2020 7th International Conference on Dependable Systems and Their Applications (DSA) | 978-0-7381-2422-3/20/$31.00 ©2020 IEEE | DOI: 10.1109/DSA51864.2020.00018

A Survey of NFC Mobile Payment: Challenges and Solutions using Blockchain and Cryptocurrencies

Dongcheng Li, W. Eric Wong*, and Matthew Chau
University of Texas at Dallas
Richardson, USA
{dxl170030,ewong,mcc180003}@utdallas.edu

Sean Pan and Liang Seng Koh
RFCyber Corporation
Texas, USA
{sean.pan,liangseng.koh}@rfcybercorp.com

***Abstract*—Near-field communication (NFC) is one of the essential technologies in the Internet of Things (IoT) that has facilitated mobile payment across different services. The technology has become increasingly popular, as cryptocurrencies like Bitcoin have revolutionized how payment systems can be designed. However, this technology is subject to security problems, such as man-in-the-middle attacks, double-spending, and replay attacks, raising the need to incorporate other solutions such as blockchain technology. Concerns about the security and privacy of payments using NFC technology raise the need to adopt blockchain-based cryptocurrency payment. For instance, NFC payment has been criticized for a lack of measures to counter potential attacks, such as brute force or double-spending. Thus, incorporating blockchain technology is expected to improve the security features of the NFC mobile payment protocol and improve user experience. Blockchain technology has been praised for enabling fair payment, as it permits direct transactions without engaging a third party. Therefore, integrating blockchain cryptocurrency in IoT devices will revolutionize the NFC payment method and provide value transfer using IoT devices. Combining NFC with blockchain technology and cryptocurrencies is necessary to address security and privacy problems. The purpose of this paper is to explore the potential behind incorporating blockchain technology and cryptocurrencies like Bitcoin in the NFC payment protocol.**

***Keywords*—NFC mobile payment, blockchain, cryptocurrency, fair payment, security, privacy**

I. INTRODUCTION

Near-field communication (NFC) is an essential technology in the Internet of Things (IoT) [1]. It is a communication technology with a short-range and high frequency, suitable for micropayments, electronic tickets, and access-control functions, and is mostly used in the finance and transport industries [2]. Many NFC mobile payment protocols have been widely used and have attracted significant attention from researchers in recent years. This technology has been vital in improving the global economy, with a consequent improvement in human well-being. As a result, NFC mobile payment has become a prominent way to conduct sales transactions in mobile commerce [3]. The introduction of Bitcoin revolutionized how payment systems can be designed and at the same time provided a novel blockchain data structure that can be adapted in several applications for the storage of data. Due to these data structures, blockchain is considered an innovative solution that can be vital in logistics and finance.

NFC has become increasingly popular, but security problems such as man-in-the-middle attacks have hindered its development [4]. To address this security problem, NFC could adopt other measures, such as blockchain technology. Compared to traditional identification technology, NFC provides a wireless connection that is fast and straightforward and offers high compatibility, together with secure elements for storing data [5]. NFC is robust, making it useful for payment and verification that require stable performance in high transaction demand, such as electronic tickets and movie tickets [6]. Despite these advantages, NFC faces many security problems. For instance, in a wireless communication environment, the information that is exchanged between devices makes NFC vulnerable to different forms of security attacks, such as the brute force attack, which may lead to the disclosure of a user's private information. Such security problems have become a growing challenge hindering the development of NFC.

Previous studies have proposed schemes that use hash function encryption to eliminate privacy and security threats [6]. Although this solution would prevent replay attacks and solve mutual authentication, it lacks vital security attributes such as message authentication. The use of electronic tickets has grown in recent years. However, security and privacy problems still exist in the ticket purchase and verification process, raising concerns among users. For the purchase process, some studies have proposed a scheme using symmetric encryption, calibration values, and asymmetric encryption [5].

This paper explores the potential of a novel mobile electronic payment and verification system that combines NFC technology with blockchain technology and cryptocurrency to address the rising security and privacy concerns of the clients.

II. NFC-BASED MOBILE PAYMENT

NFC is a short-distance technology defined in ISO/IEC 18092 [4]. The NFC structure used in communication between devices operates at a frequency of 13.56 MHz. NFC devices allow for two-way communication and ensure security using the complementary series of NFC cryptography standards (NFC-SEC). Communication between NFC devices can extend to 424 kbps, although the maximum communication range is 4 cm. NFC services have been used for such purposes as payment, coupons, and ID

978-0-7381-2422-3/20/$31.00 ©2020 IEEE
DOI 10.1109/DSA51864.2020.00018

cards. The system also allows for authentication of corporate access rights.

NFC mobile payment constitutes a collaboration between mobile phone manufacturers, operating system vendors, and banking organizations [7]. Furthermore, the NFC mobile payment system consists of a server, mobile devices, a mobile verification terminal, and a mobile point-of-sale (POS) terminal. The payment process has four stages: registration, booking, purchase, and verification. Moreover, communication for e-ticket registration and booking is carried out wirelessly [8].

