Proceedings of the Third International Conference on Smart Systems and Inventive Technology (ICSSIT 2020)
IEEE Xplore Part Number: CFP20P17-ART; ISBN: 978-1-7281-5821-1

HCH DEX: A Secure Cryptocurrency e-Wallet & Exchange System with Two-way Authentication*

Mohamed Azman
Electronics and Communications Department
National Institute of Technology, Warangal
Telangana - 506004, India
mohamedazmanm1@gmail.com

Kunal Sharma
Electrical Engineering Department
National Institute of Technology, Warangal
Telangana - 506004, India
mailkunalsharma99@gmail.com

***Abstract*—Cryptocurrencies could potentially revolutionize the way our global economy functions. It presents us with enticing features that could give way to a secure and safe monetary transaction environment. Nonetheless, the present system provides a large room for improvement, and some could consider it merely a platform yet to be built upon. HCH DEX or Hot-Cold Hybrid Decentralized Exchange presents a method to locally store Cryptocurrency Wallet data in personal devices and process transactions between two personal devices without needing any common database or centralized server system to act as a broker or service provider; any licensed Local Broker can be used to facilitate a transaction in the Blockchain and register it in the distributed ledger. Additionally, the setup has been proposed that could be realized in the form of a smart card and could be designed to not be much thicker than the cards that are ubiquitous today. It is based on the conjunction of a secure two-way authentication system that enables robust handshaking mechanisms for e-Wallets and Lightweight DLT Nodes as local facilitators. It could arguably be a small step towards a fair and just economic system that is resistant to fraudulent and unethical policies and practices at different levels.**

***Index Terms*—Cryptocurrency, Cryptocurrency Wallet, e-Wallet, Smart Cards, Two-way Authentication**

I. Introduction

Cryptocurrencies bring upon a great opportunity for our global economic systems. Trading with metals such as Gold and Silver are some of the most stable, and least exploitable systems known to man, and has been in practice for thousands of years. However, their lack of convenience drove us into adopting paper currencies followed by digital currencies. At first, with them being directly linked to the value of real natural resources, it seemed like a sensible system to trade within. However, as the ecosystem matured, it brought with it a ton of loopholes, such as trading with commodities created out of thin air. Though it brings a lot of conveniences, it may be ethically questionable and may also give a platform for debatable practices that have now been normalized. Cryptocurrencies seem to potentially bring to the table some of the advantages of trading with the likes of gold and silver as well as the advantages of digital currencies. Like precious metals, cryptocurrencies need to be mined, resources have to be spent to harvest them; like precious metals, its value is directly based on its demand. They can be traded in ways that, with our present understanding, seem to be some of the finest and the most secure forms of transactions. However, before we can consider a Distributed Ledger Technology (DLT; such as Blockchains) based cryptocurrency system for mass adoption, the potentially exploitable voids cannot overlook in the system. Some miscreants have already capitalized on the weak points by hacking the system and stealing large amounts of digital assets [1]–[3]. This work is a step towards our need of studying the voids well, and making the system more robust and resilient to any such failures yet while bringing in features enabling convenience with minimal compromises.

II. Related Work

Traditional e-Wallets are based on existing card systems such as Contactless Smart Cards [4], they generally function on a client-server system and not any sort of a distributed system. Some examples would be proximity cards, which contain RFID or UID chips, that emit a unique read-only identifier. This unique identifier is used to point to a specific dataset from within the database that it refers to in a centralized server system. Other examples would be magnetic stripe cards, barcodes, QR codes, etc. In almost all applications, the card itself stores only the unique identifier, and the rest of the data is stored in the servers. Fig 1 depicts such a system with two users, User 1 and User 2. If any information is to be exchanged or manipulated between these two users, the two users with their unique identifiers are located in the database and then change in values i.e. manipulation of data, takes place within the database itself [5]. Such a system is desirable when the entire environment is under the control of a singular entity that handles the database, or at least where all nodes of the environment have direct or indirect access to that very database. In ecosystems, where there is no central system with a centralized database, the usage of these cards would be limited by the reach of the database accessibility. Having a decentralized system brings forth various advantages in terms of security, safety, and reliability of the system as a whole. More importantly, the system, over the long term leans towards being much more tamper-proof and not easily monopolized through economic malpractices.

