applied sciences

MDPI

*Review*

# Review of Offline Payment Function of CBDC Considering Security Requirements

**Yeonouk Chu [1], Jaeho Lee [1], Sungjoong Kim [1,*], Hyunjoong Kim [1], Yongtae Yoon [1] and Hyeyoung Chung [2]**

[1] Electric Power Network Economics Laboratory, Department of Electrical and Computer Engineering, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul 08826, Korea; yeonouk1@snu.ac.kr (Y.C.); lee8808@snu.ac.kr (J.L.); joyfulkkachi@snu.ac.kr (H.K.); ytyoon@snu.ac.kr (Y.Y.)

[2] Department of Electronic Engineering, Hanyang University, 222 Wangsimni-ro, Seongdong-gu, Seoul 04763, Korea; hy2315@hanyang.ac.kr

* Correspondence: gianthips@snu.ac.kr

**Abstract:** Due to the growth of the internet and communication technologies, electronic financial systems are becoming popular. Physical cash is losing its preeminence, and digital numbers on computers represent money. However, electronic financial systems, mostly operated by private entities, have defects to be compensated for, such as high charges for using the system, security issues, and the problem of exclusion. As a solution, many countries around the world are considering central bank digital currency. For central bank digital currency to be utilized as a national legal tender, it must be universal and accessible regardless of time and place, similar to physical cash. Therefore, offline payment functions that extend the accessibility of central bank digital currency are becoming attractive. However, due to the characteristics of the electronic financial system, central bank digital currency is vulnerable to possible malicious behaviors in offline situations, such as blackouts and system shutdowns. This paper reviews research studies that deal with security matters related to the offline payment function of central bank digital currency. Offline payment solutions, including central bank digital currency and other electronic financial systems, such as electronic cash and cryptocurrency, are reviewed, and supplemental methods to improve the offline payment solutions of central bank digital currency based on trusted execution environment devices are suggested.

**Keywords:** central bank digital currency (CBDC); offline payment function; security requirements; blockchain; electronic financial systems; trusted execution environment (TEE)



**Citation:** Chu, Y.; Lee, J.; Kim, S.; Kim, H.; Yoon, Y.; Chung, H. Review of Offline Payment Function of CBDC Considering Security Requirements. *Appl. Sci.* **2022**, *12*, 4488. https://doi.org/10.3390/app12094488

Academic Editor: Roberto Saia

Received: 2 February 2022
Accepted: 26 April 2022
Published: 28 April 2022



## 1. Introduction

### *1.1. Central Bank Digital Currency*

Physical cash, paper notes, and coins have been the key medium of exchange in conventional financial systems for a long time [1]. However, in the last few decades, due to the growth of the internet and communication technologies, physical cash has been losing its preeminence [1]. Electronic financial systems have become widespread, with digital numbers on computers representing money rather than physical cash. It is a well-known fact that monetary policies, such as the open market operation, quantitative easing (QE), or quantitative tightening (QT), are executed not by printing or collecting paper notes but by using electronic funds created with keystrokes on computers [2,3].

The changes can be seen more easily in the retail sector. Technological advances are deregulating the financial industry, and many people have already become used to various payment methods operated by various entities, such as credit cards, online banking services, mobile payments, etc. [1,4,5]. Some countries are already at the stage of a so-called "cashless society" [6]. In 2016, the share of cash used for all payments in South Korea was only 14%; in China, 18%; and in the UK, 24%. The share of cash used in the United States in 2020 was 19% [7–9].

Electronic financial systems are considered to have advantages compared to conventional financial systems mainly for two reasons. First, electronic financial systems are considered to be more transparent than conventional financial systems. Unlike conventional financial systems based on physical cash, which has the characteristic of anonymity, in electronic financial systems, transactions between users can be watched and logged. Therefore, malicious users and unlawful acts can be traced and detected. Second, electronic financial systems can enable flexible and easy use of money and help vitalize the economy. In countries where electronic financial systems are in use, people can use bank services and join in e-commerce anytime and anywhere they want, as the digital currency used in the systems is free from physical constraints. This could increase the amount of currency in circulation and contribute to economic stabilization [10].

Even with these advantages, electronic financial systems still have some defects to be compensated for. First, electronic financial systems usually have charges for using the system, resulting in an additional cost to use money or currency [11]. For example, credit card networks routinely charge card fees of 3% [11]. E-wallet (electronic wallet) services managed by Sticpay charge 1~3.85% of deposit fees [12]. Such high charges can attenuate economic activity and commerce [11]. Second, without proper security policies, personal data breaches can occur in electronic financial systems. Electronic financial systems are vulnerable to digital attacks by their nature. Access to the systems via the internet, or any other possible measures, is open to anonymous users at all times. Further, when personal data breaches occur, the quantity of data breached at once could be large. In 2019, when Capital One, the fifth largest credit card issuer in the United States, was hacked, the personal data of 106 million customers were leaked [13]. In 2014, the user information of at least 20 million people was leaked in Korea, a country of 50 million [14]. Third, in electronic financial systems, the problem of financial exclusion, which refers to individuals and populations without access to common financial services, can occur. For instance, China is a country where electronic financial systems such as Alipay and Wechat are widely used. However, China's rural and farm communities use internet technologies only half as much as all users, and less than 2% access credit through the internet [15]. Additionally, many commercial electronic financial systems are closed to people with low credit ratings [16].

As a solution to these problems, many countries are considering central bank digital currency (CBDC). The International Monetary Fund (IMF) defined CBDC as a digital representation of a sovereign currency issued by and a liability of a jurisdiction's central bank or other monetary authority [17]. Under the CBDC system, the central bank directly manages the whole currency circulation, which is the biggest difference from the current electronic financial systems operated by various commercial entities and brings many advantages. First, the central bank's intervention in the payment system will minimize many steps in money circulation and promote competition between entities operating the electronic financial systems. As JP Morgan predicted, this could save charges for the system use that are spent in the present electronic financial systems [18]. Second, users will not need to use various commercial payment systems, and thus, the possibility of personal data breaches will be reduced. Unlike electronic financial systems that leave data trails through a number of commercial entities, under the CBDC system, the central bank directly manages personal data [19]. Third, the CBDC system can solve the problem of financial exclusion. Unlike electronic financial systems that do not provide financial services to unbanked people, estimated to be almost 1.7 billion people worldwide, under the CBDC system, CBDCs can be directly provided to users without using traditional bank accounts [20,21]. Blockchain technology is regarded as the option that can strengthen the merits of the CBDC system, as it is based on distributed ledger technology (DLT), which does not need intermediaries and is well known for its strong security.

### *1.2. Countries Developing CBDCs and Types of CBDCs*

Numerous countries are developing CBDCs through pilot projects, and some of those countries have already introduced them as the national legal tender. Sweden is one of

the countries currently considering adopting CBDC, E-krona, to decrease dependence on foreign electronic financial systems, such as Visa and Mastercard. The cash in circulation has fallen to 1% of its gross domestic product (GDP) [22–25]. Uruguay is also considering introducing CBDC, E-peso, to overcome the underdeveloped infrastructure issue in electronic financial systems [26,27]. The Bahamas is one of the countries that have already adopted CBDC. In 2020, the government of the Bahamas introduced the Sand Dollar, and it boosted digital transactions between people using smartphones, regardless of the existing electronic financial systems [28]. The Republic of the Marshall Islands, where the US dollar has been the public currency, issued a CBDC named Sovereign (SOV) to reduce the dependence on the US dollar and activate cross-border transactions [29,30]. China introduced the world's largest CBDC system, E-CNY (digital yuan). To date, the number of digital yuan wallets exceeds 123 million, and the accumulated amount of E-CNY used in transactions is almost CNY 56 billion [31]. The Cambodian government and the Nigerian government also introduced CBDCs named Bakong and E-Naira.

The CBDC systems that various countries are testing or already using take various forms depending on the purpose and can be classified according to three criteria [26]. First, the CBDC systems can be classified into the single-ledger-based system and the distributed-ledger-based system, according to the number of entities that manage the ledgers. Under the single-ledger-based system, it is the central authority, such as the central bank alone, which manages the ledger, and the central organization can manage the whole financial system with a uniform standard. However, this type of CBDC system can become vulnerable if the central authority is accidentally or maliciously shut down [32]. Under the distributed-ledger-based CBDC system, a concept opposite to the single-ledger-based system, transaction records are consensually shared and synchronized through a ledger that multiple entities can access [33]. The distributed-ledger-based system provides transparency by sharing the authority of managing among multiple entities and helps reduce the possibility of a concentrated digital attack through the distributed structure [34]. Second, the CBDC systems can be classified into the permissioned system and the permissionless system depending on whether only authorized entities can access the ledger or not. The permissioned CBDC system is based on a distributed ledger that is not publicly accessible. In this system, only users authenticated through certificates or other digital means can access the ledger and perform specific actions approved by the managing authority [35]. The permissionless CBDC system refers to a CBDC in which all entities can use the system without special permission. The permissioned CBDC system is regarded as faster and more efficient than permissionless CBDC but is not transparent and not helpful in solving the problems of financial exclusion [36]. Third, depending on whether the central bank directly provides financial services, the CBDC systems can be classified into the direct CBDC system and the indirect CBDC system. In the direct CBDC system, the central bank provides financial services to users, and all transaction records are managed by the central bank. On the other hand, under the indirect CBDC system, the central bank delegates the managing authority of financial systems to intermediaries, and the central bank only manages the intermediaries [37]. The various forms of CBDCs mentioned so far are expressed in Figure 1, and following the classification criteria, the CBDC systems currently in operation are categorized in Figure 1 and Table 1.

### *1.3. Importance of the Offline Payment Function of CBDCs and Security Requirements*

Regardless of type, all CBDCs have one important feature in common—CBDCs are the national currency that is to be used as legal tender replacing the physical cash. Like cash, it should be accepted irrespective of all circumstances. However, the CBDC system is basically an electronic financial system where users are required to be connected to the internet, and for this reason, so far, CBDCs have not truly worked as a national legal tender.

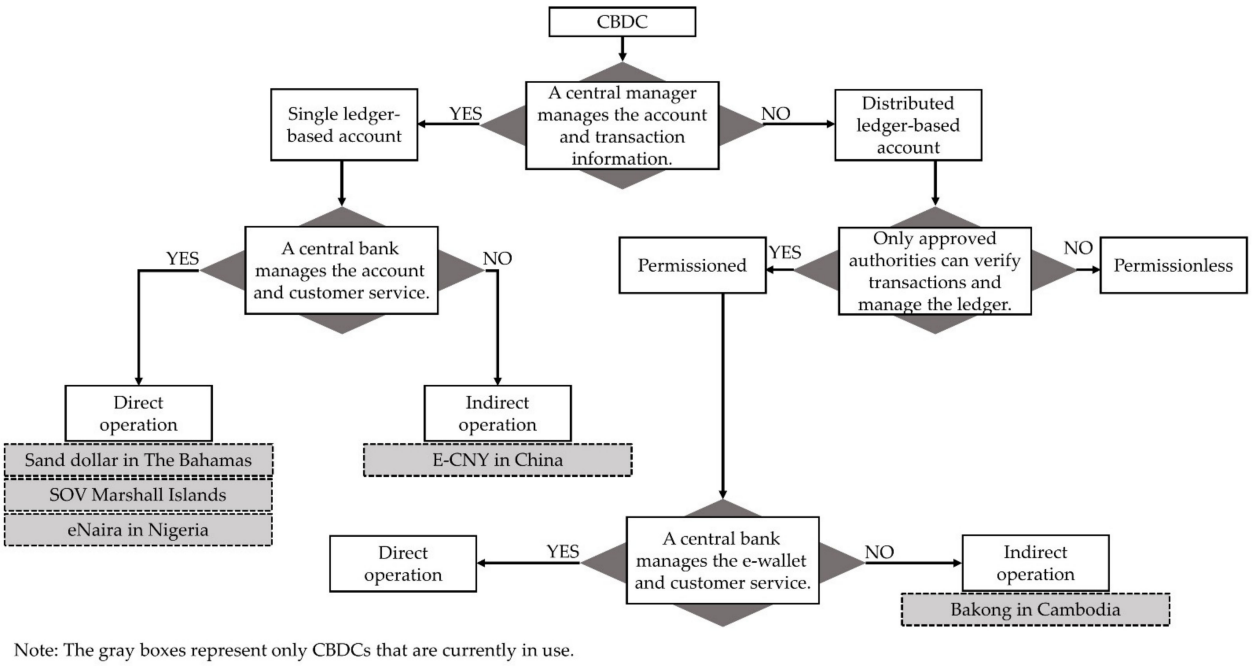


**Figure 1.** Different forms of the CBDC systems (classification standards from Ref [26]).

**Table 1.** CBDCs in use worldwide.

| CBDCs in Use Worldwide | Types | Reasons |
|---|---|---|
| Sand Dollar (The Bahamas) | Single ledger | No external organizations are involved in managing the ledger. |
| | Direct | The central bank provides financial services directly. |
| SOV (Republic of the Marshall Islands) | Single ledger | No external organizations are involved in managing the ledger. |
| | Direct | The central bank provides financial services directly. |
| eNaira (Nigeria) | Single ledger | The central bank directly manages the ledger. |
| | Direct | The central bank provides financial services directly. |
| E-CNY (China) | Single ledger | The central bank directly manages the ledger. |
| | Indirect | Commercial and private banks are designated as operating institutions to provide financial services. |
| Bakong (Cambodia) | Distributed ledger | Operated using the Iroha blockchain, which is based on Hyperledger. |
| | Permissioned | Iroha uses a permissioned blockchain. |
| | Indirect | Various digital banks provide financial services. |

CBDCs, which can be used only with the internet, can exclude many people who cannot use the internet from financial services. Further, if the system is shut down due to power outages and cyberattacks, financial services could turn out to be unavailable, which could cause a lot of confusion. Therefore, China and the Bahamas, where the CBDC system is already introduced, are reviewing the offline payment function of CBDCs, and the number of countries that are considering the offline payment function of CBDCs is expected to increase in the future [38].