NFC technology has been embedded in smartphones and mobile devices to enable the smart transfer of data and speedy and short-range communication [3]. Furthermore, NFC has also been widely used as a medium for communication in mobile payment systems, allowing customers, for instance, to purchase products from a merchant's store easily and conveniently [9].

A protocol has been proposed based on cloud-based security. This protocol is secure, overcoming vulnerabilities that emerge in Europay, MasterCard, and Visa standards, as the transactions are completed in an open environment using NFC radio waves [6]. However, this protocol also does not have the security features to prevent double-spending or brute force attacks [10]. Another protocol is the anonymous mobile payment protocol used for improving the privacy issues in mobile transactions. This protocol satisfies anonymity, non-repudiation, and unlinkability. However, it has been criticized for lack of security measures, as it offers no message integrity or prevention of brute force attacks [1].

Another proposal has been made to guarantee the transfer of money securely through several NFC mobile payment protocols [2]. One of the secure mobile payment protocols is the secure contactless NFC payment protocol using an NFC bank card that is based on online communication via an entity that is trusted. However, the protocol has no security measures, such as double-spending detection and the prevention of brute force attack and eavesdropping [4]. Furthermore, the protocol lacks fairness, as it was controlled by a single entity.

A. Benefits of NFC Mobile Payment

NFC mobile payment is now at the forefront of most economic activities. The adoption of NFC mobile payment has numerous advantages. The first significant advantage is convenience [11]. For instance, users who make transactions with NFC can make fast payments using solutions like Google Pay and Apple Pay that are pre-installed on their devices. The NFC payment process is simple to understand and easy to use.

The second benefit is versatility. NFC mobile payment is very flexible, covering various business applications [12]. It can be used for mobile banking, movie passes, restaurant reservations, train ticket bookings, and real-time updates on the user's expenditure.

Furthermore, most users report that NFC mobile payment offers a better user experience than traditional card or cash payment [3]. It helps users and organizations adapt to the latest technological developments [3]. NFC technology offers users a comfortable and uncomplicated payment solution. The improved user experience enabling organizations to gain loyalty and attract new customers.

NFC mobile payment has also been praised for improving payment security. For instance, using mobile wallets is to some extent safer and more secure than using physical credit cards or cash. Moreover, if users lose their mobile devices, their card information is protected by password, face ID, or fingerprint recognition, thus adding another layer of security [2]. Nowadays, the most popular platforms for contactless NFC-enabled mobile payments in North America are Apple Pay and Google Pay [11] [13].

1) Apple Pay

Apple Pay allows users to make transactions with ease while guaranteeing security when purchasing products through apps. It also facilitates the transfer of money between users and their family members or friends [13]. The contactless reward card in the wallet allows users to receive and redeem rewards when paying. The system's design has taken security and privacy matters into consideration to improve user experience beyond the service offered by physical debit and credit cards.

When Apple Pay is used in stores that accept contactless payments, NFC technology is used between the user's device and the payment terminal. NFC contactless technology was designed for use when devices are in close range. Thus, when sending payment information, users must authenticate using Apple's Face ID, Touch ID, or passcode [13]. For Apple Watches, Face ID requires individuals to double click the side button when the device is unlocked to activate their default card for payment. Once authentication is finished, the secure element will provide the user's device account and a security code specific to a particular transaction. Any additional information associated with the transaction will also be provided before the user completes the payment [13]. Furthermore, neither Apple nor the user's device will send the actual number of the payment card. Before payment is approved, the user's bank, card issuer, and payment network will verify the payment information [13]. The verification process entails determining the uniqueness of the dynamic security code of the user's device.

Apple Pay offers an easy-to-use, secure, and private electronic payment service for iPhone, iPad, Mac, and Apple Watch users. The app has retail compatibility thanks to PayPass technology, enabling users to store loyalty cards and accrue loyalty points. In store, users can pay with compatible POS systems with a single press of the side button [13]. The technology ensures that users do not have to enter the security codes on their cards, as all information is on their devices.

2) Google Pay

Google Pay's latest feature allows users to add NFC-powered credit and debit cards as a payment option alongside their existing bank accounts. This development permits Google to leverage tokenized payment cards. With tokenization enabled across the Google Pay payment platform, Android users can now make transactions on NFC enabled POS terminals and online merchants via phones.

Using the tokenization method, users will no longer have to use their debit or credit cards physically. To offer this feature, Google collaborated with Visa and other banking partners. The feature is currently available for Axis and SBI cardholders [13]. Google Pay will soon extend this feature to Kotak and other banks. Payments are managed via secure digital tokens attached to smartphones so that users do not have to share card details with vendors [13]. Use of the NFC feature requires phones that are capable of supporting NFC transactions.

Google recently made Google Pay easier to access on Pixel phones and other Android phones. A new power button prompt means that users are only a button tap away from their payment cards [13]. Thus, after Google Pay embraced the NFC technology, choosing which card to pay with has become more convenient.

Google merged its Android Pay and Google Pay services into a single unified service allowing users to include their cards for more manageable payment and fast checkout. NFC technology is used to relay the user's credit card information between the seller's card reader and the user's mobile device [13]. However, most users of mobile payment consider security as their top priority, owing to the nature of the financial information they share. Google Pay manages this concern using virtual account numbers, which keeps users' personal information safe and secure on their phones.