For smart cards or e-Wallets in a decentralized system such as a DLT, an option would be to consider having more data

Supported by Aufenbach Private Limited

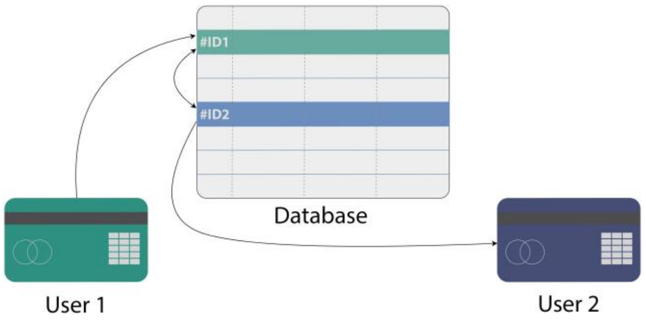

Fig. 1: Existing Systems that utilise a Common Database

on-board than just an identifier, data such as accessibility and authentication keys along with biometric verification capabilities and the like. Though this would enable immensely rugged security features, it would also require much more computational capacity especially when compared to passive units such as RFIDs/UIDs, etc. Having a fully-fledged connected computer as an e-Wallet brings a ton of possibilities, but also a ton of vulnerabilities [6], [7]. It would be best to keep it as simple and secure as possible when it comes to storing valuable commodities, and preferably with little to no backdoors. Basing an e-Wallet on an OS such as Unix/Linux would bring ease of development and interoperability between the e-Wallet and existing ecosystems. However, with it, it brings all of the exploitable vulnerabilities that come with such a large package. When it comes to realizing the product, it would be up to the product developers to choose by making appropriate compromises based on the exact use case scenarios.

Smarter credit cards have been explored and have made commendable progress in their internal technicalities. Researchers have already developed credit cards with e-ink/e-paper displays, with touch buttons, as well as with fingerprint sensors, all powered by on-board batteries lasting for years of general usage in a package not any bigger, thicker, or heavier than a normal standard credit card. Some additionally have self-destructed features when tampered with. Presently, the options available in the market allow for the user to incorporate all their cards into a single card for convenience, and select the desired card through a touch-based e-ink display; while some also use the e-ink display for one-time passwords. This shows us that the technology in terms of hardware requirements already exists as of today, and would just have to be moulded in different ways to serve the purpose of being functional in a distributed ledger environment.

In a DLT network, there may exist various types of junctions (Fig. 2) with varying abilities such as Nodes, Master Nodes, Full Nodes, Light Nodes, Archive Nodes, Pruned Nodes, Miners, etc [8]; some of them have been discussed ahead. A Full Node holds the complete copy of the entire Blockchain. A Master Node holds additional rights and features, however, not anyone can host a Master Node. Since additional rights and powers can be misused or abused, one has to deposit a collateral amount into the network to set up a Master Node. A Light Node, unlike a Full Node, does not download the complete Blockchain, it only downloads the block headers to validate the authenticity of a transaction. For this reason, they have limited functionality but are easy to maintain and run. They utilize a method called Simplified Payment Verification (SPV) to verify transactions (or any appropriate alternative [9]), which adds a lot of convenience for certain applications. Light Nodes are also known as Lightweight Nodes and are served by Full Nodes to connect to the DLT Network. Robust validation and licensing systems are necessary to avoid miscreants from exploiting Light Nodes.