The offline payment function of electronic financial systems is defined as a transaction function that does not require internet or telecom connectivity [39]. Under the electronic financial system with an offline payment function, people can use digital money stored in portable devices regardless of the communication environment, and therefore, the problems of financial exclusion or system malfunction, mentioned previously, are expected to be

solved. However, the electronic financial system with an offline payment function is in a blind spot of security problems—not only portable devices but also transactions in an offline situation are isolated from the main system. Malicious behaviors, such as hacking attempts on portable devices or fraudulent transactions that exploit the system, cannot be detected in real time.

### 1.4. Methodology and Limitation

The security problem of the offline payment function may act as an obstacle to elevating CBDCs as the national legal tender that can be used regardless of all circumstances. In this respect, this paper focuses on reviewing security requirements for offline payment functions to utilize CBDC as a national legal tender, based on research studies considering various electronic financial systems, which are predecessors of CBDC.

In Section 2, security requirements that should be fulfilled by electronic financial systems are defined, and solutions for security requirements are reviewed. Research studies dealing with the security requirements of offline payment functions as well as online payment functions of electronic financial systems were examined, considering the CBDC's character as a national legal tender. To utilize the CBDC system as a national legal tender, it is obvious that a thorough discussion on its security matters is needed. However, studies on the offline payment function of electronic financial systems tend to rely on one method, cryptographic techniques, by which the security requirements that can be fulfilled are limited, unlike various studies related to the online payment function, which are suggesting various security enhancement methods. Therefore, in this section, the scope of the review is extended to diversify the security requirements and find various solutions.

In Sections 3 and 4, studies related to the offline payment function of electronic financial systems are reviewed while examining whether the security enhancement methods suggested by these studies meet the security requirements examined in Section 2. In particular, studies dealing with not only the CBDC system but also the electronic cash (e-cash) and the cryptocurrency among electronic financial systems, were selected, since the CBDC system can be largely divided into a single-ledger-based system and distributed-ledger-based system, as covered in Section 1.2. In terms of system operation, e-cash, which is usually operated by a single entity, such as a bank or a credit card company, has similarities to single-ledger-based CBDC, and a cryptocurrency based on blockchain technology has similarities to distributed-ledger-based CBDC. Therefore, research related to the security matters of each electronic financial system can be referred to in dealing with security matters of the CBDC system.

Finally, Section 5 reviews the limitations that the solutions in the previous research study on CBDC regarding offline payment function have. In the previous research study on the offline payment function of the CBDC system, security enhancement solutions that utilize electronic devices equipped with the trusted execution environment (TEE) technique are suggested. Since those solutions have weak spots for DDoS attacks and counterfeit, improvement methods for the solutions are proposed, while still unresolved fundamental problems and countermeasures are emphasized.

The major research questions discussed in each section can be summarized as follows:

- What are the security requirements that the offline payment function of electronic financial systems should meet?
- What are the methods that can be applied to electronic financial systems to meet the security requirements?
- How well do the methods proposed in the research studies of offline payment functions of electronic financial systems meet the security requirements?
- What solutions can be suggested for improving TEE-based methods for the offline payment functions of electronic financial systems?

To figure out the research questions above while reviewing research studies, four different search engines were utilized, namely, Google Scholar (https://scholar.goo-gle.co.kr/, accessed on 11 April 2022), IEEE Xplore (https://ieeexplore.ieee.org/Xplore/home.jsp,

accessed on 11 April 2022), Elsevier (https://w-ww.sciencedirect.com/, accessed on 11 April 2022), and Springer (https://link.springer.com/, accessed on 11 April 2022). Google Scholar was used in comprehensive searching of journals, while IEEE Xplore, Elsevier, and Springer were used in advanced searching of specific topics in engineering, such as blockchain technologies, protocols, data security, and cryptology techniques. On the other hand, discussions on various electronic financial systems, including CBDC and cryptocurrency, can be found not only in research studies in the engineering and technology field but also in gray literature and research studies in the financial field, such as news, company reports, government reports, and white papers. In searching the literature, the websites used were as follows: Investopedia (https://www.investopedia.com/, accessed on 11 April 2022), Experian (https://www.experian.com/, accessed on 11 April 2022), Insider (https://www.insider.com/, accessed on 11 April 2022) and Ledger Insights (https://www.ledgerinsights.com/, accessed on 11 April 2022), and central banks' country websites.

In searching the literature through the websites mentioned above, the search keywords were selected based on the first, second, and third research questions. The keywords "electronic cash", "digital cash", "digital currency", "electronic financial systems", and "security requirements" were mainly used for the first research question, and six keywords about security requirements were found by using these keywords: No double spending, Unforgeability, Non-repudiation, Verifiability, Anonymity, and DDoS attack prevention. The combination of these six security requirements and keywords "electronic/digital currency", "e-cash", "cryptocurrency", and "CBDC" were mainly used for the second research question. The keywords "electronic/digital currency", "e-cash", "cryptocurrency", "CBDC", and "offline payment" were mainly used for the third research question.

Despite efforts to answer research questions based on the mentioned methodology, this study has some limitations. First, as countries do not disclose the specific realization methods of their CBDC systems, considering the importance of the CBDC systems as national legal tenders, the security measures of the offline payment function of the CBDC systems in use could not be reviewed. Second, this study focused on reviewing existing research studies related to the security issues of the offline payment function of CBDCs. The implementation of the offline payment function will be carried out in later research based on the review conducted in this study.

## 2. Security Requirements for CBDC and Digital Currencies

Han et al. [40] defined the six security requirements that CBDC should satisfy as no double spending, unforgeability, non-repudiation, verifiability, and anonymity. As mentioned, in examining these security requirements, we considered research studies on other forms of digital currency, such as e-cash and cryptocurrencies, which are the predecessors of CBDC, as CBDC is a research topic that not many studies have dealt with, given its importance.

### *2.1. No Double Spending*

Chohan [41] defines the problem of double spending as follows: "…A potential flaw in cryptocurrency or other digital cash schemes whereby the same single digital token can be spent more than once…". The double-spending issue has been considered to be the major obstacle that disturbs the propagation of e-cash. Brands [42] reviewed the methods of blind signatures and wallets with observers that can be used in securing the traceability of e-cash transactions. Brands stated that a restrictive blind signature method satisfies strict but efficient privacy requirements for the observer by using a tamper-resistant smart card. Krsul et al. [43] provided a solution for the double-spending issues in offline transactions by allowing the service providers to supply tokens with the same serial number to the buyer and the seller and allow transactions only between members with matching tokens. Pointcheval and Stern [44] suggested a blind Rivest–Shamir–Adleman (RSA) signature and cut-and-choose method for recipients, since preventing the emergence of malicious e-cash double spenders is fundamentally impossible.

Even in cryptocurrency, the problem of double spending can occur. Savolainen and Soria [45] describe the steps of double-spending issues in cryptocurrency as follows:

**Step 1.** The attacker purchases products/services using a cryptocurrency;
**Step 2.** The seller checks whether the attacker's purchase in **Step 1** is in the main blockchain and waits for other confirmation blocks to be added to the main chain blockchain that contains the record of the purchase in **Step 1**;
**Step 3.** In the meantime, while avoiding the seller's eyes, the attacker processes mining in a fake chain; the transaction in **Step 1** is not included;
**Step 4.** If the process in **Step 2** is completed, the seller sends the attacker products/services;
**Step 5.** After receiving products/services, the attacker secretly continues mining and lengthens the fake chain in **Step 3** to be longer than the main chain;
**Step 6.** As the longest chain is adopted as the main chain, miners will accept the fake chain that the attacker created as the new main chain, and the future proof of work will be conducted based on the new main chain;
**Step 7.** Since the new main chain does not include the record of the purchase in **Step 1**, the attacker can use the cryptocurrency used in **Step 1** again.

In cryptocurrency, double-spending issues have not occurred frequently, since, due to the decentralized characteristics of the cryptocurrency, it is not easy for attackers to possess a hashing power of more than than 50% and make the fake main chain. Further, the mechanism of proof of work, which is the key structure of cryptocurrency, requires users to make a not insignificant but feasible amount of effort in making blocks, also preventing the possibility of double spending [45]. However, the proof-of-work mechanism has been considered to be unsuitable for fast payments [46]. Therefore, as possible measures for the vulnerability of proof of work, Karame et al. [46] suggested the method of inserting observers during the transactions. The other alternative mechanism that can prevent the double-spending issue is the proof-of-stake mechanism, which is the method of allowing entities with high coin stakes to be involved in the processes of decision making. Procuring coin stakes of more than 50% of all issued coins is regarded to be more difficult than procuring the hashing power greater than 50% [47].

Regarding the CBDCs, Ref [48] dealt with the problem of double spending and proposed two solutions for it: first, setting up one or more trusted central parties that keep ownership records of CBDCs on the ledger, which is suitable for the single-ledger-based CBDCs in Figure 1; second, using DLT, which is suitable for the distributed-ledger-based CBDCs in Figure 1. What the two solutions in Ref [48] have in common is that each aims to reduce the burden on the central bank by handling the double-spending issue using the remote ledger.

### *2.2. Unforgeability*

For the currency to be utilized as a legal tender, it should be invulnerable from any malicious counterfeiting attempts. Many countries have implemented verification mechanisms based on a hologram to prevent possible counterfeits of the physical currency.

To use digital currency as physical cash, the same standard should be applied. Okamoto and Ohta [49] and Franklin and Yung [50] stated that the unforgeability of the systems must be guaranteed to introduce e-cash systems. Lockett [51] asserted the necessity of the criminal justice system to be able to prevent counterfeiting attempts with e-cash. The audit trail that is generated in the process of using e-cash can be regarded as a valuable source that guarantees the unforgeability of e-cash. However, the e-cash system is regarded as being more vulnerable to counterfeits than physical currency because the audit trail itself is imperfect, can be forged, and has operational risks [52]. Nevertheless, Shaoib et al. [53] pointed out that, in countries that lack administrative power, e-cash, with proper, well-designed algorithms detecting counterfeits, would be a better legal tender than physical currency. The same arguments can be found in some countries today that are considering the introduction of CBDC to solve the counterfeit money problem.

McKinney et al. [54] state that cryptocurrencies could easily be counterfeited compared to hard currencies. Therefore, several countries are attempting to limit the circulation of forged cryptocurrencies through legislation [54]. Crosby et al. [55] mentioned the third-party-dependent anticounterfeiting mechanism, which some research studies have suggested is not implementing the philosophy of decentralization and presented the BlockVerify method, which provides transparency to the supply chain by using distributed ledgers. Velde [56] suggested that the counterfeit issues of digital currency could be solved if Bitcoin is used, and its proof-of-work mechanism is applied.

Regarding the CBDCs, Armelius et al. [48] defined the counterfeit problem as the malicious creation of serial numbers of tokens that did not exist before and suggested a detection solution based on local devices by assigning encryption keys to each CBDC token. By letting the local device where CBDC tokens are stored check the key by the decryption technology, the counterfeit tokens can be easily detected [48].

### *2.3. Non-Repudiation*

Repudiation occurs when the entity that received the digital currency maliciously insists that they did not receive it or that the digital currency they received is fake. McCullagh and Caelli [57] stated the conditions in which repudiation could occur.

- The entity that received the digital currency insists that the signature on the digital currency is a forgery;
- The signature is not a forgery, but the entity that received the digital currency insists that the cash was obtained via:
    i. Unconscionable conduct during transactions;
    ii. Fraud instigated by a third party;
    iii. The undue influence exerted by a third party.

McCullagh and Caelli [57] specified the requirements to prevent issues of repudiation in cryptocurrency as follows:

- A service that provides proof of the integrity and origin of data, both in an unforgeable relationship, which any third party can verify at any time during the authentication process;
- An authentication with high assurance that cannot subsequently be refuted.