When a user makes a purchase, Google Pay sends a security code to the user's phone to verify the transaction. Furthermore, unlike Apple Pay, Google Pay does not require fingerprint authentication except for unlocking the screen.

B. Challenges and Concerns of NFC Mobile Payment

Lack of communication security primitives in the lower layers of NFC technology is one factor that makes this payment system susceptible to a wide range of attacks and vulnerabilities. NFC-based mobile payment protocols have, for some time, reported weak data security and payment fairness. As a result, NFC payment has been subject to different forms of attack, such as man-in-the-middle, double-spending, and brute force [7]. Without fairness in NFC mobile payment, it is impossible to create trust among all parties involved in the sale transaction.

Users have broadly used NFC as a communication medium in mobile payment systems. The system allows customers to transfer money to merchants using their mobile phones [7]. However, at the physical level, implementation of NFC payment concentrates on the speed of communication rather than the security of the transmitted data [5]. Securing the data of mobile payments should be considered vital in the NFC protocol. For instance, without this security, many threats are bound to occur on NFC-based data communications.

Three forms of attack can occur when using an NFC payment system. The first is a replay attack, where an attacker takes control of the link between two NFC devices [2]. The intruder can intercept data shared by the user before they reach the intended destination and use them for various purposes, such as stealing personal information. An example of a replay attack is the man-in-the-middle attack. The second form of attack is data manipulation, where attackers intercept and alter data during the communication [3]. The final form of attack is eavesdropping, where an attacker steals data shared by the user by using a massive antenna. The main problem that facilitates this attack is that NFC lacks countermeasures to protect the user from eavesdropping.

Researchers have proposed a variety of NFC mobile payment protocols, but they still lack measures to counter potential attacks [12]. For instance, the NFC contactless payment protocol does not have security features that protect users from brute force attacks that could be contained by implementing double-spending detection schemes [12]. Other proposed NFC protocols have also been found to lack measures to counter security challenges such as message integrity, mutual authentication, and fairness [11]. Thus, NFC protocols lack both fairness and information-security measures.

Studies on the use of NFC payment have shown that payment scenarios based on NFC technology increase security and privacy risk, given the vulnerable protocol used in the devices [1]. Due to this lack of security measures, malicious users and intruders can issue a bogus payment or impersonate legitimate users and receive payments for services they did not provide [6][10]. Another concern with NFC payment protocols is the potential for external adversaries to devise a logic link that intercepts communication between the user and the intended destination [4].

NFC protocols have also been criticized for several security concerns connected to transactions carried out over the device interface. The first is the possibility of installing malicious applications on NFC-enabled devices, such as malware, which can become a significant security concern when making transactions [9]. The second is the presence of side channels over shared components like smart cards, as secret information can be overwritten or extracted from the cards. The last avenue is malicious operating systems that attackers can use to gain privileged access to the devices and exploit vulnerabilities [8]. A combination of these issues explains why NFC tags can contain malicious threats similar to malicious URLs. For instance, an attacker could spoof the content of NFC tags and redirect users to the attacker's website, from where malicious codes could be installed on the NFC-enabled devices. In recent years, numerous studies have aimed to improve the security, privacy, and fairness of NFC mobile payment. The classification and major contributions of those studies are shown in Table I.

TABLE I. THE CLASSIFICATION AND MAJOR CONTRIBUTIONS OF STUDIES ON NFC MOBILE PAYMENT

Category	Topic	Ref. No	Year	Major Contribution	Good Attributes
User Privacy	NFC-based mobile payment protocol with user anonymity	[2]	2016	Proposes a system in which all transactions are encrypted	Non-repudiation, message confidentiality, user anonymity
	Mutual authentication scheme for NFC mobile payment	[12]	2015	Proposes a mutual authentication scheme based on GSM	Message authentication, user privacy
	Lightweight and secure NFC mobile payment protocol using symmetric cryptographic primitives	[1]	2016	Demonstrates a simple, scalable, and cost-effective security solution for resource-constrained devices and establishing secure NFC payments	User privacy, non-repudiation, message confidentiality, user anonymity
Mutual Authentication	Key authentication for NFC mobile payment	[9]	2017	Introduces a framework for achieving payment security and a key authentication scheme using bilinear pairing	Message authentication
	Secure end-to-end proximity NFC mobile payment protocol	[4]	2019	Proposes a protocol with security measures and lower communication costs	Message authentication
	Fraud analytics for NFC-enabled mobile payment system	[10]	2018	Prevents fraudulent transactions through a layered approach to NFC payment	Device authentication
User Experience	NFC secure payment and verification scheme for mobile payment	[3]	2016	Proposes an NFC mobile electronic ticket secure payment and verification scheme that uses a CS E-Ticket and offline session key generation and distribution technology to prevent major attacks	User-friendly, message authentication and integrity
	Integrated mobile payment, ticketing and couponing solution based on NFC	[7]	2014	Presents an integrated mobile service solution based on multiple NFC protocols	User-friendly, good compatibility
	Fair exchange in NFC-based mobile payment with a hybrid encryption algorithm	[11]	2017	Introduces a protocol that satisfies security properties such as integrity, resists attacks such as double-spending, and guarantees fairness in payment	Fairness of exchange, message confidentiality
Message Confidentiality	Organizational aspects and anatomy of an attack on NFC/HCE mobile payment systems	[5]	2015	Analyzes the anatomy of possible attacks, uncovering vulnerabilities and suggesting possible countermeasures for financial businesses offering mobile payment	Message confidentiality, message authentication, non-repudiation
	Anonymous authentication scheme for the protection of payment information in NFC mobile environment	[6]	2013	Proposes a zero-knowledge proof scheme and ring signature based on NTRU for protecting user information in NFC mobile payment systems without directly using the private financial information of the user	Non-repudiation, message confidentiality
	Fair exchange in NFC-based mobile payment with a hybrid encryption algorithm and formal verification	[8]	2019	Proposes a lightweight and secure NFC mobile payment protocol with comprehensive properties	Message confidentiality, integrity, and authentication, Fairness of exchange