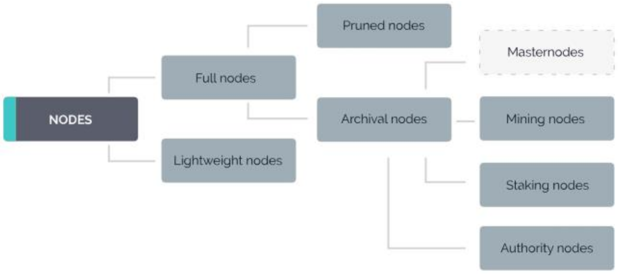

Fig. 2: Types of Nodes

Fundamentally, a Cryptocurrency Wallet or a Crypto Wallet is a tool one can use to interact with a Blockchain network. Despite what many may believe, Cryptocurrency Wallets don’t store cryptocurrencies. Instead, they behave as a sort of gateway to the Blockchain network that provides the tools necessary to communicate with the Blockchain. They possess the ability to generate and process the information needed to utilize the cryptocurrencies. The system usually creates multiple pairs of private keys and public keys along with several Blockchain addresses; it is a general practice to utilize seed phrases that precede the keys. When sending or receiving, the currency doesn’t leave the Blockchain, they are just transferred from one address to another after verification of the exchanged keys and validation from the network.

Cryptocurrency Wallets may be classified into four different types, namely:

- Exchange Wallets
- Software Wallets
- Hardware Wallets
- Paper Wallets

Depending on their working mechanism, they may also be classified into:

- Hot Wallets
- Cold Wallets

Hot Wallets are those that are in any way connected to the internet, while Cold Wallets are those that are disconnected from the internet. Exchange Wallets and Software Wallets are Hot Wallets while Hardware Wallets and Paper Wallets are

Cold Wallets. Hot Wallets come with a lot of conveniences while Cold Wallets come with better safety factors [10], [11].

In general, Exchange Wallets are the most commonly used. In this type of Crypto Wallets, the user creates an account on a digital platform managed by a service provider (also known as an Exchange). This account is generally protected by a password, a passcode, etc along with two-factor authentication systems as well as optional biometric authentication. However, the currency itself, as well as the keys required to access the currency are managed by the service provider; the Exchange creates a wallet address for the user, which the user can control through the provided interface. This can be highly convenient in terms of ease of usage, however, there are some considerations, for example, the control of the user's funds are solely based on the user's profile authentication. If the password and the like are compromised, all the funds would be vulnerable. Even if two-factor authentication is set up, it could be fairly easy for someone who knows or has access to the user to exploit the system. Additionally, the Exchanges i.e. the service providers also have in their power to freeze or hold the user's funds, hence may be undesirable as it opposes the main purpose of having a decentralized system. For this reason, Decentralized Exchanges (DEX) are being considered for deployment [12], [13], they are cryptocurrency exchanges with no central jurisdiction and allow for peer-to-peer transactions.

Software Wallets are in some ways the simplest and the easiest to access after Exchanges; they are very similar to Exchange Wallets except that they are under the user's control. They can be downloaded and installed into the user's system or browser and often have features that allow the user to directly interact with payment platforms. Like in Exchange Wallets, access is based on passwords and the like. They aren't a great deal more secure than Exchange Wallets, but the user holds more control over their funds as the wallet data is stored locally in the user's device.

Hardware Wallets, on the other hand, are completely disconnected from the internet when not in use. They usually are realized as USB based plugin devices that appear similar to USB Flash Drives. Since they are practically inaccessible offline, they offer a high factor of safety and security. The user has to physically plug the device in, and enter the passcode on the hardware to be granted access into the wallet. If the passcode is to be entered on to the hardware directly, it would ensure that keyloggers and other software tools wouldn't be able to steal the access codes and other sensitive data. Once connected, there generally exists a standard software interface that allows the user to send and receive currency. These devices are much more secure as they not only have to be physically stolen, but they will also need the passcode or any other additional authentication means such as the passwords for the software interface. Though there are a few software vulnerabilities, they are largely much safer than software-only equivalents.

Paper Wallets are simple and pretty secure, however, they lack a lot of convenience factors and hence, for the most part, are obsolete. They are similar to Hardware Wallets, in that they are completely offline. They are usually based on printed sheets of paper with public keys and private keys printed out, mostly in QR Codes that need to be scanned to be used. They usually don't have a second layer of protection and hence function much like printed currencies. One of the major drawbacks of Paper Wallets is that they can only be used to transfer a fixed amount of currency, the user can't send funds partially from the wallet, the only option is to transfer the entire balance.