Research studies on computer networks, such as Coffey and Saidha [58], Zhou and Gollmann [59], Zhang and Shi [60], and Kremer et al. [61], focused on the non-repudiation protocol. Specifically, Kremer et al. [61] proposed the following requirements for fair non-repudiation protocol (FNRP):

- FNRP should provide the payer non-repudiation of receipt to verify the transaction from the Adjudicator;
- FNRP should provide the payee non-repudiation of origin to verify the transaction from the Adjudicator;
- When FNRP ends, the transaction parties should obtain both non-repudiation of receipt and non-repudiation of origin (all together, the non-repudiation evidence, NRE). If the receipt and origin evidence are not obtained, the transaction can be seen as problematic;
- FNRP with the trusted third party (TTP) must individually create an NRE regardless of TTP involvement;
- FNRP that does not use the trusted third party (TTP) should present fairness probabilistically;
- FNRP can be terminated by the transaction parties who have confirmed that FNRP has secured fairness after a reasonable period.

Cryptocurrencies cut off the possibility of repudiation by keeping the transaction data in each block in the blockchain. Specifically, due to the base logic that the longest block is selected as the main chain and more than 50% of hashing power or stakes is needed to create the fake chain, the possible repudiating attempts by substituting the existing main

chain for the fake one can rarely occur. According to Nakamoto [62], in the Bitcoin system, when 10 new blocks are added to the current main chain, the possibility of deleting the existing block by an attacker even with 10% of the mining power is only 0.0000012%. In addition, the Ethereum system prevents the possibility of repudiation by using the hash function Keccak-256 to perform the message digest for the data logged in each block and writing the hash value to the block at the same time. According to IBM, a message digest is defined as a fixed-size numeric representation of the contents of a message, computed by a hash function [63]. According to Robinson [64], an attacker needs the value of the reversed Keccak-256 function to maliciously alter the contents in the block with a hash value, but realistically, it is impossible.

Regarding CBDCs, not many discussions have been had regarding non-repudiation. According to Minwalla [65], the CBDC based on DLT in which only approved authorities are allowed to verify transactions and manage the ledger, the so-called permissioned CBDCs in Figure 1, was regarded as a solution for the repudiation problem, as approved authorities can provide a non-repudiation policy [65]. However, the permissioned CBDCs are vulnerable to the manipulation of the blockchain. Therefore, to use the permissioned CBDCs as a solution for non-repudiation, additional security safeguards that prevent manipulation of the blockchain are needed [65].

### 2.4. Verifiability

To detect and penalize any malicious acts that evade the security protocols, the electronic financial system should be verifiable—the transactions must be recorded, and the records must not be falsified.

Payeras-Capellà et al. [66] and Seo and Kim [67] researched the verifiability of the protocols for e-cash systems. Payeras-Capellà et al. [66] propose a fair electronic protocol that uses the trusted third party (TTP) to check irrelevant actions within the transaction. Seo and Kim [67] reviewed the functions of an electronic funds transfer (EFT) protocol, which transfers money from bank accounts to other agencies through a computer system without the direct intervention of bank staff, and proposed a domain-verifiable signcryption scheme as an improvement of the EFT protocol. The scheme appoints pre-specified participants to check the transactions, allowing the protocol to have verifiability in the absence of TTP [67].

Cryptocurrencies such as Bitcoin and Ethereum are verifiable, as all the transactions are recorded in blocks [68]. Sánchez [69] proposes the Raziel system, which combines the multi-party computation (MPC) protocol and zero-knowledge proofs (ZKP). The MPC is a protocol in which individuals that do not trust each other do not share their input value, such as personal information, but share the encoded input value. The ZKP is a process in which code users can verify codes without opening information on the smart contracts. The Raziel system, which utilizes the benefits of both methods, has an advantage in verifying the smart contract without revealing personal information [68].

Like cryptocurrencies based on DLT, CBDCs that use DLT satisfy the verifiability condition. However, not all CBDCs can be said to be based on DLT—some CBDCs, such as the permissioned CBDCs mentioned in Figure 1, only allow approved authorities to verify transactions and manage the ledger, and those CBDCs do not have the same verifiability standards as cryptocurrencies [70]. Therefore, Ripjar [70] suggested that the CBDC systems use the know your customer (KYC) process as a verifiability measure. The CBDC system can accomplish the verifiability through the KYC process, which only allows verified users to use the CBDC system by ex-ante identification process and keeping the transaction history among them.

### 2.5. Anonymity

Cash transactions leave no trace of users. Such a characteristic is good for protecting a person's privacy but could be exploited for crimes such as tax evasion, causing negative externality in society [71]. Unlike cash, electronic financial systems can control anonymity—that is, electronic payment users' information can be disclosed under some predetermined

circumstances. Camenisch et al. [72] presented a protocol for e-cash systems that revokes anonymity through a trustee when illegal situations (Figure 2), such as blackmailing and money laundering, occur.

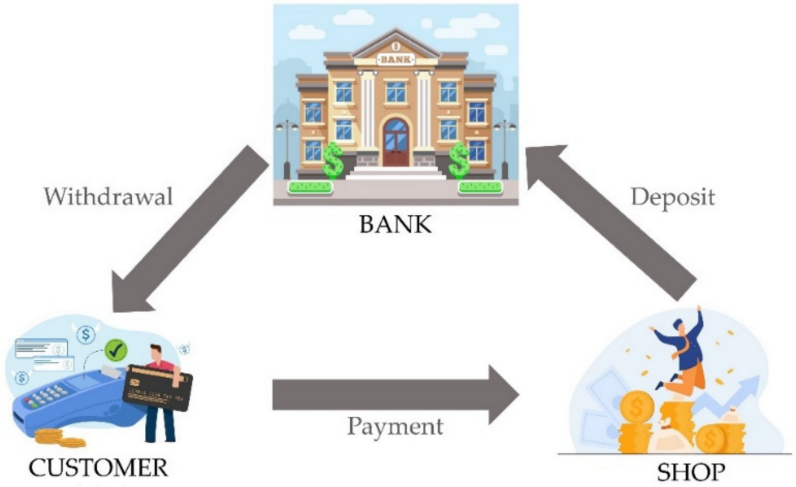


**Figure 2.** The process of the transaction proposed by Camenisch et al. [72].

Möser [73] defined cryptocurrency as an electronic payment method not with "real anonymity" but with "pseudonymity". Numerous cryptocurrencies, including Bitcoin and Ethereum, need to build the reliability of the system by using a distributed ledger while ensuring users' anonymity. Public key cryptography, which generates pseudonymous addresses for the users in the transactions, is generally used for the purpose. However, not even public key technology can secure users' anonymity when users' public key usage is continued many times. Therefore, Reid and Harrigan [74] argued that the public key must be updatable according to the cryptocurrency users' will.

Anonymity is also an important issue in CBDCs. Providing complete anonymity in CBDCs can cause the same money-laundering problems that happen in conventional financial systems. Accordingly, AML authorities have suggested the concept of anonymous vouchers, which limit the amount of CBDC that each user can utilize under the guarantee of anonymity [75].

### *2.6. Other Considerations: The DDoS Attack Prevention Plan*

The distributed denial of service (DDoS) attack is a malicious attempt of multiple users to make the system or service unavailable by draining the network resource [76–78]. Electronic financial systems with many users, such as online-based payment services, credit cards, and online banking services, are especially vulnerable to DDoS attacks, and therefore, there have been studies concerning the countermeasures [77,79,80].

Douligeris and Mitrokotsa [81] and Mankins et al. [82] proposed the concept of "Resource Pricing" that charges system users with server usage costs to reduce the possibility of DDoS attacks. Johnson et al. [83] and Wu et al. [84] reported on possible DDoS attacks during the Bitcoin mining process. The Bitcoin miners usually construct pools to increase the probability of success in the mining process. During the process, they may try a DDoS attack to interrupt other pools' mining activities. Johnson et al. [83] showed that a DDoS attack on large mining pools could be more effective than a DDoS attack on small mining pools in increasing the attackers' mining success probability. Starting from the general-sum stochastic game, Wu et al. [84] proposed a DDoS attack prevention plan based on the Nash learning algorithm by formulating mutual competition between the mining pools.

In Ref [85], a possible DDoS attack in CBDC networks is presented. Multiple malicious users can cause traffic by sending false transaction records to the CBDC networks multiple

times. To prevent possible DDoS attacks in CBDC systems, a method of limiting the users' transaction frequency and total spending limit is needed.

### 2.7. Summary

As discussed in Sections 2.1–2.6, in electronic financial systems, six security requirements, no double spending, unforgeability, non-repudiation, verifiability, and anonymity, are important issues regardless of whether the currency is e-cash, cryptocurrency, or CBDC. What research studies in Sections 2.1–2.6 suggested as a security enhancement plan for those requirements can be classified into five categories: blockchain technology, trusted third party, certification of the transaction members, tracking of transaction records, and cryptographic techniques.

## 3. Offline Payment Function after Types of Currency

Research studies related to the offline payment function of digital payment methods have been gaining attention with the emergence of e-cash in the 1990s and early 2000s. Abrazhevich [86] defined the offline payment function as follows:

- A currency that can be exchanged even in the absence of a network connection;
- A transaction that can be established without a third party acting as an arbitrator.

Chaum and Brands [87] mentioned that an offline payment function without bank intervention has the advantage of cost efficiency and speed. Another advantage of the offline payment function can be observed in terms of capacity. Furthermore, Eslami and Talebi [88] mentioned the advantage of a database was significantly reduced in size for the data-related bank transactions in the offline payment function.

Further research from the works based on the advantages has progressed, focusing on the implementation of offline payment functions in the field of e-cash. Eslami and Talebi [88] proposed an untraceable offline e-cash system using the ElGamal signature scheme to ensure user privacy. In this system, double spending can be prevented by revealing the identity information of double spenders to other users through the ElGamal signature scheme.

On the other hand, Wang et al. [89] argued that the system proposed by Eslami and Talebi is vulnerable to man-in-the-middle attacks and does not completely prevent double-spending attacks. A man-in-the-middle attack occurs when the payer sends money to the payee through a mechanism in which a man-in-the-middle intercepts the money by eavesdropping. Wang et al. [89] conducted a study to solve the problems that may arise in existing offline payment function using discrete logarithm problems and cryptographic techniques, such as the Schnorr signature and blind signature.

As many studies have dealt with topics related to the offline payment function, offline transaction methods, such as near field communication (NFC) [90], quick response (QR) code [91], and Bluetooth [92], are now diversified, and it is apparent that these studies are meaningful. Among studies related to e-cash, Camenisch et al. [72] present an online payment protocol and an offline payment function for auxiliary means. Bitcoin emerged after studies related to e-cash. Although only a few studies have dealt with the offline payment function of Bitcoin, Dmitrienko et al. [93] presented a solution to enable a secure offline payment function of Bitcoin. With the appearance of CBDC, Sato and Sudo [94] proposed a solution to use the offline payment function in situations where online payment of CBDC is impossible, such as network malfunction or underground environment, by using dual offline payment. Here, dual offline payment refers to when a payment is completed when both the payer and the payee are offline. Sato and Sudo [94] stated the necessity of offline payment function for CBDC by covering the problems that may arise from making transactions and payments possible through offline payment. Eventually, Christodorescu et al. [95] conducted a direct protocol study that implements the offline payment function of CBDC. This section analyzes the three studies above that dealt with the offline payment function for each of the different types of currencies, e-cash, Bitcoin, and CBDC.

### 3.1. Offline Payment Function with E-Cash Proposed by Camenisch

Camenisch et al. [72] divided the members participating in a transaction into the bank, the customer (payer), and the shop (payee) before presenting the transaction protocol of e-cash. Based on their involvement, the transaction is analyzed in three phases as drawn in Figure 2: 1. Withdrawal phase, 2. Payment phase, 3. Deposit phase. The three stages of the transaction are as follows:

- Withdrawal phase: a transaction phase that involves a bank and a customer (payer);
- Payment phase: a transaction phase that involves a customer (payer) and a shop (payee);
- Deposit phase: a transaction phase that involves a shop (payee) and a bank.

In online payments, undesired events are less likely to occur in the transaction process, since the three phases of a transaction occur continuously, monitoring or confirming continuously whether malicious actions occur during the processes or not. In contrast to online payment, the three phases occur separately in an offline payment function. Unlike online payment, the probability of malicious actions could increase during offline payment.

To prevent malicious action, Camenisch et al. [72] presented the requirements that the transaction members, the payer, and the payee, must satisfy in the offline payment function as follows:

- The shop (payee): must be assured that the bank will accept the payment [72];
- The customer (payer): must be assured that the withdrawn money will later be accepted for payment and that the bank cannot claim that the money has already been spent. Furthermore, they may require that their privacy be protected [72].

Camenisch et al. [72] introduced a method to prevent fraudulent actions in the offline payment function of e-cash by using observers for preventing double spending through a trusted third party. This method begins when a trustee, who acts as an observer in a transaction, obtains a coin list of a payer that can be acquired from the withdrawal protocol if the payer acts with malicious intent, such as when a coin contained in the coin list is used more than once. The trustee intervenes in the offline payment function to prevent fraudulent actions.