III. CRYPTOCURRENCY-ENABLED MOBILE PAYMENT

Blockchain serves as a facilitating technology for evolving cryptocurrencies like Bitcoin to improve the value of peer-to-peer exchange without including a third party. It is an immutable, distributed, and append-only data structure that is developed by block sequences that are tied together chronologically [14]. The network is composed of a set of nodes (validator and miner) that keeps trust records of all transactions based on algorithms in a trustless environment [15]. Blockchain facilitates the idea of smart contracts, also known as the “unstoppable code”, defined as programs that every blockchain node runs automatically and updates the replica based on the execution results without a third party's intervention [16], which ensures the fairness of exchange between multiple parties.

One prominent feature of blockchain-enabled cryptocurrencies is transparency, which means that every participant in the network can view all transactions stored on the blockchain [17], which establishes trust among users.

Another critical feature of blockchain-enabled cryptocurrency is liveness, also known as finality or eventuality of the consensus, which allows every participant to reach the same blockchain while continuously embedding new valid transaction blocks [18][19], this offers mutual authentication to all involving parties. Blockchain-based cryptocurrencies also have the block’s information and the message sender’s wallet address bound to the hash of the public key [20]. The security of the digital signature guarantees that no attacker can send messages without the secret key [21], which guarantees the confidentiality of all engaged parties and the Non-repudiation of each transaction.

A. Benefits of Cryptocurrency-Enabled Mobile Payment

Blockchain-enabled cryptocurrencies offer attractive advantages over the traditional models, such as the ability to operate without a trusted third-party to ensure fairness of exchanges, establish trust across business networks and among people, offer a system with fault tolerance and an immutable history of the data, and provide cryptographic operations, such as digital signatures and hash functions, embedded in every transaction of every chained block, which guarantees the inalterability and integrity of the data stored, as well as deliver a high degree of anonymity for their users' identity and full transparency of the activities recorded on the ledger while simultaneously increasing user privacy and ensuring data security and tamper-resistance [22][23], all through the blend of a distributed ledger, smart contracts, cryptographic algorithms, and group consensus. Table II compares some of the most popular cryptocurrencies.

One significant aspect of blockchain-based cryptocurrencies is their application for lightweight clients and privacy. Most open blockchain platforms have met the heavy resource requirements by supporting lightweight clients and targeting devices such as smartphones that only download and verify a small certain part of the chain [20]. Solutions like Pico Coin and the Simple Payment Verification model have enabled clients to connect to a full node that has access to complete chain, which assists in action confirmation [24].

The transactions provided by blockchain-enabled cryptocurrencies contain input and output bound to the address owned by the user [25]. The provisions of blockchain-enabled cryptocurrencies have improved user privacy, as a full node has to validate all transactions by the client to confirm them, which may result in a user privacy violation [26]. To mitigate this issue, many cryptocurrencies provide clients with support filters to improve user privacy, which allow clients to define anonymity sets to hide their real addresses from the full node [21]. An example in the Bitcoin blockchain is the bloom filters that allow clients to define a set of transactions with false-positives as requested from the full node [27]. Moreover, the approach involves a trade-off between privacy and communication efficiency [28]. For instance, a filter returning many false-positives provides a large anonymity set but demands more communication [26].

Blockchain-based cryptocurrencies provide security measures against double-spending attacks on transactions. For instance, ByzCoin mitigates double-spending and selfish mining attacks by producing collectively signed transaction blocks within one minute of the transaction submission [29], therefore alleviating the propagation delay problem and reducing the possibility of double-spending attacks. In a blockchain peer-to-peer network, an attacker gaining control of the entire network is rather unrealistic. Messages are authenticated through cryptographic functions and spoofing is infeasible [29].

Finally, when using blockchain-based cryptocurrencies among lightweight clients, the user cannot be sure that they have received all the transactions fitting their filter from a full node [23]. For instance, the full node may not include faulty transactions in response since the client will detect any faulty transactions when computing the Merkel root [30]. However, the clients will not be able to detect whether they have received all the transactions they requested.