Our proposed system is a hybrid of Hardware Wallets and Software Wallets (i.e. hybrid of Cold Wallets and Hot Wallets, hence the name Hot-Cold Hybrid or HCH). It possesses a smart card with an underlying communication model for the encrypted software channels, along with (Local and Decentralised) Exchange Brokers that facilitate the transactions. In other words, it's a Hardware Wallet with its own on-board basic Software interface; but since the Hardware Wallet isn't an active Node in the Blockchain, Local Brokers or Exchanges that are active Nodes in the Blockchain can be wirelessly used to facilitate the transactions. The following sections dive into the details of the system design.

III. PROPOSED SYSTEM

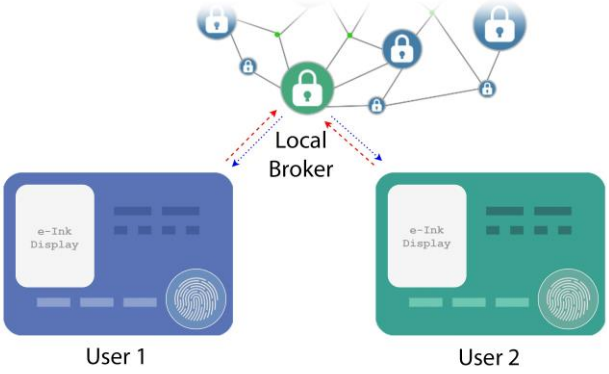

Fig. 3: Decentralised Transactions through Local Brokers

In our proposed system, each smart card unit comprises a microcontroller while each Local Broker (or Local Exchange) comprises a microprocessor. The smart card shall be realized as a traditional sized card with an onboard touch-enabled display and a fingerprint sensor; it could compose of a microcontroller with bi-directional wireless capabilities built-in, such as NFC, Wi-Fi, or a proprietary connection, along with the basic requirements such as memory units, antenna, etc. As for the display, it could have an e-ink (electronic ink) display with touch capabilities [14] for enabling on-board passcode verification, as they can be fabricated in a very slim and energy-efficient form factor. E-ink displays consume zero power when in a said state and only require power when changing from one state to another. As for biometrics,