The anonymity of the information that the trustee can obtain through the withdrawal protocol must be guaranteed. Therefore, in the proposed offline payment function, the trustee must satisfy two requirements as follows:

- The trustee can communicate only with the customer;
- It should be impossible for the bank to obtain and track payment information, even if the bank subsequently obtains information related to the customer through the trustee.

Once these requirements for the trustee are satisfied, the transaction in the offline status will proceed safely. The solution for fraudulent actions in the offline payment through the trustee will be discussed in further detail in Section 4.

### 3.2. Offline Payment Function with Cryptocurrency Proposed by Dmitrienko

There have been numerous discussions in research studies on whether to consider Bitcoin as a currency or an investment product [96]. If Bitcoin becomes utilized as a currency in the form of cash, the offline payment function may be inevitable (e.g., when using a vending machine or the primary server network, in a situation where the central server network cannot be accessed).

Dmitrienko et al. [93] proposed security solutions for problems that may arise in the offline status to enable offline transactions of Bitcoin. They review four problems that need to be solved to set up an offline payment function for Bitcoin. They proposed solutions from the perspective of the following problems.

#### 3.2.1. Issues and Suggestions for the Large Capacity of the Blockchain

A device capable of offline payment function (e.g., pos system, mobile phone) has a capacity limit for storing the blockchain. Based on blockchain capacity problems in the past, the simple payment verification (SPV) was devised to enable simple verification with

only a block header level with a relatively small capacity. However, even the block header for SPV is too large to be downloaded on mobile devices.

As a solution to this problem, Dmitrienko et al. [93] proposed a time-based transaction confirmation verification. This method allows transaction confirmation to proceed even when the transaction details are not connected to the entire blockchain. Time-based transaction confirmation verification proceeds as follows:

- $t_i$ and $t_{i+n}$ as timestamps when the $i$-th and $i$+$n$-th blocks are created, respectively;
- $\delta$ as a security parameter;
- The transaction should be finished if, and only if, $\delta_n t_i - t_{i+n} \leq n\delta$

Through the method mentioned above, the time constraints can be controlled. Accordingly, it is possible to lower the probability of an attack being successful when the offline payment function is processed. Offline payment function can be proceeded in a secure environment by setting the variables.

#### 3.2.2. Issues and Suggestions When Hosting Platform Has Malicious Intent

A typical wallet does not have a networking interface. Therefore, the offline wallet can proceed with transactions only by forming the networking interface with assistance from the hosting platform. At this point, there is a problem, in that users' wallets may be at risk if the hosting platform causes fraudulent actions with malicious intent in an arbitrary situation.

Dmitrienko et al. [93] proposed the delayed parameters verification as a solution to the users' risk. Delayed parameters verification divides the transaction confirmation verification process into two stages. The two stages are as follows:

- Stage of storing pre-loading transactions for future use (validation parameters are not verified at this stage);
- Stage in which the recipient directly checks the validation parameters.

In delayed parameters verification, there is no benefit that the recipient can gain through manipulating the parameters. Thus, this method guarantees fraudulent actions do not occur, since the recipient directly confirms the validation parameter.

#### 3.2.3. Issues and Suggestions for the Absence of a Timer

When confirming transactions on the Bitcoin network, there is also a problem associated with measuring the generated time zone. However, a source that can measure time, such as a timer, does not necessarily exist in an offline wallet.

Limits on transaction amounts can solve the problems above. The upper bound of the time window can be estimated with a high probability without a separate timer by setting limits on the transaction amount. In addition, it is possible to solve the problem by supplementing the excess approximation value.

#### 3.2.4. Issues and Suggestions for Wallet Damage

Dmitrienko et al. [93] mentioned damage to offline wallets as the last problem. There is no doubt that offline wallets are difficult to damage due to various security technologies and hardware. However, if the attacker spends considerable time and effort to attack the offline wallet, the offline wallet will be damaged eventually, and the attacker can complete successful fraudulent actions.

Dmitrienko et al. [93] proposed a "distributed wallet revocation scheme" to solve this problem. This method allows the recipient to cancel the transaction if fraudulent actions occur or the wallet is damaged. Through this method, the recipient can directly block attacks from the attackers.

### *3.3. Offline Payment Function with CBDC Proposed by Christodorescu*

Visa has recently devised a protocol and device using Christodorescu et al.'s [95] research that can be downloaded into a personal smartphone or tablet and transacted without an intermediary [97]. The CBDC offline payment protocol proposed by Christodorescu

et al. [95] is a fundamental study that can increase the possibility of utilizing CBDC as national legal tender. Christodorescu et al. [95] proposed a method to avoid the risks that may occur in offline transactions of CBDC through the offline payment system (OPS) protocol using encryption technology based on a trusted execution environment (TEE) [98–101].

#### 3.3.1. TEE Model and UA

The offline payment protocol is the protocol that allows the payer and the payee to form transactions through balance changes in their respective offline accounts even when they do not liaise with the server. It is critical to understand the TEE model and untrusted application (UA) to understand the offline payment protocol in detail. The TEE model is a software stack stored in a ROM embedded secure device. It consists of a trusted operating system (TOS) and trusted applications (TA). TOS enables developers to access security devices. TA, which exists more than once in the model, allows using special-purpose functions that are only secured.

If UA is used benignly, it provides a function to receive digital currency when a user is connected to a server online, a function to verify transaction details, and a function to store transaction details. However, if UA is abused, some elements can threaten users.

#### 3.3.2. Components of Offline Payment System

The four components of the OPS proposed by Christodorescu et al. [95] are as follows:

- OPS Server TA: Deployed in the server, manages customer accounts, and sets up customer devices;
- OPS Sender UA: Deployed in the sender's device, provides offline payment interface to users by interacting with OPS TA and registers UA and TEE by interacting with the server;
- OPS Receiver UA: Deployed in the receiver's device, provides an interface to check receiver interface and offline payment;
- OPS TA: Deployed in the sender's secure device in TEE, manages the user's offline balance only for secure access.

#### 3.3.3. Protocol for Preparing Offline Payment System

The offline payment process begins with two stages of preparation protocol. First, the TEE-enabled device is registered in the server through the client setup protocol. When a device is registered through this protocol, the server opens an account on the device, initializes it, and provides a certificate to enable offline payment. Then, the user registers OPS TA to the server through TA registration protocol and completes preparations for using the offline payment function. When the process for preparation is completed, a direct transaction process can be executed.

#### 3.3.4. Protocols Included in the Transaction Process of Offline Payment System

After the preparation process mentioned in Section 3.3.3, the user goes through the deposit protocol process, which deposits currency from an online account to an offline account to prepare an amount of currency to be used for offline payment. On the contrary, there is also the withdraw protocol, which withdraws the balance from an offline account to an online account. When the balance is sufficient in the offline account, the offline payment between users is enabled through the offline payment protocol through the following process:

- Deduction of the amount of money to be sent from the balance of the sender's offline account;
- Addition of the received amount of money to the recipient's account.

At this time, the recipient can receive the currency to their online account through the claim protocol and may receive currency to their offline account through the collect protocol. When the recipient receives the currency, the offline payment ends. Figure 3 is an illustration of the offline payment device protocol proposed by Christodorescu et al. [95]. The detailed algorithm sequence diagram for offline payment is shown in Figure 4.

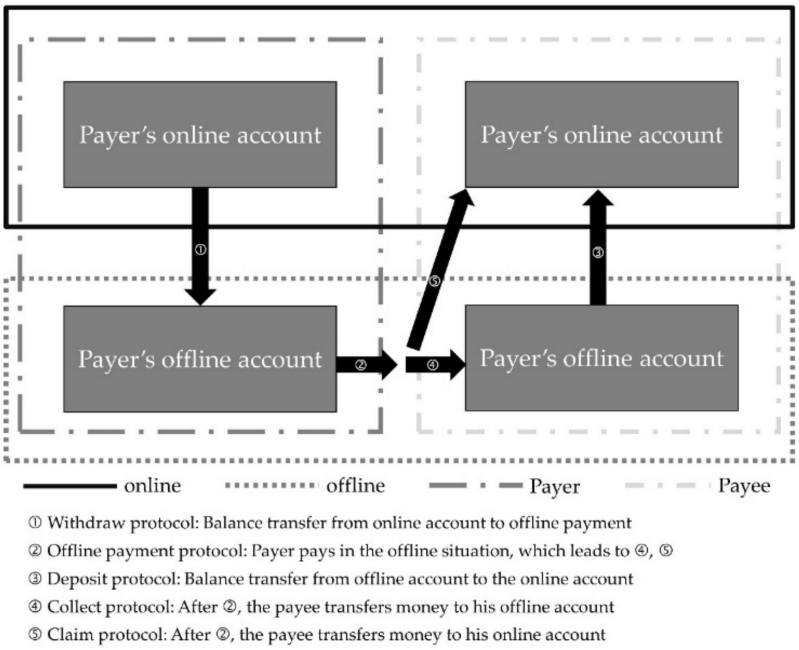


**Figure 3.** Operation of the protocol on a device using TEE technology proposed by Christodorescu et al. [95].

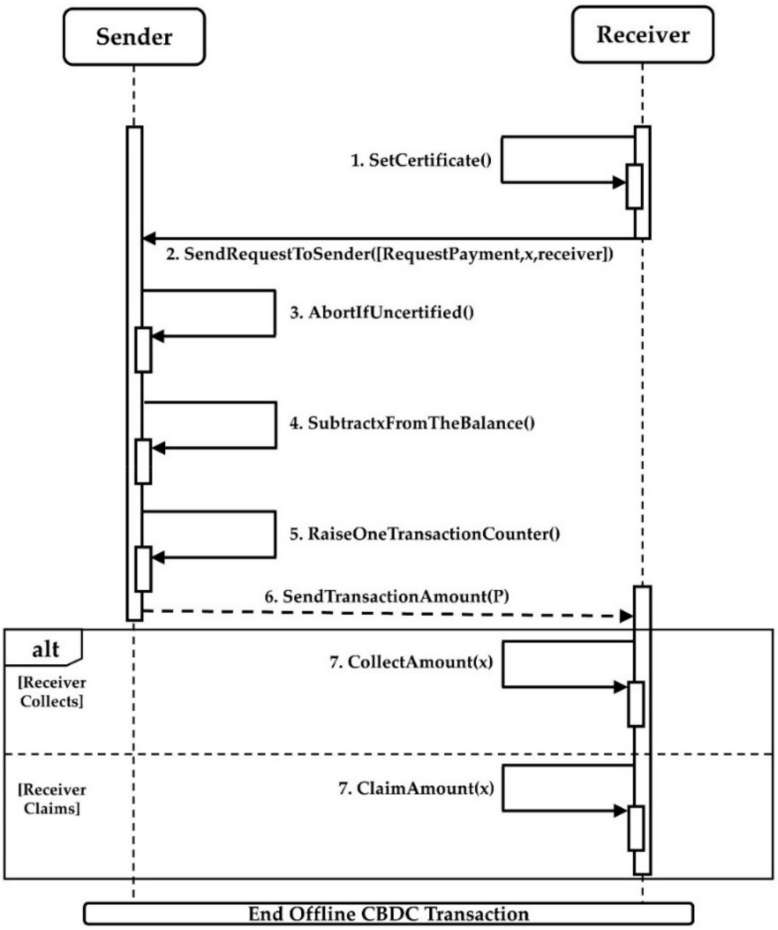


**Figure 4.** A sequence diagram of the detailed transaction process between the sender and the receiver using the offline payment protocol suggested by Christodorescu et al. [95].

3.3.5. Security Enhancement of Devices through Cryptographic Technology

When executing the offline payment protocol, the process of transaction execution by obtaining a public key and a certificate becomes enabled, based on the public-key infrastructure (PKI). The PKI consists of certificate authorities (CA) that manage the validity of certificates, registration authorities (RA) that verify the identity of users, and directory services that store the certificates. The transactions between users A and B through digital certificates [102] are processed as follows:

**Stage 1** User A requests a certificate from RA, and RA sends a certificate issued by the CA to A through communication with the CA;
**Stage 2** CA publishes A's certificate through the directory service, and B verifies A's published certificate;
**Stage 3** After completing B's certificate verification, the transaction between A and B proceeds.

Christodorescu et al. [95] used the two-tier hierarchical infrastructure method based on the PKI. Transactions are processed by issuing certificates from the presented device. The process of issuing a certificate starts with the TA registration protocol mentioned above. Details are as follows:

**Stage 1** User A creates a signing key pair—$(T_A.vk,\ T_A.sk)$;
**Stage 2** Send information related to $T_A.vk$ to the server to issue a certificate—$[cert]$;
**Stage 3** Save $(vk_A,\ cert.vk)$ in $S.Registry$, which is the server's storage.

In this case, *vk* and *sk* represent a public key and a private key. Information encrypted with the public key can be decrypted only with the paired private key. When an offline payment occurs in A's device through this method, the counterpart can confirm that A is not a malicious user through A's certificate. Consequently, they can proceed with secure transactions.

## 4. Security Requirements in Current Offline Payment Functions

In this section, the relationship among the offline payment functions through e-cash, cryptocurrency, and CBDC and their technical feasibility on the security requirements are analyzed from the perspective of no double spending, unforgeability, non-repudiation, verifiability, anonymity, and DDoS attack prevention.