TABLE II. COMPARISON OF POPULAR CRYPTOCURRENCIES

	Algorithms	**Permissioned**	**Decentralized level**	**Consensus**	**51% attack**	**Double-spending attack**	**Scalability**	**Smart contract language**	**TPS**	**Block Time (Minutes)**
EOS	SHA256, secp256k1, ECDSA	Yes	Semi-centralized	DPoS	Vulnerable	Vulnerable	Relatively Strong	C, C++	4000	0.5
XRP	SHA256, secp256k1, ECDSA	Yes	Decentralized	PBFT	Relatively Safe	Relatively Safe	Relatively Strong	Golang, C++	1500	0.06
Bitcoin	SHA256, secp256k1, ECDSA	No	Decentralized	PoW	Vulnerable	Vulnerable	Low	Golang, C++	7	10
Litecoin	SHA256, secp256k1, ECDSA	No	Decentralized	PoW	Vulnerable	Vulnerable	Low	Golang, C++	28	2.3
Zcash	SHA256, secp256k1, Jubjub, ECDSA, zk-SNARKs	No	Decentralized	PoW	Vulnerable	Vulnerable	Low	C++	27	2
Stellar	SHA-256, SHA-512, ed25519, EdDSA	No	Decentralized	PBFT	Relatively Safe	Relatively Safe	Relatively Strong	Solidity	1000	0.08
Tezos	BLAKE2, SHA-512, ed25519, secp256k1, secp256r1, EdDSA, EC-DSA	No	Semi-centralized	DPoS	Vulnerable	Vulnerable	Relatively Strong	Michelson	1000	1

B. Challenges and Concerns of Blockchain-Based Cryptocurrencies

The security threat is a significant issue with exchange platforms, wallet providers, mining pools and other intermediaries that provide custodian services for cryptocurrencies. Today, various schemes for preventing such cyber threats have been introduced to facilitate the assets and privacy protection of the users [41]. However, most of the current strategies for the crypto-intermediaries to prevent cyber threats have not been advanced to provide bank-level security to successfully avoid cyber-attacks [41]. The custodian service providers for cryptocurrencies provides its users with quick access to their funds and allow users to trade their cryptocurrencies into fiat currencies with ease. This kind of user-friendless also create a false sense of security to less informed users [41].

The use of bloom filters in blockchain-enabled cryptocurrencies when receiving transactions from an assisting full node creates a trade-off between privacy and performance [31]. For instance, when a client increases the false-positive rate, it will receive more transactions which can result in increased privacy [30]. However, the client will also require sufficient network capacity to download all the transactions [31]. In the end, the filter will match everything when the client downloads the full blocks or only match the client's address if the client does not have any privacy [26].

In cryptocurrencies' light clients, bloom filters can also leak more information than previously imagined [32]. For instance, when the bloom filter contains only a moderate number of addresses, an attacker could, with high probability, guess the address correctly, risking the user's privacy and security [32]. With ten addresses, for example, the probability of guessing correctly is 0.99. Even with a large number of addresses, the attacker could correctly identify the user's address with high probability if the client possesses more than one bloom filter [32]. Furthermore, resolving this issue can be challenging, because an attacker that uses additional de-anonymization heuristics can further increase their probability of guessing correctly [33]. Blockchain-based cryptocurrencies should therefore develop a solution that ensures that lightweight clients can verify that their transactions are confirmed. The verification process should also guarantee that no valid transaction is omitted.

Finally, it is essential to note that high-value assets like cryptocurrencies make high-value targets of attack. Bitcoin's security also depends on its ecosystem and its number of users [34]. Blockchain technology unlocks the potential of cryptocurrencies like Bitcoin to a broad market base while opening avenues for additional threats. Cybercriminals will generally target weak points of blockchain technology [35]. Any key feature of the technology can attract interest from intruders who wish to explore and capitalize on the weakness and launch an attack on the blockchain-enabled cryptocurrency.

IV. ANALYSIS AND COMPARISON

IoT devices have expanded at an exponential pace with the rapid expansion in networking technologies. Smart IoT devices have replaced physical credit cards and provided an easy way to order and pay for services using technologies such as Google Pay and Apple Pay that use NFC [36]. However, payment through IoT devices has faced many problems, such as security and privacy, flexibility, and scalability [37]. The introduction of blockchain-enabled cryptocurrencies has played a significant role in addressing the challenges associated with the traditional NFC payment method in IoT devices [38]. Blockchain utilizes distributed ledger technology, providing IoT solutions with greater data security and reliability.

Integrating IoT devices with blockchain cryptocurrencies has revolutionized payment methods. The combination of blockchain and IoT devices provides fair value transfer in payments for services such as electricity and water bills [39]. Another novelty of blockchain cryptocurrencies is the design of crypto-economic consensus algorithms that relax the assumption that some agents are honest and economically rational [37].

A. Combining NFC with Blockchain and Cryptocurrencies

Combining blockchain-enabled cryptocurrencies with NFC mobile payment would have significant benefits. The first benefit is increased security and privacy, which is the major hurdle that mobile payment is yet to overcome [25]. The use of cryptographic operations, hash functions and group consensus in blockchain technology would address the security and privacy concerns because it satisfies the attributes of message confidentiality, message integrity , mutual authentication, and non-repudiation of Transactions which means it can prevent scams like double-spending and spoofing, eavesdropping, and man-in-the-middle attack.

