Print Your Own Money: A Cash-Like Experience for Digital Payment Systems

YE WANG, ETH Zurich
YU CHEN, ETH Zurich
SHENYI WANG, ETH Zurich
CHENHANG ZHOU, Nanyang Technological University
XIAOCHEN ZHENG, ETH Zurich
ROGER WATTENHOFER, ETH Zurich

Digital money is getting a lot of traction recently, a process which may accelerate even more with the advent of Central Bank Digital Currency (CBDC). Digital money has several disadvantages: Payments are difficult or outright impossible in emergency situations such as the failure of the electricity grid or Internet. CBDC may also be difficult to handle for children, the elderly, or non-resident travelers.

To overcome these problems, we design a cash-like CBDC experience. Our design process has three stages: interviews, system design, and system tests. Based on the interviews, we design and implement a CBDC component which is physical and offline. We then test our system for usability.

We discuss a spectrum of trust levels to allow for offline payments and argue that our system can handle emergencies and exceptional situations for digital payments.

ACM Reference Format:
Ye Wang, Yu Chen, Shenyi Wang, Chenhang Zhou, Xiaochen Zheng, and Roger Wattenhofer. 2021. Print Your Own Money: A Cash-Like Experience for Digital Payment Systems. 1, 1 (April 2021), 15 pages.

1 INTRODUCTION

Money and payments have changed their form many times in history. Currently we are witnessing yet another transition, from cash (banknotes and coins) to digital currency (payment apps and other forms of digital payments).

While this transition is happening everywhere, we can learn most from countries that are at the forefront of this development. In Sweden or China for instance, digital payments are already so predominant that many shops have stopped accepting cash [1, 27]. In a study by the Swedish Retail and Wholesale Council, more than half of the retail businesses expect to not accept cash after 2025 [1]. In the last years, bank branches and ATMs have been vanishing in Sweden [25]. It seems now a matter of time until Sweden will essentially be cash free. Note that if cash is not used on a regular basis, its security will be in jeopardy: People will not recognize the security features of rarely seen banknotes, and hence their trust in banknotes may suffer. Once cash is at this stage, it will not be produced anymore, since the production and logistics costs of cash are high. We believe...
that cash may be disappearing surprisingly quickly. First in countries like Sweden, then in other parts of the world [27].

Digital currency can have several forms. Digital currency could either be issued by companies, e.g., Facebook’s Diem project. Even more likely, our future money will be Central Bank Digital Currency (CBDC). Many central banks are already pushing ahead with the development of CBDC [7]. In Sweden, it is known as the e-krona [26], in Uruguay, the digital peso [15], and in China DC/EP, short for Digital Currency Electronic Payment [16, 18].

CBDC is a digital currency issued by a country’s central bank [4, 6]. The philosophy of CBDC is remarkably similar to that of cash. The user experience of CBDC will be akin to payment apps or credit/debit cards. Payments will be contactless, and transfers between private individuals will be possible. The majority of central banks believe that CBDC will eventually be available to the public, and more than 75% of central banks have already been engaging in CBDC work [7].

However, the world of CBDC is not without trouble. One technically challenging point is how money can be transferred in an emergency situation, for instance if the electricity grid or the Internet is not available. In such a unique scenario, transactions should still be possible. Bona fide handling of transactions in emergency situations would potentially enable a fraudster to spend the same money twice with a manipulated smartphone. Such a combination of circumstances would be rare, but important to consider before rolling out CBDC [27]. Another issue with CBDC is that everybody participating in the system needs to have a CBDC account. This may be an issue for children, the elderly, or possibly non-resident travelers. These examples show that a backup plan is necessary. As argued above, cash cannot come to the rescue.

In this paper, we design a cash-like CBDC experience. Our design process has three stages: interviews, system design, and system tests. First, we conducted 15 interviews in China, where digital payment systems are predominant, to acquire insights into how a CBDC system should satisfy their different needs. Based on these interviews, we developed a prototype CBDC system. Finally, we tested the prototype’s performance on four different devices and invited six users to experience it in different simulated scenarios. We collected and analyzed the problems the test users encountered during the test session. We discuss their perception of our new money system.

More precisely, in this paper we propose a system where you can print your own money. We mean this quite literally: You print some QR code on a piece of paper (or any other physical media), which is then the physical equivalence of digital money. We can increase trust and handling by (additionally) using NFC technology.

Self-printed cash can be accepted in transactions through digital payment systems. Our system has two main advantages: first, it serves people who do not necessarily have accounts. Children, the elderly, or travelers can use self-printed money to access financial services supported by digital payment systems; second, people can conduct transactions offline in emergencies. In some sense, our proposal gets close to what economists call token-based digital money (instead of account-based digital money), since a payee is able to verify the validity (genuine and unspent) of the payment token [9]. To the best of our knowledge, we are the first to suggest such a form of printable digital money to accommodate the different social needs.