### *4.1. Offline Payment Function with E-Cash Proposed by Camenisch*

In the research by Camenisch et al. [72], the offline payment functions considering the security requirements of no double spending, verifiability, and anonymity were researched, and the following solutions were proposed for the security measure, no double spending.

To satisfy the security requirements in terms of no double spending, two additional methods were proposed by Camenisch et al. [72]. The first method proposed in the research was to provide the authority to the bank to identify the double spenders. The second method proposed was to utilize observers to prevent double spending. The major difference between the first and the second method proposed is whether the double spending is identified prior to its occurrence by the bank or after the event by the third-party observer.

In the first method, the bank becomes authorized to identify the double spender through a cryptographic technology called a Schnorr signature. The detection and identification of the double spender are enabled through the calculation of the secret key in both signatures, as the double spender signs more than one message, whereas it is only possible to detect an event that occurred in the past. However, considering the characteristics of the first method, the preventive measures cannot be taken, whereas it would be possible to detect double spending in advance of its occurrence in the presence of a trustee.

The second method introducing the trustee, considered to be the third-party observer, in the transaction, is capable of preventing double spending prior to or as soon as it occurs. However, since it requires the additional entity as an observer in the system, it could result in a greater cost.

Regarding the security requirements related to anonymity and verifiability, Camenisch et al. [72] stated that fraudulent actions would not occur as long as the offline payment is processed with anonymity among the users. However, under the circumstance where anonymity is violated, fraudulent actions, such as money laundering and blackmail, could occur. Thus, as a measure for the violation, Camenisch et al. [72] proposed anonymity revocation to verify the identity of the members who participated in the transaction. The anonymity revocation proposed by Camenisch et al. [72] is to remove the anonymity of the violating users and provide them verifiability for transactions.

Among the requirements for the offline payment function presented in Section 2, three security requirements are not covered by Camenisch et al. [72]: unforgeability, non-repudiation, and DDoS attack prevention. It is necessary to devise a new method to satisfy the security requirements of unforgeability and non-repudiation in Camenisch et al. [72].

### *4.2. Offline Payment Function with Cryptocurrency Proposed by Dmitrienko*

Among the security requirements mentioned, Dmitrienko et al. [93] reviewed the fulfillment of no double spending and unforgeability for the offline payment function of Bitcoin. The risk of double spending on offline payment functions comes from the fact that the payer can use the public key more than once. In an online payment situation using blockchain, a record of double spending can be stored in a block to prevent double spending. However, it is difficult to prevent double spending from transactions via offline payment functions. In addition, since Bitcoin is traded through a distributed ledger method, it is even more difficult to use a solution introducing a trusted third party, as stated in Camenisch et al. [1]. Thus, a different approach is required to satisfy the security requirements of no double spending and unforgeability in offline payment functions.

The method proposed by Dmitrienko et al. [93] creates an offline wallet using tamper-proof secure hardware. However, unlike the security mechanism for the online payment, where no double spending is satisfied through several surveillants, this method is less stable due to the reliance on technology-based hardware support.

As an alternative to the method above, Dmitrienko et al. [93] proposed the utilization of the deposit system. This enables only wallets that have received the certificate from the certification authority to participate in offline payment functions. At this time, the certification authority must provide a certificate to the wallet to prove the amount of cryptocurrency sent. Through these two methods, the security requirements on no double spending can be satisfied even in an offline payment situation.

To satisfy the security requirements of unforgeability, the verification and confirmation mechanism based on the time-variant transaction mentioned in Section 3 could be introduced. This method imposes a time limit on the transaction confirmation verification in existing Bitcoin, and the transaction becomes recognized only when a block is created within the time limit specified. The probability of the occurrence of coin forgery $\alpha$ can be reduced by adjusting the time $\delta$ required for offline payment. If the coin forgery cannot be prevented for a specific time limit $\delta$, the forgery can be resolved by lowering the limit $\delta$. For instance, if the attacker has 40% hashing power and the time limit $\delta$ is set to 1600 s, the coin forgery attack cannot be prevented. However, when $\delta$ is set to 800 s, the probability of coin forgery $\alpha$ can be reduced down to a probability lower than a certain probability that can satisfy unforgeability even in offline payment situations.

Meanwhile, Dmitrienko et al. [93] did not deal with non-repudiation, verification, anonymity, and prevention from DDoS attacks. Additional examination is required to satisfy the above conditions, considering that the transaction details of Bitcoin are difficult to connect to the blockchain in the situation of offline payments.

### *4.3. Offline Payment Function with CBDC Proposed by Christodorescu*

Christodorescu et al. [95] proposed TEE technology applicable to the devices capable of the payment method by CBDC. However, in the proposed system via CBDC offline payment function, fraudulent activities may occur when executing the withdraw protocol,

protocol for offline payment function, and deposit. This section provides a review of the security requirements for the devices utilizing the offline payment function by CBDC.

In the protocols for withdrawal and deposit, double spending can be prevented through counters "i" in the device and server. When the currency is transferred from the server to the offline account or from the offline account to the server, 1 is added to the device's counter "T.i" and the server's counter "S.i.". Then, it is possible to confirm whether double spending has occurred through sync, which is a process of checking whether "T.i" and "S.i" are of the same value. In the offline payment protocol, double spending can be prevented by an offline payment counter "j" in the device that increases by 1 whenever the transaction occurs, and the device proceeds with a transaction and a payment log that stores transaction details.

In the presented device, non-repudiation can be prevented by using a two-tier hierarchical infrastructure. The certificate of the users with the TEE device is stored in the server storage, S.Registry, through the TA registration protocol. When the payer transfers money to the payee, the payee can verify the payer's certificate in the storage before the payment starts. After the payer's information is checked, the payee then processes payment requests to the payer, and offline payment function can proceed when the payer sends the currency. In this way, both the payer and the payee cannot repudiate that offline payment has already been processed.

When offline payment occurs, transaction information P, including the amount of currency sent, sender's certificate, information on the recipient, and transaction counter "j" to prevent double spending are stored in the device's T.inPaymentLog. This information makes it possible to determine the part of the transaction in which problems occurred, and the security requirement of verifiability in offline payment is satisfied.

The device user cannot view the transactional history through the TEE device. The entity responsible for the management of the device only has access to the TEE device and verifies the transactional information. Therefore, the anonymity for average users utilizing the devices in the offline payment by CBDC can be maintained.

On the other hand, Christodorescu et al. [95] proposed that the offline payment system does not directly deal with unforgeability and prevents DDoS attacks. Despite someone freely duplicating or creating a CBDC via offline payment, it is still not easy to detect whether CBDC is forged, and countermeasures are required. In addition, when the transactions are in the process between the server through withdraw protocol and the offline account through the deposit protocol, they are connected to the server. Thus, it is essential to prepare a countermeasure against malicious users generating traffic to the server. Table 2 represents whether research studies on existing offline payment functions satisfy the security requirements.

**Table 2.** Confirmation as to whether research studies on existing offline payment functions satisfy the requirements.

| | No Double Spending | Unforgeability | Non-Repudiation | Verifiability | Anonymity | DDoS Attack Prevention |
|---|---|---|---|---|---|---|
| Camenisch et al. [72] | O | X | X | O | O | X |
| Dmitrienko et al. [93] | O | O | X | X | X | X |
| Christodorescu et al. [95] | O | X | O | O | O | X |

## 5. Discussion

Prior research studies on digital payment methods have attempted to expand the purpose and utilization of each payment method through the implementation of functions of offline payments. Further from the research phase, there are currently efforts to introduce offline payment functions by CBDC in their domestic systems. However, the authorities have considered offline payment functions by CBDC to be problematic from the perspective

of security issues. The three studies reviewed in Sections 3 and 4 stated the security imperfections of the offline payment function, regardless of the novelty of the research.

### *5.1. Limitations in Satisfying Security Requirements for Offline Payment Function*

As shown in Table 3, the methods introduced in the existing research can be categorized into five types to satisfy the security requirements of the digital payment method mentioned in Section 2. The five types of methods are as follows: 1. Blockchain technology, 2. Trusted third party involvement, 3. Supply of certificates to transactions members, 4. Tracking flow of money, 5. Cryptographic technique.

**Table 3.** A study on various types of security reinforcement plans for digital payment methods.

| Security Enhancement Plan | Research | Security Requirements | Detail |
|---|---|---|---|
| Blockchain technology | Savolainen and Soria [45] | No double spending | Prevention of double spending through proof of work (A method for users to check whether the transaction is true or false). * Not applicable when an attacker has over 50% of hashing power. |
| | Crosby et al. [55] | Unforgeability | Transparency to the supply chain through BlockVerify using blockchain's distributed ledger technology and security. |
| | Velde [56] | Unforgeability | Solution for issues over counterfeiting currency with proof of work. |
| | Nakamoto [62] | Non-repudiation | Proposal of methodology difficult to maliciously modify and delete Bitcoin's transaction history recorded in a blockchain. |
| | Dorsala et al. [68] | Verifiability | Methods to cut off the possibility of a fraudulent act within a transaction by saving all trade conducted in a network on a block. |
| | Reid and Harrigan [74] | Anonymity | Reinforcement of user anonymity by creating only the necessary numbers of the public key for each user. |
| Trusted third party | Karame et al. [46] | No double spending | Monitoring double spending by adopting the "inserting observers" method to solve problems caused by Bitcoin's fast payment. |
| | Payeras-Capellà et al. [66] | Verifiability | Introduction of a trusted third party, who becomes directly involved when there is inappropriate behavior within the transaction. |
| Certification of the transaction members | Krsul et al. [43] | No double spending | Proposal of the transaction system, tolerating the transactions for the buyer and seller with only the serial numbers matching. |
| | Kremer et al. [61] | Non-repudiation | Proposal of the transaction system tolerating the entities capable of NRE formulation and the system issuing non-repudiation of receipt to the payer and original non-repudiation receipt to the payee. |
| Tracking of transaction records | Brands [42] | No double spending | Improvement of the security system for the traceability history of e-cash trade, examining one-show blind signatures and wallets with the observer's method. |
| | Camenisch et al. [72] | Anonymity | Suggestions on the improvement of the system tracking the user, using anonymity revocation when irrelevant behavior within the e-cash system is detected. |
| Cryptographic techniques | Pointcheval and Stern [44] | No double spending | Proposal of the cryptographic technique for the users to use a blind RSA signature to prevent double spending. |
| | Seo and Kim [67] | Verifiability | Suggestion for the improvement of cryptographic technique considering the transaction security, utilizing the domain-verifiable signcryption scheme that only gives a predetermined $n$ number of EFT protocol participants access to check the transaction. |
| | Robinson [64] | Non-repudiation | Proposal of the security system with Keccak-256 and a hash value to prevent malicious changes during the transaction process in block contents. |
| | Sánchez [69] | Verifiability | Improvement of the security system for the transaction process with a combination of MPC protocol and ZKP to guarantee verifiability without revealing personal information. |
| | Möser [73] | Anonymity | Proposal of the system creating an environment with a pseudonym via Ethereum's hash value address that hides personal information in the pseudonymity. |

#### 5.1.1. Applying Blockchain Technology

Savolainen and Soria [45], Crosby et al. [55], Velde [56], Nakamoto [62], Dorsala et al. [68], and Reid and Harrigan [74] reviewed how the financial system is capable of satisfying the security requirements through blockchain technologyin online situations. Transactional information and member information are recorded via blockchain, and it is possible to confirm whether the fraudulent activity has occurred. Various CBDC systems also use DLT, the core technology of blockchain networks, to enhance security in online

situations [103–105]. However, since it is difficult to proceed with transactions under the surveillance among entities in offline payments, a consensus algorithm, such as PoW, cannot be introduced. For these reasons, there are still technical barriers to be resolved for blockchain technology to be adopted in offline situations.

#### 5.1.2. Trusted Third Party (TTP) Involvement

In the research conducted by Karame et al. [46] and Payeras-Capellà et al. [66], the method of the trusted third party (TTP) involvement can be considered in a transaction. TTP observes transactions and monitors the users of the transaction system to prevent fraudulent activities. In addition, there have been methods devised to prevent fraudulent activities by the direct intervention of TTP during the transaction process, not only for monitoring. TTP can intervene in the protocol for withdrawal and deposit. Therefore, the currency circulating in the offline wallet of the payer or payee can be disclosed using TTP. This method of using TTP is being considered a security enhancement measure in many CBDC studies [106,107]. However, TTP can intervene only under the circumstance when connected to an online network. Thus, when transacting via the protocol for offline payment, it is not possible to observe the status of the offline payment protocol directly, since TTP is not available offline. For this reason, it is not easy to introduce the method of trusted third party (TTP) involvement in an offline payment function.

#### 5.1.3. Pre-Certification for Members Participating in the Transaction or Post-Certification of Transaction Confirmation

Krsul et al. [43] proposed a method to prevent double-spending transactions by receiving tokens with the same serial number from a third party. However, this method cannot proceed during the transaction unless both parties are pre-approved. Thus, this method is difficult for applying CBDC to various offline payment functions, since it is difficult to use CBDC in general.