Another benefit of combining NFC with blockchain-enabled cryptocurrencies would be an improvement in instant mobile payments [22], which would lead to improved user experience and thus encourage widespread adoption. Combining these technologies is expected to make mobile payments instant and easy to use, as developers have focused on creating user-friendly apps with a faster network with which users can send money in a matter of seconds [40].

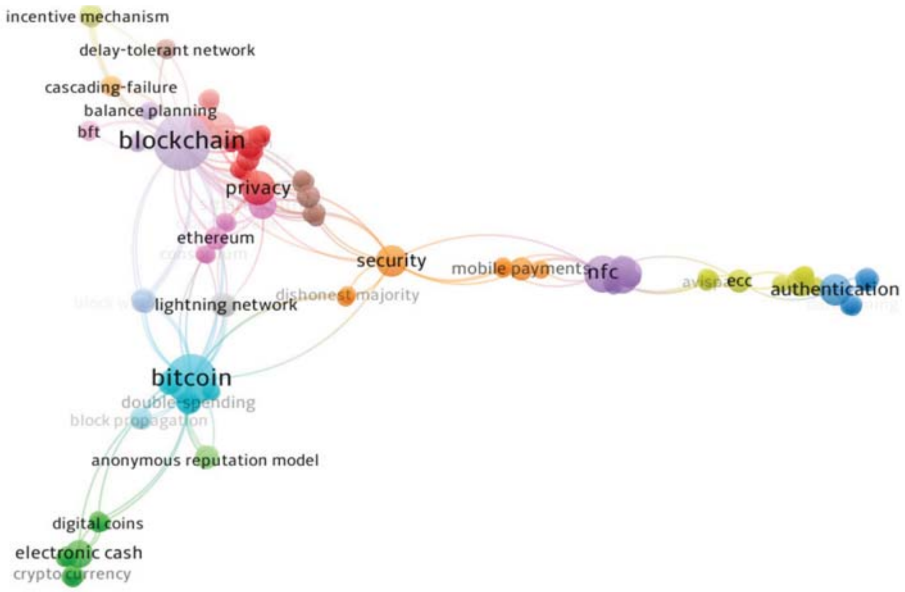

Figure 1. The relationship mapping between the keywords of studies on blockchain-based cryptocurrencies and NFC mobile payment

As well as enabling fast payments for goods and services, combining NFC, blockchain, and cryptocurrencies is also expected to improve peer-to-peer lending, which is the latest trend in the payment industry [32]. Peer-to-peer lending is expected to be strengthened by the incorporation of blockchain technology. Combining the technologies will enable borrowers to use their mobile devices to secure loans from lenders while bypassing the regulations and paperwork of traditional banking structures [30], which saves the time and money of borrowers and lenders compared to traditional loan services.

The use of blockchain-enabled cryptocurrencies in NFC payments is also expected to expand wearable and IoT devices. Mobile payment is growing beyond smartphones and tablets. Wearable devices such as bracelets, watches, and rings will also emerge in the market thanks to the use of blockchain technology [33]. Furthermore, there is an impending explosion of IoT devices. With the incorporation of blockchain technology and cryptocurrencies into NFC payment, users will be able to store payment information without having to worry about security issues [35]. The combination of these technologies will make payments easier in the future. For instance, with a wave of a hand, a smart watch will detect the translucent cryptography on products and perform a hash function, thus improving instant payment [34].

B. Challenges of Combining NFC Payment with Cryptocurrencies and Blockchain

The main challenge associated with combining NFC payment with blockchain technology and cryptocurrencies is bypassing the privacy and security concerns related to the technologies [39]. Each technology comes with its own security and privacy concerns, which must be addressed before combining them for a better payment experience [20]. For instance, most existing blockchain-based protocols have searchable encryption schemes that support only exact keyword searches between the user and the cloud server, which can be a security concern when implemented in NFC payment [37]. Cryptocurrencies have also been criticized for performance concerns, which will make it challenging to combine them with NFC to improve user experience [24]. It is therefore necessary to address all performance, privacy, and security concerns associated with blockchain technology, cryptocurrencies, and NFC mobile payment before combining them.

V. CONCLUSION AND FUTURE DIRECTIONS

This paper has provided a detailed analysis of the advance in NFC mobile payment and blockchain-based cryptocurrencies, which are expected to undergo continual and significant development. Each concept was detailed by analyzing features associated with using NFC mobile payment and blockchain-enabled cryptocurrencies.

We have selected 68 papers and approximately 200 keywords from studies related to the technical aspects of NFC mobile payment, blockchain fair payment, and cryptocurrency. The VOSviewer software was used to investigate the co-occurrence of the keywords.

From Figure 1, we can see the two central themes that emerged from the analysis were security and privacy. Given the nature of payment that involves the transfer and sharing of personal information, the security and confidentiality of this data have been a primary concern among users. Each level of technology has therefore focused on guaranteeing user privacy and protection from intruders. Only by addressing these concerns can a payment solution be considered feasible and adaptable by all users. A combination of blockchain technology, cryptocurrencies, and NFC is expected to improve the future of mobile payment, and the use of IoT devices such as smart watches will revolutionize the way users pay for products.