2 BACKGROUND

2.1 Central Bank Digital Currency

Digital money issued by central banks is not a new concept. It has been proposed since 1985 [2, 28]. However, there was no clear framework and technical support for promoting CBDC in the 1990s. With emerging blockchain technologies in the last decade [8, 11, 17, 19], central banks got a blueprint to develop and promote CBDC [3].
By 2020, 60% of central banks have conducted CBDC experiments or proofs-of-concept, while 14% are moving forward to development and pilot arrangements [7]. China is one of the leading countries in CBDC and has released many details of the DC/EP system to the public [16]. The frontend of DC/EP is similar to the frontend of a payment app such as AliPay. Payments are contactless, and transfers between private individuals are made directly between their smartphones.

On top of providing an official digital payment system supported by the central bank, the People’s Bank of China considers DC/EP equivalent to cash [31]. To enable transactions without network services, two solutions of offline payments have been proposed [32, 33]. The first one [32] uses Near Field Communication (NFC) technology and Bluetooth to construct a communication channel between payer and payee. Digital currency chips are required for transaction terminals, which have the strong anti-cracking ability. The chip can verify the authenticity of digital currency and the legality of transactions without permission from the system. The second proposal [33] does not require additional hardware. The payment’s authorization is ensured by the user identification, the public key, and the digital certificate of the user. The transfer information is recorded in the transaction ledger after one of two parties rejoins the system. The recipient can use the money as an input of a transaction after the confirmation of the transaction from the system.

Previous solutions only consider transactions without network services, while both payers and payees have to register for the system and keep digital devices. However, this is not the only scenario where offline payment is necessary. In this paper, we study people’s perceptions of different forms of money, i.e., in which scenarios and why they use cash and digital payments. Our digital payment system aims to enable all social groups to access financial services and meet their needs in different scenarios as far as possible.

2.2 Digital Money and Cash

There is a growth of HCI work concerning the interactions between digital money and people. Kumar et al. [14] studied a variety of payment situations in India to inspire the design of digital payment systems. O’Neill et al. [22] considered how different payment methods impacted the loan collection work in India. They suggest that it took considerable work to make digital payments usable. Pal. [23] studied the cash-banning demonetization event in India. Cash shortage enforced the adoption of digital payments to some extent, but the usage of digital payments dropped again after new banknotes became available. Pritchard et al. [24] studied the drivers’ and passengers’ reactions when cash payment was replaced by Oyster, a digital card payment, on London buses. The lack of information and communication led to both parties’ negative impacts even though being cash-free actually has benefited the public. Shen et al. [27] reported that after digital payments becoming predominant in China, cash became not acceptable in many daily retail scenarios. However, in China cash is still used in some scenarios.

These studies have been predominantly qualitative and stop at understanding the defects of current digital payment systems [27]. Fewer studies have utilized these inspiring findings to improve the existing systems or design new systems to address the challenges of digital payment systems.

To fill this gap in the literature, we utilize qualitative findings to design a new digital payment system in the context of CBDC. Our work provides a prototype implementation that should be compatible with any form of digital payment system.

2.3 Design of Payment Systems

By observing the difficulties for people who are over eighty years old to use digital payments in the UK [30], Vines et al. [29] explore the design of preserving and augmenting the paper check for digital payments. They invited 16 eighty-somethings to participate in design workshops and experiment with two designs called community and digital check.
The community check is designed as pre-paid certification. People pay the community check (a special designed checkbook) to merchants, and merchants send the check along with their bank account information to the issuer of the community check. When the issuer receives a check from a merchant, the issuer will transfer the money to the merchant. This is very different from our design, where the money of a payment is immediately transferred to the merchant, without involving a third party.

Their digital check is a set of special papers and pens with a camera and Bluetooth. The pen will capture the information written by users and send it to the bank through a computer. Users can make digital payments by signing the specially designed check physically. This is also very different from our design, as it needs much more technology. So while some of the goals of Vines et al. [29] are similar to ours, both their implementations are divergent.

Our design also supports both physical and digital forms of payments, and the two approaches can be combined. When a payment method fails, users can easily convert to the other form of money with a personal device. Our system does not rely on special devices and objects. Users can print cash with any digital devices on paper or other media, which ensures generality (anyone who has digital devices can easily print money) and reduces the cost (no need to buy additional equipment). Moreover, users can conduct offline payments without access to a device, while payees are not necessarily connected to the Internet.

3 OUR APPROACH

We aim to understand the upcoming problems people might encounter using different payment methods in daily life with the development of CBDC. Therefore, we conducted interviews in China where digital payment systems have been widely accepted by society. On top of the physical, digital, and social ubiquity, and technical, social, and interoperability challenges of digital payments reported by Shen et al. [27], we would like to explore more scenarios and summarize reasons for different payment preferences.