Kremer et al. [61] proposed suggestions on the methods to certify a transaction. Numerous online CBDC systems also use a method of authorizing users by verifying them in advance [108]. However, it is difficult to confirm that the two entities have received the certificates offline. Additionally, malicious users are capable of easily deleting the certificates issued. For this reason, it is critical to carefully review the prevention of repudiation in an offline payment using a certificate.

#### 5.1.4. Tracking Flow of Money

The methods of tracking transactional information covered in Brands [42] and Camenisch et al. [72] are also difficult to apply to offline payments. Unlike online situations where transactional information can be recorded and tracked on a central server, users do not have access to the main server in offline situations. Thus, transactional information should be recorded in the device's storage rather than on the central server.

Reinforcing security by tracking the flow of money is also discussed in CBDC [106,109]. However, in this offline situation, it is difficult to monitor whether the fraudulent activity has occurred in the transactions based on the information recorded in the storage; forgery/falsification can occur freely. Due to these problems, tracking the flow of money in offline payments of CBDC is hard to implement.

#### 5.1.5. Using Cryptographic Technique

Pointcheval and Stern [44], Seo and Kim [67], Robinson [64], Sánchez [69], and Möser [73] used cryptographic techniques for security. Of the five methods, the cryptographic technique could be considered to be the only technique that perfectly applies to the offline payment function. The PKI method, mentioned in Section 3, allows safe transactions even though the certificate authority is offline, since a certificate states whether the counterpart is a trusted user. In addition, Christodorescu et al. [3] proposed implementing offline payment through certificate issuance using the two-tier hierarchical infrastructure

method based on PKI. Many studies focusing on offline transactions deal with security elements through the method of using cryptography technology.

### 5.2. Discussion to Satisfy Security Requirements for Offline Payment Function—Focusing on the Research about Offline Payment Protocol of CBDC

It is possible to confirm that several documents dealt with the offline payment function of CBDC. Riksbank proposed a method of limiting the amount that can be remitted when CBDC transactions occur in offline situations [110]. Richards et al. [111] stated that using CBDC as a token-based rather than account-based system is advantageous for offline payment. In an account-based system, the balances of the payer and the recipient are updated during transactions, and a token-based system is recorded only for those who hold CBDCs [112]. Crunchfish's turn-key solution eliminates the risk of server overload, failure, and downtime for offline digital currency [113]. It is also possible to use a method in which the central bank allows only authorized CBDCs to be transacted through one signer. The World Economic Forum proposed a method of limiting the number of transactions offline [114]. Additionally, a method of making reliable hardware for offline payments is used [115].

However, throughout the research conducted thus far, Christodorescu et al. [95] is the only research that proposed the implementation of the CBDC offline payment function in the form of a protocol. The security requirements that Christodorescu et al. [95] did not satisfy, for example unforgeability and DDoS attack prevention, can be supplemented by applying the existing method and proposing a new method.

#### 5.2.1. Solutions to Satisfy Security Requirement of Unforgeability

- Dmitrienko et al.'s [93] method: In the case of CBDC, using the distributed ledger scheme, forgery attacks can be prevented through the time-based transaction confirmation verification mechanism proposed by Dmitrienko et al. [93]. In the blockchain methods available, n—confirmation blocks had to be created to confirm the transaction. Based on this method, in an offline situation using the time-based transaction confirmation verification mechanism, the attacker is forced to create n—confirmation blocks within the time limit $n\delta$. Thus, the probability of forgery is reduced. The probabilistic relationship between delta and the probability of forgery is described in detail in Section 4.2.
- Method of modifying the increasing conditions of a counter of a device and using sync: In this method, after modification of the increasing conditions of a counter of a device, it is possible to confirm that a forgery attack has occurred through sync. Table 4 shows the description of the variables used.

**Table 4.** Variables are used in modifying the increasing conditions of the counter of a device and using sync.

| Variable | Definition | Function |
|---|---|---|
| T.i | A counter in a device | A variable that increases by 1 when a withdraw protocol or deposit protocol occurs, indicating how many times both protocols have progressed. |
| S.i | A counter in a server | A variable that increases by 1 when a withdraw protocol or deposit protocol occurs along with T.i. |
| T.bal | Account balance of a device | The amount of money the offline payment device holds to make a transaction. |

To use this method, it is necessary to modify the conditions for T.i to increase. In the current method, the increase in T.i occurred secondary to withdrawal (a process of transferring balances from an online account to an offline wallet) or deposit (a process of transferring money from an offline wallet to an online account). During the process for withdrawal and deposit, when all T.bal changes except the offline payment, the condition

must be modified to increase T.i. Applying this modification will increase T.i when money is forged in offline wallets, in addition to the withdrawal and deposit processes. Next, when the sync process occurs, if the offline payment device intentionally rejects the sync operation, or if the values of T.i and S.i are different, the transaction of the corresponding device must be blocked entirely. Figure 5 is a schematic diagram of the above method.

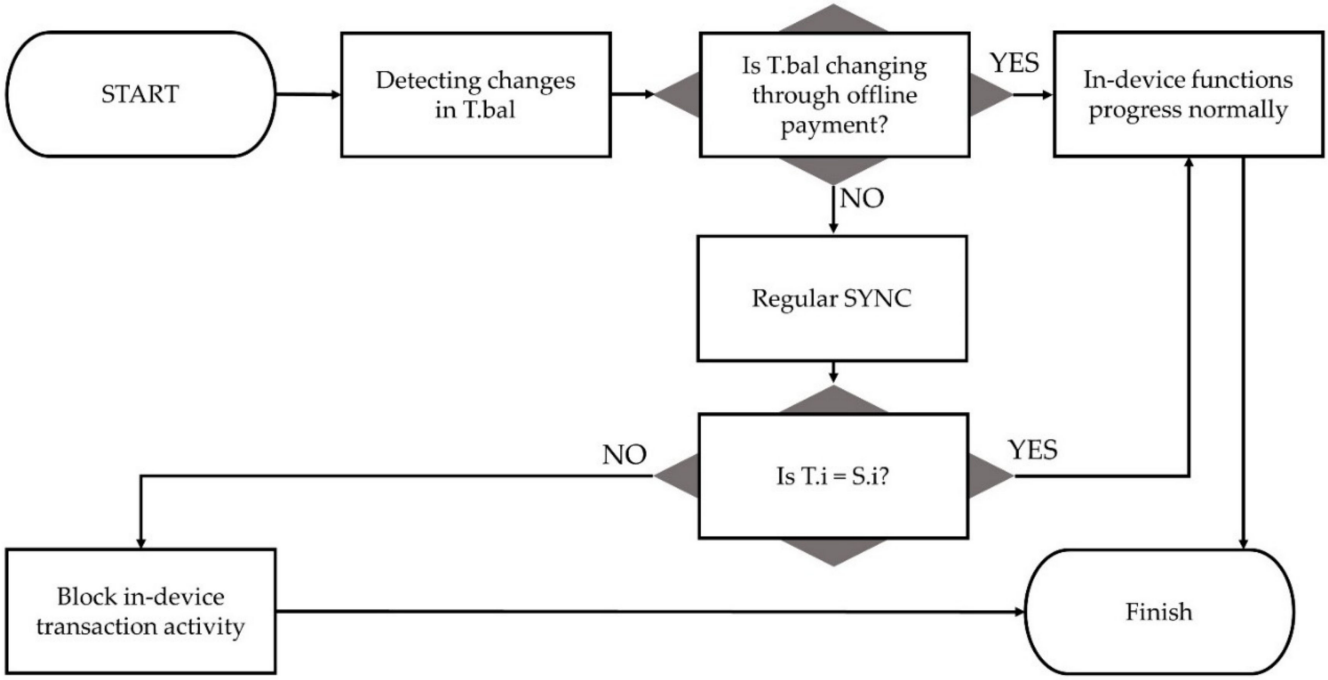


**Figure 5.** Flowchart of the method to sync every regular time to satisfy the security requirement of unforgeability.

5.2.2. Solutions to Satisfy Security Requirements of DDoS Attack Prevention

- Method of charging a fee when using the withdrawal or deposit function: The charging system used in the withdraw and deposit protocol can be applied [85]. In the current digital payment system, the profit considered when charging a fee that an attacker can be charged is designed to be less than the cost of a DDoS attack. In the model proposed by Christodorescu et al. [95], when using the withdraw and deposit protocol, the motive for attempting a DDoS attack can be eliminated by charging a fee.
- Method of limiting the number of transactions when using withdraw or deposit function: There is also a way to limit the number of transactions, as shown in Figure 6. The source is blocked so that the withdraw/deposit protocol to generate traffic to the server cannot be intentionally used excessively. DDoS attacks can be prevented through this method.

5.2.3. Additional Considerations to Strengthen the Security Requirements

Despite the security of Christodorescu et al. [95] being reinforced through the methods mentioned above, there is still a fundamental problem related to the dependence on TEE technology. This problem is not limited only to the implementation of the security by Chirstodorescu et al. [95], but all offline payment systems have no other available options but to use terminals, such as cards or smart devices, which will inevitably encounter a problem. Any effort contributing to strengthening the security of the offline payment function can become futile through continuous attacks on the terminal itself by hackers.

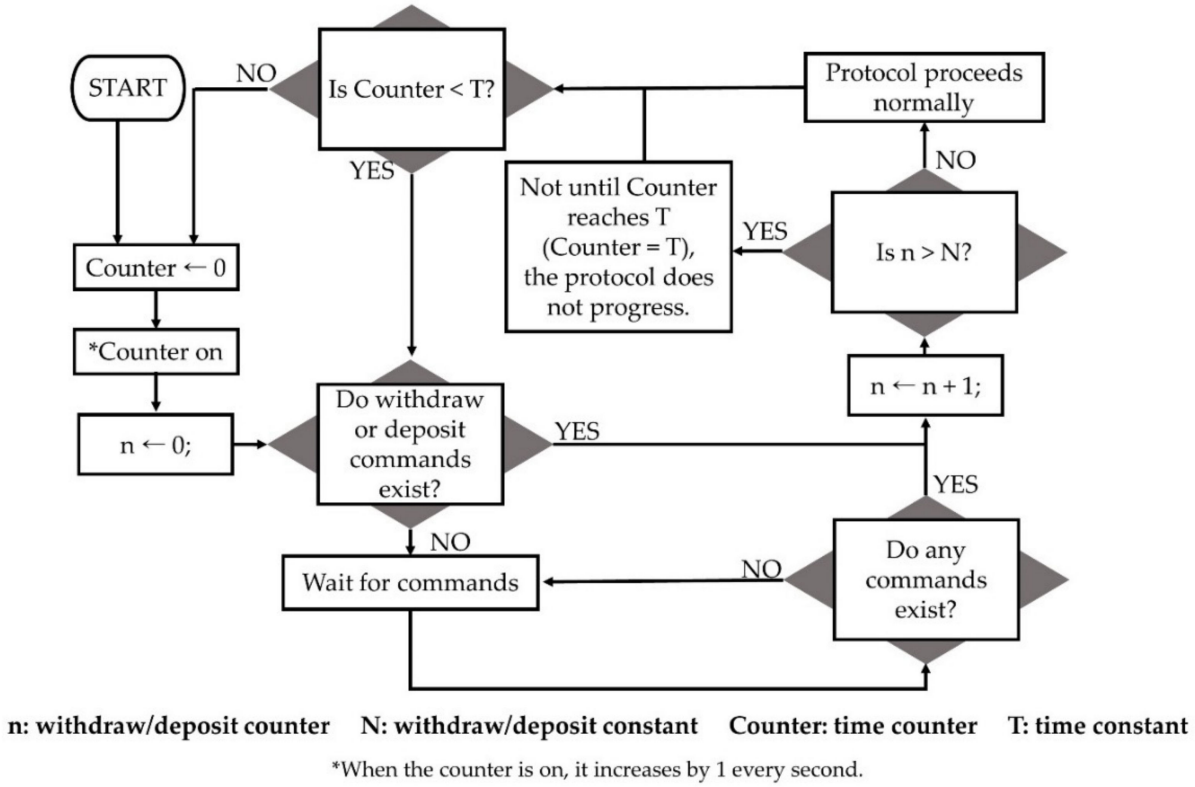


**Figure 6.** Flowchart of the method to limit the number of transactions to satisfy the security requirements to prevent DDoS attacks.

For this reason, even if the terminal used in the system operates in offline payment mode for a certain amount of time due to various environmental constraints, in other cases, transactional information that was operated in an offline payment mode must be recorded on the online server through periodic synchronization with the online server. Synchronization can facilitate the judicial process after a fraudulent action that breaks down all security elements. Although this method solves the problem from the ex-post point of view, it can reduce the motivation of hackers to attack.

## 6. Conclusions

Thus far, there have been efforts to introduce payment systems with greater efficiency and safety. As a consequence, offline payment functions utilizing e-cash as national legal tender have been emerging with the prospects suggested by several research studies throughout multiple countries.