Therefore, there is a need for further research focusing on user experience of cryptocurrency-enabled NFC mobile payment through channels like Google Pay and Apple Pay. Further research should also focus on the security and privacy concerns users have regarding NFC payment protocols and on the impact IoT technologies have had on these payment schemes.

REFERENCES

[1] M. Badra and R. B. Badra, “A Lightweight Security Protocol for NFC-based Mobile Payments,” Procedia Computer Science, vol. 83, pp. 705 – 711, 2016.

[2] S.-W. Chen and R. Tso, “NFC-based Mobile Payment Protocol with User Anonymity,” 2016 11th Asia Joint Conference on Information Security (AsiaJCIS), 2016.

[3] K. Fan, P. Song, Z. Du, H. Zhu, H. Li, Y. Yang, X. Li, and C. Yang, “NFC Secure Payment and Verification Scheme for Mobile Payment,” Wireless Algorithms, Systems, and Applications Lecture Notes in Computer Science, pp. 116 – 125, 2016.

[4] S. Bojjagani and V. Sastry, “A secure end-to-end proximity NFC-based mobile payment protocol,” Computer Standards &amp; Interfaces, vol. 66, p. 103348, 2019.

[5] M. Cavallari, L. Adami, and F. Tornieri, “Organisational Aspects and Anatomy of an Attack on NFC/HCE Mobile Payment Systems,” Proceedings of the 17th International Conference on Enterprise Information Systems, 2015.

[6] S.-W. Park and I.-Y. Lee, “Anonymous Authentication Scheme based on NTRU for the Protection of Payment Information in NFC Mobile Environment,” Journal of Information Processing Systems, vol. 9, no. 3, pp. 461 – 476, 2013.

[7] H. Rodrigues, R. José, A. Coelho, A. Melro, M. Ferreira, J. Cunha, M. Monteiro, and C. Ribeiro, “MobiPag: Integrated Mobile Payment, Ticketing and Couponing Solution Based on NFC,” Sensors, vol. 14, no. 8, pp. 13389 – 13415, 2014.

[8] C. Thammarat and W. Kurutach, “A lightweight and secure NFC-base mobile payment protocol ensuring fair exchange based on a hybrid encryption algorithm with formal verification,” International Journal of Communication Systems, vol. 32, no. 12, 2019.

[9] X. Chen, K. Choi, and K. Chae, “A Secure and Efficient Key Authentication using Bilinear Pairing for NFC Mobile Payment Service,” Wireless Personal Communications, vol. 97, no. 1, pp. 1 – 17, 2017.

[10] P. P. Vishwakarma, A. K. Tripathy, and S. Vemuru, “A Layered Approach to Fraud Analytics for NFC-Enabled Mobile Payment System,” Distributed Computing and Internet Technology Lecture Notes in Computer Science, pp. 127 – 131, 2017.

[11] C. Thammarat, W. Kurutach, and S. Phoomvuthisarn, “A secure lightweight and fair exchange protocol for NFC mobile payment based on limited-use of session keys,” 2017 17th International Symposium on Communications and Information Technologies (ISCIT), 2017.

[12] S.-W. Park and I.-Y. Lee, “Mutual Authentication Scheme Based on GSM for NFC Mobile Payment Environments,” Advances in Computer Science and Ubiquitous Computing Lecture Notes in Electrical Engineering, pp. 391 – 395, 2015.

[13] E. Kazan, "The Innovative Capabilities of Digital Payment Platforms: A Comparative Study of Apple Pay & Google Wallet." ICMB. 2015.

[14] E. Erdin, M. Cebe, K. Akkaya, S. Solak, E. Bulut, and S. Uluagac, “A Bitcoin payment network with reduced transaction fees and confirmation times,” Computer Networks, vol. 172, p. 107098, 2020.

[15] E. Erdin, M. Cebe, K. Akkaya, E. Bulut, and A. S. Uluagac, “A Heuristic-Based Private Bitcoin Payment Network Formation Using Off-Chain Links,” 2019 IEEE International Conference on Blockchain (Blockchain), 2019.

[16] Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna, G. Jourjon, and A. Seneviratne, “A Delay-Tolerant Payment Scheme Based on the Ethereum Blockchain,” IEEE Access, vol. 7, pp. 33159 – 33172, 2019.

[17] C. Hannon and D. Jin, “Bitcoin Payment-Channels for Resource Limited IoT Devices,” Proceedings of the International Conference on Omni-Layer Intelligent Systems, 2019.

[18] S. Wang, Y. Wang, and Y. Zhang, “Blockchain-Based Fair Payment Protocol for Deduplication Cloud Storage System,” IEEE Access, vol. 7, pp. 127652 – 127668, 2019.

[19] X. Yan, X. Yuan, Q. Ye, and Y. Tang, “Blockchain-Based Searchable Encryption Scheme with Fair Payment,” IEEE Access, vol. 8, pp. 109687 – 109706, 2020.

