilize fiat currency are specially designed and configured to safely store and protect consumer and merchant information and credentials and to transmit sensitive data between computing systems. In addition, existing payment systems are often configured to perform complex calculations, risk assessments, and fraud algorithm applications extremely fast, as to ensure quick processing of fiat currency transactions. Accordingly, the use of traditional payment networks and payment systems technologies in combination with blockchain currencies may provide consumers and merchants the benefits of the decentralized blockchain while still maintaining security of account information and provide a strong defense against fraud and theft.

Blockchain currency Database

A method for managing fractional reserves of blockchain currency includes: storing, in a first central account, at least a fiat amount associated with a fiat currency; storing, in a second central account, at least a blockchain amount associated with a blockchain currency; storing, in an account database, a plurality of account profiles, wherein each account profile includes data associated with a consumer including at least a fiat currency amount, a blockchain currency amount, an account identifier, and an address; receiving, by a receiving device, a transaction message associated with a payment transaction, wherein the transaction message is formatted based on one or more standards and includes a plurality of data elements, including atleast a data element reserved for private use including a specific address and a transaction amount; identifying, by a processing device, a specific account profile stored in the account database where the included address corresponds to the specific address included in the data element in the received transaction message; and updating, by the processing device, the blockchain currency amount included in the identified specific account profile based on the transaction amount included in the data element in the received transaction message.

A system for managing fractional reserves of blockchain currency includes a central database, an account database, a receiving device, and a processing device. The central database is configured to store: a first central account including at least a fiat amount associated with a fiat currency; and a second central account including at least a blockchain amount associated with a blockchain currency. The account database is configured to store a plurality of account profiles, wherein each account profile includes data associated with a consumer including at least a fiat currency amount, a blockchain currency amount, an account identifier, and an address. The receiving device is configured to receive a transaction message associated with a payment transaction, wherein the transaction message is formatted based on one or more standards and includes a plurality of data elements, including at least a data element reserved for private use including a specific address and a transaction amount. The processing device is configured to: identify a specific account profile stored in the account database where the included address corresponds to the specific address included in the data element in the received transaction message; and update the blockchain currency amount included in the identified specific account profile based on the transaction amount included in the data element in the received transaction message.

Block diagram of system architecture for blockchain currency storage

Fig: 1 a block diagram illustrating a high level system architecture for managing blockchain currency storage and linkage thereof to privately verified identifies and use thereof in the processing of blockchain transactions using payment networks

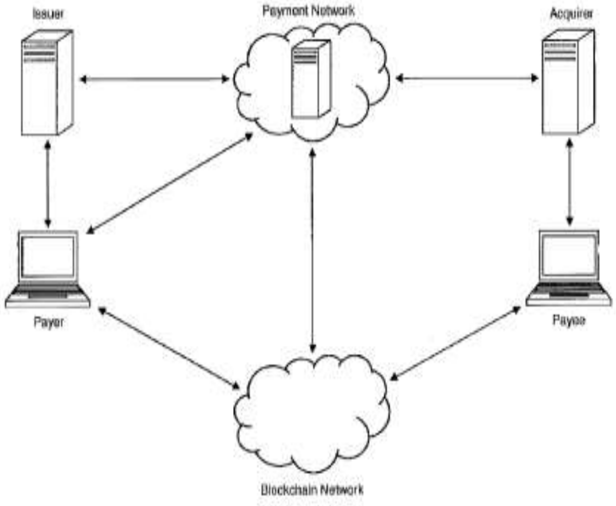

FIG. 1

FIG. 1 illustrates a system for the managing of blockchain and fiat currency and use thereof in payment transactions using a traditional payment network, including the linkage of verified identifies to blockchain¬based transactions and assessing of risk in blockchain-based transactions.

In the system, a blockchain transaction may occur between the computing device of a payer and the computing device of a payee. As used herein, "payer" may refer to a computing device and/or a consumer that is funding a payment transaction, and "payee" may refer to a computing device and/or a consumer that is receiving payment in a payment transaction. The blockchain transaction may be processed by one or more computing devices that comprise a blockchain network. The blockchain network may receive at least a destination address (e.g., associated with the payer) and an amount of blockchain currency and may process the transaction by generating a block that is added to a blockchain that includes a record for the transaction.

The computing device of the payer may digitally sign the transaction request using an encryption key stored in the computing device, such as stored in an electronic wallet. The digital signature may be, include, or otherwise be associated with an address that is generated using the encryption key, which may be associated with blockchain currency in the blockchain, and may be used to transfer blockchain currency to an address associated with the payee and/or their computing device. In the address may be encoded using one or more hashing and/or encoding algorithms, such as the Check encoding algorithm.

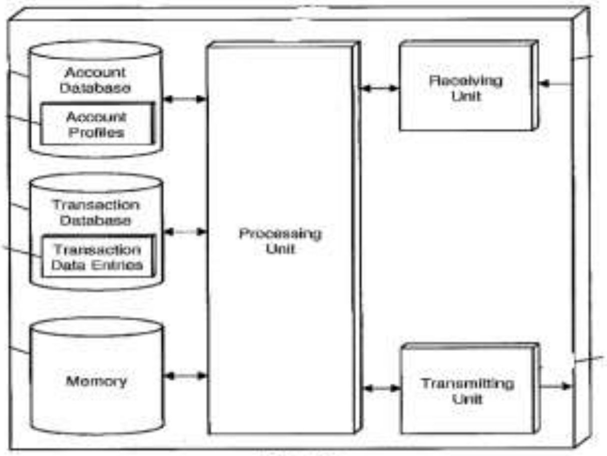

FIG. 2

FIG. 2 is a block diagram illustrating the processing server of FIG. I for authorizing blockchain transactions and linking blockchain transactions to privately verified identifies.