CBDC, which is currently considered attractive to several national financial institutions, can also be utilized as national legal tender when offline payments can proceed safely. However, in offline transactions, there are still strong possibilities that transactional information cannot be stored on the server. Moreover, even if the transaction records are forged or falsified, they cannot be recognized. Consequently, currently available digital payment methods that satisfy these security requirements have limitations with regard to the introduction of digital payment methods in offline payment functions.

Accordingly, in this paper, current methods, such as blockchain technology, trusted third party involvement, supply of certificate to transactions members, tracking the flow of currency, and cryptographic technique were reviewed to improve the security of offline payment functions.

Moreover, considering the eventual purpose of the TEE device proposed by Christodorescu et al. [95] for offline transactions, it is possible to see that the criteria for the security requirements of a transaction are still not satisfied. Hence, in this review, possible methods

of modifying the system security against DDoS attacks and unforgeability during a transaction made as an offline payment via a TEE device proposed by Christodorescu et al. [95] were reviewed.

In addition to the security methods reviewed, it was possible to confirm the fact that the payment system through CBDC has been gaining attention recently as an alternative to national legal tender, and the research studies thereupon are now active. However, the issues related to the security requirements remain to be resolved due to its technical nature; the offline environment in which the participants transact cannot be fully monitored. Thus, it is critical for countries planning to introduce payment methods based on currently available CBDC in an offline environment to further investigate and research thereon to improve the security of transaction systems.

**Author Contributions:** Conceptualization, Y.C. and S.K.; methodology, S.K.; validation, Y.C., J.L. and S.K.; investigation, Y.C.; resources, Y.Y.; writing—original draft preparation, Y.C. and S.K.; writing—review and editing, H.K. and H.C.; visualization, Y.C.; supervision, J.L. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported by the Seoul National University Electric Power ResearchInstitute (SEPRI).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict or interest.

## References

1. De Almeida, P.; Fazendeiro, P.; Inácio, P.R. Societal risks of the end of physical cash. *Futures* **2018**, *104*, 47–60. [CrossRef]
2. Who Prints Money in the U.S.? Available online: https://www.investopedia.com/ask/answers/082515/who-decides-when-print-money-us.asp (accessed on 11 April 2022).
3. Recent Federal Reserve Monetary Policy. Available online: https://www.youtube.com/watch?v=0PmXbTcOVhU (accessed on 11 April 2022).
4. Tobin, J. *Financial Innovation and Deregulation in Perspective*; Cowles Foundation for Research in Economics at Yale University: New Haven, CT, USA, 1986; pp. 19–29.
5. Hofmann, C. The changing concept of money: A threat to the monetary system or an opportunity for the financial sector? *Eur. Bus. Organ. Law Rev.* **2020**, *21*, 37–68. [CrossRef]
6. Garcia-Swartz, D.D.; Hahn, R.W.; Layne-Farrar, A. The move toward a cashless society: A closer look at payment instrument economics. *Rev. Netw. Econ.* **2006**, *5*. [CrossRef]
7. Coyle, K.; Kim, L.; O'Brien, S. *2021 Findings from the Diary of Consumer Payment Choice*; Federal Reserve Bank of San Francisco: San Francisco, CA, USA, 2021.
8. Khiaonarong, T.; Humphrey, D. Cash use across countries and the demand for central bank digital currency. *J. Paym. Strategy Syst.* **2019**, *13*, 32–46.
9. World Cash Report: 2018. Available online: https://www.g4scashreport.com/ (accessed on 11 April 2022).
10. Zandi, M.; Singh, V.; Irving, J. The Impact of Electronic Payments on Economic Growth. *Moody's Anal. Econ. Consum. Credit. Anal.* **2013**, *217*.
11. Why Central Bank Digital Currencies? Available online: https://libertystreeteconomics.newyorkfed.org/2021/12/why-central-bank-digital-currencies/ (accessed on 11 April 2022).
12. How e-Wallets Charge Fees: Every Step of the Process. Available online: https://www.sticpay.com/news/news_detail/how-e-wallets-charge-fees-every-step-of-the-process (accessed on 11 April 2022).
13. Equifax Hack: 5 Biggest Credit Card Data Breaches. Available online: https://www.investopedia.com/news/5-biggest-credit-card-data-hacks-history/ (accessed on 11 April 2022).
14. Huge South Korean Data Leak Affects almost Half the Country. Available online: https://www.businessinsider.com/south-korea-data-leak-2014-1 (accessed on 11 April 2022).
15. Turvey, C.G.; Xiong, X. Financial inclusion, financial education, and e-commerce in rural china. *Agribusiness* **2017**, *33*, 279–285. [CrossRef]
16. Gill, W.; Hara, S.; Whitney, L. *Study on Risks and Opportunities of Digitalization for Financial Inclusion*; European Commission: Brussels, Belgium, 2018.
17. Kiff, M.J.; Alwazir, J.; Davidovic, S.; Farias, A.; Khan, M.A.; Khiaonarong, M.T.; Malaika, M.; Monroe, H.; Sugimoto, N.; Tourpe, H.; et al. *A Survey of Research on Retail Central Bank Digital Currency*; International Monetary Fund: Washington, DC, USA, 2020.

18. J.P. Morgan Releases Unlocking $120 Billion in Cross-Border Payments Report. Available online: https://www.jpmorgan.com/news/jpmorgan-central-bank-digital-currency-report (accessed on 11 April 2022).
19. Progress of Research & Development of E-CNY in China. Available online: http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf (accessed on 11 April 2022).
20. The Number of Americans with Bank Accounts Rises. Available online: https://www.experian.com/blogs/ask-experian/research/the-decline-of-the-unbanked-and-underbanked/ (accessed on 11 April 2022).
21. Central Bank Digital Currency Can Contribute to Financial Inclusion but Cannot Solve Its Root Causes. Available online: https://www.atlanticcouncil.org/blogs/geotech-cues/central-bank-digital-currency-can-contribute-to-financial-inclusion-but-cannot-solve-its-root-causes/ (accessed on 11 April 2022).
22. Sweden Takes Another Step Toward a Digital Currency. Available online: https://www.investopedia.com/sweden-takes-another-step-toward-a-digital-currency-5092069 (accessed on 31 January 2022).
23. The e-Krona and the Macroeconomy. Available online: https://www.econstor.eu/handle/10419/232929 (accessed on 11 April 2022).
24. Riksbank, S. Special Issue on the e-Krona. In *Sveriges Riksbank Economic Review*; Sveriges Riksbank: Stockholm, Sweden, 2018.
25. Armelius, H.; Guibourg, G.; Levin, A.; Söderberg, G. The rationale for issuing e-krona in the digital era. *Sver. Riksbank Econ. Rev.* **2020**, *2*, 6–18.
26. Lee, J.Y. Central Bank Digital Currency. Bank of Korea. Available online: http://www.bok.or.kr/portal/bbs/B0000232/view.do?nttId=10049812&menuNo=200706&pageIndex=2 (accessed on 11 April 2022).
27. Licandro, G. *Uruguayan e-Peso on the Context of Financial Inclusion*; Banco Central Del Uruguay: Montevideo, Uruguay, 2018.
28. About Sand Dollar—Bahamas. Available online: https://www.sanddollar.bs/about (accessed on 11 April 2022).
29. What Is SOV? Available online: https://sov.foundation/ (accessed on 11 April 2022).
30. Marshall Islands Readies to Make Waves in Digital Currency. Available online: https://www.centralbanking.com/fintech/7697246/marshall-islands-readies-to-make-waves-in-digital-currency (accessed on 11 April 2022).
31. With 56 bln Yuan in Transactions, Where is China's Heading? Available online: http://www.news.cn/english/2021-11/10/c_1310303262.htm (accessed on 11 April 2022).
32. Distributed Ledger Technology and the Future of Money and Banking. Available online: https://www.degruyter.com/document/doi/10.1515/ael-2019-0095/html (accessed on 11 April 2022).
33. Distributed Ledgers. Available online: https://www.investopedia.com/terms/d/distributed-ledgers.asp (accessed on 11 April 2022).
34. Rejeb, A.; Rejeb, K.; Keogh, J.G. Centralized vs. decentralized ledgers in the money supply process: A SWOT analysis. *Quant. Financ. Econ.* **2021**, *5*, 40–66. [CrossRef]
35. Permissioned Blockchain. Available online: https://www.investopedia.com/terms/p/permissioned-blockchains.asp (accessed on 11 April 2022).
36. Permissioned vs. Permissionless Blockchains. Available online: https://101blockchains.com/permissioned-vs-permissionless-blockchains/#prettyPhoto (accessed on 11 April 2022).
37. The Technology of Retail Central Bank Digital Currency. Available online: https://www.bis.org/publ/qtrpdf/r_qt2003j.htm (accessed on 11 April 2022).
38. Soderberg, G.; Bechara, M.; Bossu, W.; Che, N.X.; Kiff, J.; Lukonga, I.; Griffoli, T.M.; Sun, T.; Yoshinaga, A. Behind the Scenes of Central Bank Digital Currency: Emerging Trends, Insights, and Policy Lessons. *FinTech Notes* **2022**, *2022*, 35.
39. RBI Releases Framework for Facilitating Small Value Digital Payments in Offline Mode. Available online: https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=53038 (accessed on 11 April 2022).
40. Han, X.; Yuan, Y.; Wang, F. A Blockchain-based Framework for Central Bank Digital Currency. In Proceedings of the 2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Zhengzhou, China, 6–8 November 2019.
41. Chohan, U.W. The Double Spending Problem and Cryptocurrencies. *SSRN* **2021**, 3090174. [CrossRef]
42. Brands, S. Untraceable Off-line Cash in Wallet with Observers. In Proceedings of the Annual International Cryptology Conference, CRYPTO 1993: Advances in Cryptology—CRYPTO' 93, Santa Barbara, CA, USA, 22–26 August 1993.
43. Krsul, I.V.; Mudge, J.C.; Demers, A.J. Method of Electronic Payments that Prevents Double-Spending. Patent US5839119A, 17 November 1998.
44. Pointcheval, D.; Stern, J. Security Arguments for Digital Signatures and Blind Signatures. *J. Cryptol.* **2000**, *13*, 361–396. [CrossRef]
45. Savolainen, V.; Soria, J. Too Big to Cheat: Mining Pools' Incentives to Double Spend in Blockchain Based Cryptocurrencies. *SSRN* **2019**, 3506748. [CrossRef]
46. Karame, G.O.; Androulaki, E.; Capkun, S. Double-spending fast payments in bitcoin. In Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS '12), Raleigh, NC, USA, 16–18 October 2012.
47. Bentov, I.; Lee, C.; Mizrahi, A.; Rosenfeld, M. Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y. *ACM SIGMETRICS Perform. Eval. Rev.* **2014**, *42*, 34–37. [CrossRef]
48. Armelius, H.; Claussen, C.A.; Hull, I. On the possibility of a cash-like CBDC. In *Sveriges Riksbank Staff Memo*; Sveriges Riksbank: Stockholm, Sweden, 2021.
49. Okamoto, T.; Ohta, K. Universal Electronic Cash. In Proceedings of the Annual International Cryptology Conference, CRYPTO 1991: Advances in Cryptology—CRYPTO '91, Santa Barbara, CA, USA, 11–15 August 1991.