[20] Y. Zhang, D. Yang, and G. Xue, “CheaPay: An Optimal Algorithm for Fee Minimization in Blockchain-Based Payment Channel Networks,” ICC 2019 - 2019 IEEE International Conference on Communications (ICC), 2019.

[21] M. Baza, N. Lasla, M. M. Mahmoud, G. Srivastava, and M. Abdallah, “B-Ride: Ride Sharing with Privacy-preservation, Trust and Fair Payment atop Public Blockchain,” IEEE Transactions on Network Science and Engineering, pp. 1 – 1, 2020.

[22] S. Zhang and J.-H. Lee, “Double-Spending with a Sybil Attack in the Bitcoin Decentralized Network,” IEEE Transactions on Industrial Informatics, vol. 15, no. 10, pp. 5715 – 5722, 2019.

[23] R. Yu, G. Xue, V. T. Kilari, D. Yang, and J. Tang, “CoinExpress: A Fast Payment Routing Mechanism in Blockchain-Based Payment Channel Networks,” 2018 27th International Conference on Computer Communication and Networks (ICCCN), 2018.

[24] H. Wang, Z. Yu, Y. Liu, B. Guo, L. Wang, and H. Cui, “Crowdchain: A Location Preserve Anonymous Payment System Based on Permissioned Blockchain,” 2019 IEEE International Conference on Smart Internet of Things (SmartIoT), 2019.

[25] G. Avarikioti, L. Käppeli, Y. Wang, and R. Wattenhofer, “Bitcoin Security Under Temporary Dishonest Majority,” Financial Cryptography and Data Security Lecture Notes in Computer Science, pp. 466 – 483, 2019.

[26] C. Lin, D. He, X. Huang, M. K. Khan, and K.-K. R. Choo, “DCAP: A Secure and Efficient Decentralized Conditional Anonymous Payment System Based on Blockchain,” IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2440 – 2452, 2020.

[27] B. Rainer, M. Brenner, T. Moore, and M. Smith, Financial Cryptography and Data Security FC 2014 Workshops, BITCOIN and WAHC 2014, Christ Church, Barbados, March 7, 2014, Revised Selected Papers. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014.

[28] J. Tapsell, N. A. Raja, and M. Konstantinos. "An evaluation of the security of the Bitcoin Peer-to-Peer Network." 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018.

[29] E. K. Kogias, et al. "Enhancing bitcoin security and performance with strong consistency via collective signing." 25th {usenix} security symposium ({usenix} security 16). 2016.

[30] S. Wang, C. Zhang, and Z. Su, “Detecting nondeterministic payment bugs in Ethereum smart contracts,” Proceedings of the ACM on Programming Languages, vol. 3, no. OOPSLA, pp. 1 – 29, 2019.

[31] H. Watanabe, S. Ohashi, S. Fujimura, A. Nakadaira, K. Hidaka, and J. Kishigami, “Niji: Autonomous Payment Bridge Between Bitcoin and Consortium Blockchain,” 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018.

[32] E. Androulaki, J. Camenisch, A. D. Caro, M. Dubovitskaya, K. Elkhiyaoui, and B. Tackmann, “Privacy-preserving auditable token payments in a permissioned blockchain system,” Proceedings of the 2nd ACM Conference on Advances in Financial Technologies, 2020.

[33] P. Li, T. Miyazaki, and W. Zhou, “Secure Balance Planning of Off-blockchain Payment Channel Networks,” IEEE INFOCOM 2020 - IEEE Conference on Computer Communications, 2020.

[34] J. Lind, O. Naor, I. Eyal, F. Kelbert, E. G. Sirer, and P. Pietzuch, “Teechain,” Proceedings of the 27th ACM Symposium on Operating Systems Principles, 2019.

[35] T. A. Alghamdi, I. Ali, N. Javaid, and M. Shafiq, “Secure Service Provisioning Scheme for Lightweight IoT Devices with a Fair Payment System and an Incentive Mechanism Based on Blockchain,” IEEE Access, vol. 8, pp. 1048 – 1061, 2020.

[36] S. Matetic, et al. "{BITE}: Bitcoin Lightweight Client Privacy using Trusted Execution." 28th {USENIX} Security Symposium ({USENIX} Security 19). 2019.

[37] M. Sallal, G. Owenson, and M. Adda, “Evaluation of Security and Performance of Master Node Protocol in the Bitcoin Peer-to-Peer Network,” 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2020.

[38] L. Wang, J. Gao, and X. Li. "Efficient Bitcoin Password-protected Wallet Scheme with Key-dependent Message Security." IJ Network Security 21.5 (2019): 774-784.

[39] D. Nguyen, T. Dat, and W. Ma. "A Study on Combing EEG signals and Crytography for Bitcoin security." Australian Journal of Intelligent Information Processing Systems (2019): 34.

[40] G. O. Karame, E. Androulaki, and S. Capkun, “Double-spending fast payments in bitcoin,” Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12, 2012.

[41] K. Oosthoek and C. Doerr, “From Hodl to Heist: Analysis of Cyber Security Threats to Bitcoin Exchanges,” 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2020.