Permissioned Ledgers

Permissioned, or private ledgers have attracted attention from businesses (Bogart & Rice, 2016). This type of ledger restricts transparency by disclosing the identity of participants in the network; access is restricted to a certain number of participants, which are known to each other, and is subjected to approval from other members of the network.

No ‘proof-of-work’ is needed to validate transactions, unlike in the case of permissionless ledger, and therefore there is no incentivization system (Biondi et al.,2016). Permissioned ledgers can be distributed for closed communities that share similar but competing interests, or they can be private for one or more organizations that share common interests.

Permissionless ledgers

Permissionless, or public, ledgers are seen by some as the ‘purest’ form of Blockchains (Brennan & Lunn,2016). A typical example of a permissionless, or public, Blockchain is the one that underlies the Bitcoin network. In this type of configuration, the participation is ‘permissionless’ and anyone can take part in the ledger and validate transactions, with fully devolved authority (Bogart & Rice, 2016). Participants are identified through pseudonyms or are kept anonymous, and transactions are validated by ‘miners’ through an incentivization system (Biondi et al., 2016). This form of distributed ledger enables high security but also incurs high transaction costs due to the resource-intensive consensus mechanism8 (Brennan & Lunn, 2016)

Distributed Ledger Technology(DLT)

DLT/Blockchain is likely to require individual users to interact with the ledger and
transact using their individual private keys. Therefore, the management of keys – and protocols for key loss or theft – will be important (Mills et al., 2016), and they must be designed to avoid

introducing additional vulnerabilities through a 'back door' (Tierion, 2016).For ledgers that are shared between multiple legal entities – whether permissioned or permissionless – a key challenge will be establishing liability among partners for the activities taking place on the ledger. Examples are liability for losses experienced by businesses in the event of an operational failure or compromised keys, or legal responsibility in the event of data loss or theft.

DLT/Blockchain would need to carefully consider the security and integrity of end-users' data stored on the ledger. The decentralized nature of DLT/Blockchain and the distributed access and management rights across multiple nodes in the network could present
a serious security risk, with malicious entities potentially having multiple 'back doors' through which to attack the system

Strong encryption in Distributed Ledger Technology(DLT)

DLT/Blockchain may present opportunities in this regard, such as multiple copies of a ledger in the event of a cyberattack or computer failure, the distribution of access and management rights across multiple nodes may in itself present a security risk, in that malevolent entities have multiple 'back doors' through which to attack the system . The issue of trust in the system, ascertaining integrity of other users in the distributed ledger, and carrying out transactions in a consistently secure manner are thus key challenges to wider DLT/Blockchain adoption.

DLT/Blockchain can remove the need for actively intermediated data synchronization and concurrency control by a trusted third party in a supply chain, and this could also translate into efficiency gains (Mattila et al., 2016). Similar observations are made by Brennan & Lunn (2016), who argue that the opportunity for sectors which currently rely on trusted third-party intermediation could be in the form of cost removal, improved transactional efficiency and novel revenue streams.

DLT Based Ledger increases security in transactional systems

DLT/Blockchain has the potential to increase the resilience of systems and data storage due to its distributed nature and its lack of a central point of failure (Deloitte, 2016 et al.,). The opportunities provided by the distributed nature of the technology are also highlighted by Mainelli (2017), who suggests that DLT/Blockchain provides a technology that is not owned by a single entity and that therefore in the event of failure everyone can keep their own copy of data and transactions. This form of resilience and security provides the opportunity to create new identity systems where users own the data, which remains universally consistent and cannot be destroyed.

Conclusion

The purpose of this paper is to review extant research on this technology and assess the impact of blockchain in the audit profession, including new risks, change in procedures and additional opportunities. There are many challenges to contend with although it is a field characterized by rapid change and uncertainty, steps can be taken to better understand the current realities of DLT/Blockchain.As any other technology, Blockchain is evolving and
therefore, the information provided on this paper may need to be revised in the near future.

References

1) Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf. Accessed 4 November 2019
2) O'leary, D. (2017). Configuring Blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems. Intelligent Systems in Finance, Accounting and Management, 24, 138-147. https://doi.org/10.2139/ssrn.3102671

3) O'neal, S. (2019). Big Four and Blockchain: Are auditing giants adopting yet? https://cointelegraph.com/news/big-four-and-blockchain-are-auditing-giantsadopting-yet. Accessed 17 October 2019

4) Rozario, A. & Vasarhelyi, M. (2018). Auditing with smart contracts. The International Journal of Digital Accounting Research, 18 (1), 1-27.https://doi.org/10.4192/1577-8517-v18_1

5) Fanning, K. & Centers, D. (2016). Blockchain and its coming impact on financial services. The Journal of Corporate Accounting and Finance, 53-57.https://doi.org/10.1002/jcaf.22179.https://onlinelibrary.wiley.com/doi/pdf/10.1002 /jcaf.22179. Accessed 28 February 2019