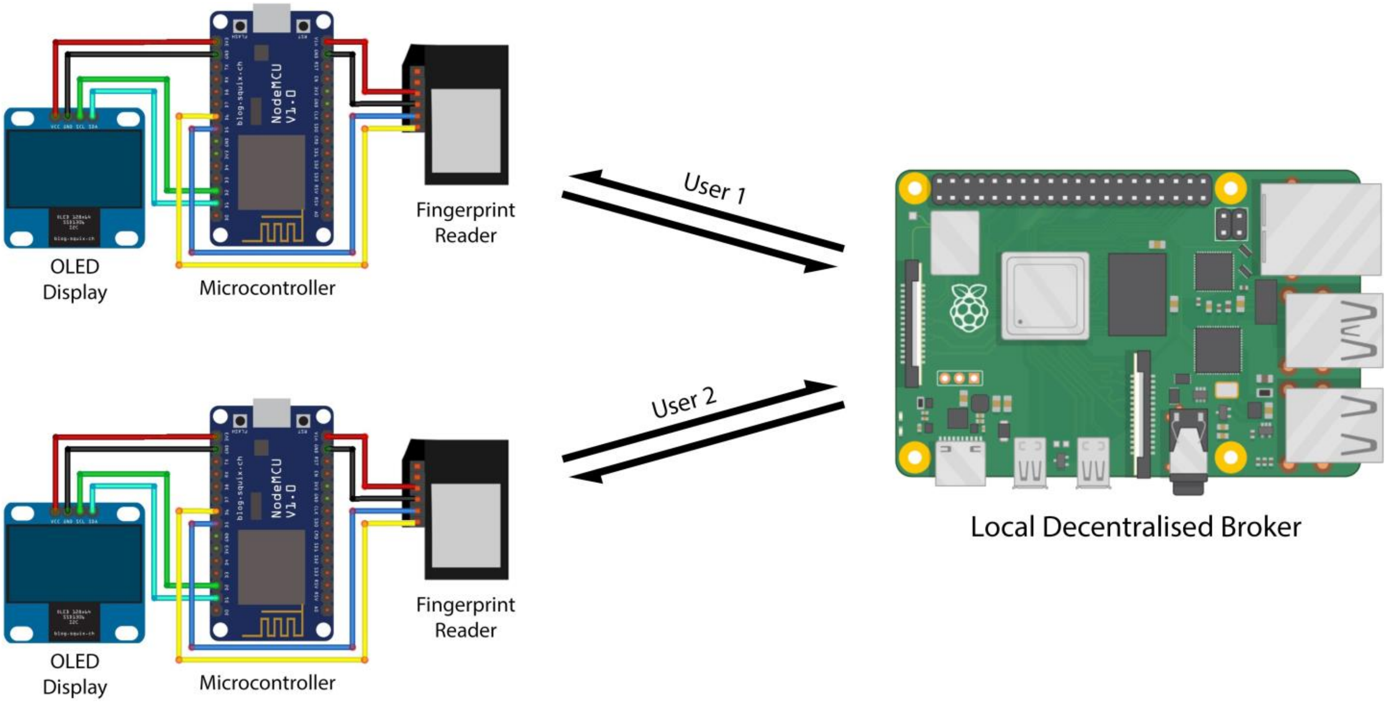

Fig. 4: Prototype Setup

capacitive fingerprint scanners [15] could be implemented in a very slim package. The device may be designed to be actively powered with wireless induction-based charging/recharging capabilities or with the help of pogo contact pins for an onboard battery; alternatively, the device may also be designed to be passively powered by the Local Brokers.

As for the Local Brokers, they may be configured as Light Nodes and realized as small licensed modules (licensed by Full Nodes) that will be actively connected to the Internet and may be placed in areas where people would generally gather, for example at restaurants, shops, malls, receptions, etc. The smart cards could wirelessly interact with the Local Brokers when the proximity requirements are met; it could be designed to be as low range as a kiosk or as long-range as covering an entire office/bank or shopping mall premises. Each microprocessor unit shall be a licensed and approved member and an active participating node in the Blockchain. It should be configured as a Lightweight node or a Light node such that it can process transactions with reasonable computing capacities and minimal delays. The smart card unit possesses the ability to communicate bi-directionally with the Local Broker (depicted in Fig 3). The two participating smart cards will exchange their encrypted keys when the users unlock their cards via fingerprints, passcodes, etc, and authenticate themselves as genuine users and legitimate stakeholders through the Local Broker. Upon authentication from both ends, each participant would be added as an active beneficiary for the other. Thereafter, a transaction can take place, whereby one smart card sends the necessary data (including public keys and Blockchain addresses) to the other smart card via the Local Broker. Further security features and authentication layers such as but not limited to channel and payload encryption may also be implemented when the smart card establishes links with the Local Broker; in such a case, the Local Broker will have to authorize each participating user.

One of the limitations of the proposed system is that it can only be used in the presence of a Local Broker, and within the defined proximity requirement. If an NFC-like wireless interface is used, the proximity requirements would be in the orders of centimeters, while if a WiFi-like wireless interface is used, it would be in the order of up to hundreds of meters. An option to be considered would be to utilize Software or Exchange-based wallets for smaller and frequent transactions and the proposed system for larger transactions; this might address the aforementioned limitation. Presently, a Blockchain transaction usually takes more time than desired. Perhaps, to further enhance the system by reducing the time (user interaction time) taken for a transaction to complete, the following proposition could be explored: Say, a transaction of a said amount has been approved between two users. The recipient user will have the amount in his/her e-Wallet, however, immediately after the transaction, the amount will have limited movement, i.e. those specific assets will be temporarily frozen. Once the Local Broker, i.e. the Light Node that facilitated the said transaction completes its Blockchain approval process through a Full Node, and the transaction is globally (over the decentralized network) marked as valid, then the said transaction is deemed fully complete. The next time the receiving (as well as the sending) e-Wallet connects to the Blockchain through any Local Broker, that transaction is locally marked fully complete, and the assets are unfrozen. However, empirical tests are yet to be carried out for the true effectiveness of such a system. There have been methods explored to tackle the Blockchain Trilemma [16]–[18], significantly reducing the transaction times; these too could be considered. The IOTA [19] team too, has made modifications to the Blockchain architecture, cutting down the total transaction time significantly; this would innately address the aforementioned limitation altogether.