50. Franklin, M.; Yung, M. Secure and efficient off-line digital money (extended abstract). In Proceedings of the International Colloquium on Automata, Languages, and Programming, ICALP 1993: Automata, Languages and Programming, Lund, Sweden, 5–9 July 1993.
51. Lockett, N. Legal perspectives on digital money in Europe. *Eur. Bus. Rev.* **1999**, *99*, 235–241. [CrossRef]
52. Al-Laham, M.; Al-Tarawneh, H.; Abdallat, N. Development of electronic money and its impact on the central bank role and monetary policy. *Issues Inf. Sci. Inf. Technol.* **2009**, *6*, 339–349.
53. Shoaib, M.; Ilyas, M.; Khiyal, M.S.H. Official digital currency. In Proceedings of the Eighth International Conference on Digital Information Management (ICDIM 2013), Islamabad, Pakistan, 10–12 September 2013.
54. Mckinney, R.E., Jr.; Shao, L.P.; Rosenlieb, D.C., Jr.; Shao, D.H. Counterfeiting in cryptocurrency: An emerging problem. In *Handbook of Digital Currency*; Academic Press: Cambridge, MA, USA, 2015; pp. 173–187.
55. Crosby, M.; Pattanayak, P.; Verma, S.; Kalyanaraman, V. Blockchain technology: Beyond bitcoin. *Appl. Innov.* **2016**, *2*, 6–10.
56. Velde, F. Bitcoin: A Primer. 2013. Available online: https://www.chicagofed.org/publications/chicago-fed-letter/2013/december-317 (accessed on 11 April 2022).
57. McCullagh, A.; Caelli, W. Non-Repudiation in the Digital Environment. 2000. Available online: https://firstmonday.org/ojs/index.php/fm/article/download/778/687?inline=1 (accessed on 11 April 2022).
58. Coffey, T.; Saidha, P. Non-repudiation with mandatory proof of receipt. *ACM SIGCOMM Comput. Commun. Rev.* **1996**, *26*, 6–17. [CrossRef]
59. Zhou, J.; Gollmann, D. A fair non-repudiation protocol. In Proceedings of the 1996 IEEE Symposium on Security and Privacy (IEEE), Oakland, CA, USA, 6–8 May 1996.
60. Zhang, N.; Shi, Q. Achieving non-repudiation of receipt. *Comput. J.* **1996**, *39*, 844–853. [CrossRef]
61. Kremer, S.; Markowitch, O.; Zhou, J. An intensive survey of fair non-repudiation protocols. *Comput. Commun.* **2002**, *25*, 1606–1621. [CrossRef]
62. Nakamoto, S.; Bitcoin, A. Bitcoin: A Peer-to-Peer Electronic Cash System. *Decentralized Bus. Rev.* **2008**, 21260.
63. Message Digests and Digital Signatures. Available online: https://www.ibm.com/docs/en/ibm-mq/7.5?topic=concepts-message-digests (accessed on 11 April 2022).
64. Robinson, P. The merits of using ethereum mainnet as a coordination blockchain for ethereum private sidechains. *Knowl. Eng. Rev.* **2020**, *35*, e30. [CrossRef]
65. Security of a CBDC. Available online: https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-11/ (accessed on 11 April 2022).
66. Payeras-Capellà, M.M.; Ferrer-Gomila, J.L.; Huguet-Rotger, L. Anonymous payment in a fair e-commerce protocol with verifiable TTP. In Proceedings of the International Conference on Trust, Privacy and Security in Digital Business, Copenhagen, Denmark, 22–26 August 2005; Springer: Berlin/Heidelberg, Germany, 2005.
67. Seo, M.; Kim, K. Electronic funds transfer protocol using domain-verifiable signcryption scheme. In Proceedings of the International Conference on Information Security and Cryptology, Seoul, Korea, 9–10 December 1999; Springer: Berlin/Heidelberg, Germany, 1999.
68. Dorsala, M.R.; Sastry, V.N.; Chapram, S. Fair Protocols for Verifiable Computations Using Bitcoin and Ethereum. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–8 July 2018.
69. Sánchez, D.C. Raziel: Private and verifiable smart contracts on blockchains. *arXiv* **2018**, arXiv:1807.09484 2018.
70. Everything You Need to Know about Central Bank Digital Currencies (CBDCs) and What It Means for Financial Institutions. Available online: https://ripjar.com/cbdcs-central-bank-digital-currencies/ (accessed on 4 April 2022).
71. Benshalom, I. Taxing Cash. *Columbia J. Tax Law* **2012**, *4*, 65. Available online: https://heinonline.org/HOL/LandingPage?handle=hein.journals/colujoutl4&div=4&id=&page= (accessed on 11 April 2022).
72. Camenisch, J.; Maurer, U.; Stadler, M. Digital payment systems with passive anonymity-revoking trustees. *J. Comput. Secur.* **1997**, *5*, 69–89. [CrossRef]
73. Möser, M. Anonymity of Bitcoin Transactions. In Proceedings of the Münster Bitcoin Conference, Münster, Germany, 17–18 July 2013.
74. Reid, F.; Harrigan, M. An analysis of anonymity in the bitcoin system. In *Security and Privacy in Social Networks*; Springer: New York, NY, USA, 2013; pp. 197–223.
75. Exploring Anonymity in Central Bank Digital Currencies. Available online: https://www.ecb.europa.eu/home/html/index.en.html (accessed on 4 April 2022).
76. Mirkovic, J.; Reiher, P. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Comput. Commun. Rev.* **2004**, *34*, 39–53. [CrossRef]
77. Urs, B.A. Security issues and solutions in e-payment systems. *Fiat Iustitia* **2015**, *1*, 172–179.
78. Wang, B.; Zheng, Y.; Lou, W.; Hou, Y.T. DDoS attack protection in the era of cloud computing and software-defined networking. *Comput. Netw.* **2015**, *81*, 308–319. [CrossRef]
79. Dwivedi, A.; Dwivedi, A.; Kumar, S.; Pandey, S.K.; Dabra, P. A cryptographic algorithm analysis for security threats of Semantic E-Commerce Web (SECW) for electronic payment transaction system. In *Advances in Computing and Information Technology*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 367–379.

80. Huang, Y.; Geng, X.; Whinston, A.B. Defeating DDoS attacks by fixing the incentive chain. *ACM Trans. Internet Technol. (TOIT)* **2007**, *7*, 5–es. [CrossRef]
81. Douligeris, C.; Mitrokotsa, A. DDoS attacks and defense mechanisms: Classification and state-of-the-art. *Comput. Netw.* **2004**, *44*, 643–666. [CrossRef]
82. Mankins, D.; Krishnan, R.; Boyd, C.; Zao, J.; Frentz, M. Mitigating distributed denial of service attacks with dynamic resource pricing. In Proceedings of the Seventeenth Annual Computer Security Applications Conference (IEEE), New Orleans, LA, USA, 10–14 December 2001.
83. Johnson, B.; Laszka, A.; Grossklags, J.; Vasek, M.; Moore, T. Game-theoretic analysis of DDoS attacks against Bitcoin mining pools. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 3–7 March 2014; Springer: Berlin/Heidelberg, Germany, 2014.
84. Wu, S.; Chen, Y.; Li, M.; Luo, X.; Liu, Z.; Liu, L. Survive and thrive: A stochastic game for ddos attacks in bitcoin mining pools. *IEEE/ACM Trans. Netw.* **2020**, *28*, 874–887. [CrossRef]
85. 4 Key Cybersecurity Threats to New Central Bank Digital Currencies. Available online: https://www.weforum.org/agenda/2021/11/4-key-threats-central-bank-digital-currencies/ (accessed on 4 April 2022).
86. Abrazhevich, D. Classification and characteristics of electronic payment systems. In Proceedings of the International Conference on Electronic Commerce and Web Technologies, Munich, Germany, 4–6 September 2001; Springer: Berlin/Heidelberg, Germany, 2001.
87. Chaum, D.; Brands, S. Minting electronic cash. *IEEE Spectr.* **1997**, *34*, 30–34. [CrossRef]
88. Eslami, Z.; Talebi, M. A new untraceable off-line electronic cash system. *Electron. Commer. Res. Appl.* **2011**, *10*, 59–66. [CrossRef]
89. Wang, C.; Sun, H.; Zhang, H.; Jin, Z. An improved off-line electronic cash. In Proceedings of the International Conference on Computational and Information Sciences (IEEE), Shiyang, China, 21–23 June 2013.
90. Van Damme, G.; Wouters, K.M.; Karahan, H.; Preneel, B. Offline NFC payments with electronic vouchers. In Proceedings of the 1st ACM Workshop on Networking, Systems, and Applications for Mobile Handhelds, Barcelona, Spain, 17 August 2009.
91. Nigeria's OyaPay Now Integrates the Use of Bluetooth and QR Payments for Offline Use. Available online: https://innov8tiv.com/nigerias-oyapay-now-integrates-the-use-of-bluetooth-and-qr-payments-for-offline-use/ (accessed on 4 April 2022).
92. Visa Proposes CBDC Protocol That Lets Consumers Exchange Digital Cash via Bluetooth or NFC. Available online: https://www.nfcw.com/2020/12/18/369783/visa-proposes-cbdc-protocol-that-lets-consumers-exchange-digital-cash-via-bluetooth-or-nfc/ (accessed on 4 April 2022).
93. Dmitrienko, A.; Noack, D.; Yung, M. Secure Wallet-Assisted Offline Bitcoin Payments with Double-Spender Revocation. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '17), Abu Dhabi, United Arab Emirates, 2–6 April 2017.
94. China DC/EP Research and Perspectives of CBDC in Japan. Available online: https://www.nri.com/en/knowledge/publication/fis/special/lst/2020/07/07 (accessed on 31 January 2022).
95. Christodorescu, M.; Gu, W.C.; Kumaresan, R.; Minaei, M.; Ozdayi, M.; Price, B.; Raghuraman, S.; Saad, M.; Sheffield, C.; Xu, M.; et al. Towards a Two-Tier Hierarchical Infrastructure: An Offline Payment System for Central Bank Digital Currencies. *arXiv* **2012**, arXiv:2012.08003.
96. Wiseman, S.A. Property or currency: The tax dilemma behind Bitcoin. *Utah Law Rev.* **2016**, 417. Available online: https://heinonline.org/HOL/LandingPage?handle=hein.journals/utahlr2016&div=15&id=&page= (accessed on 11 April 2022).
97. Central Bank Digital Currency and the Future: Visa Publishes New Research. Available online: https://usa.visa.com/visa-everywhere/blog/bdp/2020/12/17/central-bank-digital-1608165518834.html (accessed on 4 April 2022).
98. Sabt, M.; Achemlal, M.; Bouabdallah, A. Trusted execution environment: What it is, and what it is not. In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Washington, DC, USA, 20–22 August 2015.
99. McGillion, B.; Dettenborn, T.; Nyman, T.; Asokan, N. Open-TEE—An open virtual trusted execution environment. In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Washington, DC, USA, 20–22 August 2015.
100. Jang, J.S.; Kong, S.; Kim, M.; Kim, D.; Kang, B.B. Secret: Secure channel between rich execution environment and trusted execution environment. In Proceedings of the NDSS, San Diego, CA, USA, 8–11 February 2015.
101. Busch, M.; Westphal, J.; Müller, T. Unearthing the {TrustedCore}: A Critical Review on {Huawei's} Trusted Execution Environment. In Proceedings of the 14th USENIX Workshop on Offensive Technologies (WOOT 20), Boston, MA, USA, 10–11 August 2020.
102. Weise, J. *Public Key Infrastructure Overview*; Sun BluePrints OnLine: Palo Alto, CA, USA, 2001; pp. 1–27.
103. Distributed Ledger Technology: Current Situation and Major Issues. Available online: https://www.bok.or.kr/viewer/skin/doc.html?fn=FILE_201803300855017061.pdf&rs=/webview/result/E0000654/201701 (accessed on 4 April 2022).
104. Execution is the Key to Success of CBDC Using Blockchain and DLT. Available online: https://www.thehindubusinessline.com/opinion/execution-is-the-key-to-success-of-cbdc-using-blockchain-and-dlt/article65207913.ece#comments_65207913 (accessed on 4 April 2022).
105. Bank of Korea Opens Bidding for CBDC DLT Technology Provider. Available online: https://www.ledgerinsights.com/bank-of-korea-opens-bidding-for-cbdc-dlt-technology-provider-won/ (accessed on 4 April 2022).
106. World Bank. *Central Band Digital Currencies for Cross-Border Payments: A Review of Current Experiments and Ideas*; World Bank: Washington, DC, USA, 2021.

107. World Economic Forum. *Privacy and Confidentiality Options for Central Bank Digital Currency*; World Economic Forum: Cologny, Switzerland, 2021.
108. Are Central Bank Digital Currencies (CBDCs) the Money of Tomorrow? Available online: https://www2.deloitte.com/ie/en/pages/financial-services/articles/central-bank-digital-currencies-money-tomorrow.html (accessed on 4 April 2022).
109. Löber, K.; Houben, A. *Committee on Payments and Market Infrastructures Markets Committee*; Bank for International Settlements: Basel, Switzerland, 2018.
110. Riksbank: DLT Tokens Don't Provide Cash-Like CBDC Benefits. Available online: https://www.ledgerinsights.com/riksbank-dlt-tokens-dont-provide-cash-like-cbdc-benefts/ (accessed on 4 April 2022).
111. Richards, T.; Thompson, C.; Dark, C. Retail central bank digital currency: Design considerations, rationales and implications. In *1. 1 Managing the Risks of Holding Self-Securitisations as Collateral 2. 11 Government Bond Market Functioning and COVID-19 3. The Economic Effects of Low Interest Rates and Unconventional 21 Monetary Policy 4. Retail Central Bank Digital Currency: Design Considerations, Rationales*; Australia; 2020. Available online: https://www.rba.gov.au/publications/bulletin/2020/sep/pdf/bulletin-2020-09.pdf#page=35 (accessed on 4 April 2022).
112. Central Bank Digital Currencies: System Design and Interoperability. Available online: https://www.bis.org/publ/othp42.htm (accessed on 11 April 2022).
113. Offline Payments Eliminate the Risk of Disruptions and Downtime. Available online: https://www.crunchfish.com/offline-payments-eliminate-the-risk-of-disruptions-and-downtime/ (accessed on 11 April 2022).
114. CBDC Technology Considerations. Available online: https://www.weforum.org/reports/digital-currency-governance-consortium-white-paper-series/cbdc-tech-considerations (accessed on 11 April 2022).
115. CBDC-Powered Offline Payment Systems—A True Rival to Cryptocurrencies? Available online: https://rafaelbelchior.medium.com/cbdc-powered-offline-payment-systems-a-true-rival-to-cryptocurrencies-38d13b5d3767 (accessed on 11 April 2022).