IV. Prototype Design

As for the prototype, the smart card system was based on a NodeMCU ESP8266 and the Local Broker on a Raspberry Pi 4. The NodeMCU ESP8266 comes equipped with an onboard Wi-Fi chip, which was utilized to connect to the Local Broker. In place of an e-ink display, a 0.96" I2C OLED Display (SSD1306) with a resolution of 128x64 pixels was used. As for the fingerprint sensor for user authentication, the SFG R303a Fingerprint Identification Module was connected to the ESP; it has a TTL UART interface for connecting with the ESP8266. The connection setup has been shown in Fig 4. For bidirectional communication between the microcontroller and the microprocessor, MQTT protocol was utilized, along with E2E encryption [20], [21]. TLS or other forms of channel or payload encryption [22], [23] could also be considered (possibly in conjunction with each other) based on the availability of computing resources. For sending data from microcontroller to microprocessor as well as from the microprocessor to the microcontroller, a Mosquitto MQTT broker [24] was set up on the microprocessor. Based on the status of encryption, an appropriate port may be selected (1883 is the default for MQTT, 8883 is the default for MQTT over TLS i.e. Secure MQTT). The Eclipse Paho MQTT library [25] too was utilized when setting the microprocessor up. When the microprocessor needs to send data to the microcontroller, the microprocessor becomes a publisher to the MQTT broker (i.e. on the microprocessor) and the microcontroller becomes the subscriber. When the microcontroller needs to send data to the microprocessor, the microcontroller becomes the publisher to the MQTT broker (i.e. on the microprocessor) and the microprocessor becomes the subscriber.

The first user will have to unlock the device by using fingerprint authentication. Once unlocked, the user can send the Local Broker a request to pair with the second user. Once validated and authorized by the Local Broker, the request will be passed on to the second user. If the second user accepts the request, the two will be added as real-time beneficiaries of each other. Once this link has been established, the users, when active, can send and receive digital assets stored in the device memory through the Local Broker. The transaction can then be validated through the usual Blockchain transaction validation process; various schemes may be implemented to make the process speedy and instantaneous.

V. Conclusion

The paper presents a simple but powerful option whereby users can exchange digital assets such as cryptocurrencies between two e-Wallets from within personal devices, without the need for a common database, or service providers such as Banks, Exchanges, etc, furthering the decentralization of our systems. The transactions are registered in the Blockchain through a licensed Light Node acting as a Local Broker making it secure and safe. The Local Broker may be placed at any cafe, grocery, library, shop, restaurant, or, say for example, at general payment counters, etc; they could also be placed at offices, banks or dedicated exchanges.

In another embodiment, the e-Wallets could be as proposed, the Local Brokers, however, instead of being dedicated devices, could be implemented as secure applications on smartphones; this would keep the e-Wallets as cold storage units when not in use, but provide convenience when making transfers. The presented implementation is a basic proof of concept that could give way to more specific and targeted development in the desired discipline and scope. The proposed architecture may be deployed in various secure means with flexible system designs. The authors hope to see further development in this line, with a well-built ecosystem that is robust and resilient to small scale exploitation or large scale planned exploitation at any level i.e. safe from animus individuals or animus organizations, governments, etc. Further, the edge devices too need to be improved and designed such that they are holistically pushing us forward, and not such that they address some problems while opening doors for many more.

References

[1] Statista, "Value of cryptocurrency theft worldwide from 2016 to 2018," https://www.statista.com/statistics/960226/theft-of-cryptocurrency-value/, July 2019.

[2] M. Guri, "Beatcoin: Leaking private keys from air-gapped cryptocurrency wallets," in *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)*, July 2018, pp. 1308–1316.

[3] C. Evans-Pughe, A. Novikov, and V. Vitaliev, "To bit or not to bit?" *Engineering Technology*, vol. 9, no. 4, pp. 82–85, May 2014.

[4] C. Wright, "Smart-card-based mobile wallets," https://medium.com/swlh/smart-card-based-mobile-wallets-9cb75595b71d, Jan 2019.

[5] V. Kalaichelvi, "Smart card technology in some studies on protocols and their implementation for secured electronic voting system (anna university)," Aug 2014.

[6] K. Singh, N. Singh, and D. Singh Kushwaha, "An interoperable and secure e-wallet architecture based on digital ledger technology using blockchain," in *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, Sep. 2018, pp. 165–169.

[7] C. H. Fancher, "In your pocket: Smartcards," Jan 1999.

[8] T. Burke, "The essential diversity of blockchain nodes," Dec 2018.

[9] A. Palai, M. Vora, and A. Shah, "Empowering light nodes in blockchains with block summarization," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2018, pp. 1–5.

[10] M. Rahouti, K. Xiong, and N. Ghani, "Bitcoin concepts, threats, and machine-learning security solutions," *IEEE Access*, vol. 6, pp. 67 189–67 205, 2018.

[11] A. G. Khan, A. H. Zahid, M. Hussain, and U. Riaz, "Security of cryptocurrency using hardware wallet and qr code," in *2019 International Conference on Innovative Computing (ICIC)*, 2019, pp. 1–10.

[12] R. Bhutoria, "Decentralized exchange (dex) sector report," https://medium.com/circle-research/decentralized-exchange-dex-sector-report-8077f5d0120e, December 2018.

[13] TokenInsight, "Mainstream transaction pairs are scarce, and transaction efficiency and depth are poor-2019 research report on decentralized exchanges shows," https://medium.com/tokeninsight-offcial/2019-research-report-on-decentralized-exchanges-shows-ea458feda3c2, June 2019.

[14] "E ink displays," https://en.wikipedia.org/wiki/EInk.

[15] "Emv card with fingerprint biometrics - introducing the biometric payment card," https://www.gemalto.com/financial/cards/emv-biometric-card.

[16] K. Qin and A. Gervais, "An overview of blockchain scalability, interoperability and sustainability."

[17] S. Viswanathan and A. Shah, "The scalability trilemma in blockchain."

[18] CertiK, "The blockchain trilemma: Decentralized, scalable, and secure?"

[19] J. Cech, "Release strategy for chrysalis (iota 1.5)," https://blog.iota.org/release-strategy-for-chrysalis-iota-1-5-4ea8741ea3a1, May 2020.

[20] F. S. Chowdhury, A. Istiaque, A. Mahmud, and M. Miskat, "An implementation of a lightweight end-to-end secured communication system for patient monitoring system," in *2018 Emerging Trends in Electronic Devices and Computational Techniques (EDCT)*, March 2018, pp. 1–5.

[21] O. Sadio, I. Ngom, and C. Lishou, "Lightweight security scheme for mqtt/mqtt-sn protocol," in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, Oct 2019, pp. 119–123.

[22] R. Siva, "Iot-mqtt payload encryption at the application layer," https://medium.com/@renugopal17.siva/iot-mqtt-payload-encryption-at-the-application-layer-58f8957d4b5f, Nov 2018.

[23] "Securing mqtt systems - mqtt security fundamentals," https://www.hivemq.com/blog/mqtt-security-fundamentals-payload-encryption/, Jun 2015.

[24] "Eclipse mosquitto™ an open source mqtt broker," https://mosquitto.org/.

[25] "Eclipse paho," https://www.eclipse.org/paho/.