A total of 15 users have participated in our study. All of them have experiences with both cash and digital money. There are seven female participants and eight male participants. Eleven participants are between 18 and 50 years old, and four participants are between 50 and 60. We conduct semi-structured interviews with participants from June 2020 to October 2020 and follow an interview guide, ensuring consistency across participants. The following questions are investigated during each interview:

- What payment methods do you use in different scenarios?
- Why do you choose this payment method?
- Why don’t you choose other payment methods?
- What challenges do you have when using different payment methods?

After interviews, we use an open coding method [10] to analyze our interview data. We consider the payment scenarios into four categories: cash-only, cash-preferred, digital-preferred, and digital-only, and discuss why people accept payment methods with different levels in these scenarios. We compare our findings with previous studies and figure out the main principle for our system design: keeping both digital and physical presentations of money in the system and optimizing the conversion between these two forms of money. Furthermore, we consider the main challenge of digital payment systems: offline payments.
## Scenarios | Reasons
--- | ---
Cash-only | Payees only accept cash  
Some groups are unable to use digital devices/payments  
Cash has special meaning in traditional cultures  
No signal or no power to the digital device
Cash-preferred | Receive cash from others and do not want to keep it  
Cash helps with financial management (knowing exact amount)  
Extra discount when using cash  
No transaction fee
Digital-preferred | Be scared of sanitation of cash  
Avoid managing cash with different size, weight, and amount  
No change required  
Only need to carry a single device
Digital-only | Remote transactions  
Payees only accept digital money

Table 1. Reasons for people to choose payment methods under different scenarios.

## 4 COMPATIBILITY OF CASH AND DIGITAL MONEY

We start with understanding people’s preferences on payment methods in different scenarios (Table 1). Most of our interviewees prefer digital payments after they get used to them. However, digital payments still fail in many scenarios, resulting in cash transactions.

The first reason of using cash is usability. Compared to digital payments, anyone who can perform basic computations can quickly learn how to use cash. People do not need to learn how to use an additional device or register with banks and other financial companies to enable cash payment. There are no entry barriers: Children without income and older people who are not familiar with mobile devices can use cash easily. Therefore, when handling transactions with older people, some interviewees prefer using cash: “I give cash to the elderly in my family as their living expenses. They do not have an Alipay account and do not use smartphones. Cash is the only payment method that they may use.” (P8, Male, 42)

The same situation arises when parents deal with financial activities related to their children. They are more resistant to supporting their children to use digital payments. Even for college students, the majority of them do not hold any debit/credit cards [20, 21]. One of our interviewees considers that his children are too young to manage their money, so he has not let them use digital payments: “Usually we pay directly for anything they need, but occasionally we give them some cash as pocket money.” (P15, Male, 51)

Furthermore, cash sometimes represents more than just money. As a general equivalent, cash can be used not only to measure the value of goods, but also to exchange various commodities. In ancient times, people presented a higher purpose of faith by offering sacrifices. Then, with the continuous development of religion, the form of worship has undergone some changes. It is integrated into modern society, so some people will choose other ways to show their piety. In some Buddhist places in East Asian countries, such as Japan and China, some believers will offer incense money [5, 13] in cash to express their blessings. Cash is not used as an object of transactions, but as a store of value [34], which is the same as an oblation: “I only bring cash when I go to the temple to pray. I put some money into the merit box every time.” (P4, Female, 18) In many countries' traditional cultures, cash also serves as a gift, carrying blessings. In China, people will put money in red envelopes to give to the elders and children as New Year money when the New Year comes. Therefore, many interviewees indicated that they keep using cash in these scenarios: "When we
People sometimes behave as a payee of cash, or receive change from merchants [14]. In such scenarios, people may consider using cash as soon as possible, which increases the cash flow in society: "I hate keeping cash. It’s very troublesome. I especially don’t like the pile of coins that are not convenient to carry. If my friends give me cash after I pay the bill or bring something to them, I will first use cash in my next payment." (P7, Female, 31) We further ask her why she does not deposit the money in her bank account and then use them digitally. She considers it is not worthwhile to go to a bank to deposit small amounts of cash: "There is no need to go to the bank just for a few dollars."

Moreover, as the findings reported by Shen et al. [27], we also find that people struggle with the current system because they cannot easily choose the payment method they want. For example, if the users do not want to use cash, but the merchant only accepts cash, the users must go to banks to withdraw cash before the transaction or give up such a transaction. If the users are accustomed to using cash but the merchant does not have change or only support digital payments, then the users cannot complete the transaction.

These qualitative findings spark design ideas of our digital money system. We admit that cash, or the physical form of money, is necessary for the current money system. Therefore, in our digital money system, digital money should also be possibly represented physically. Moreover, we should optimize the current process of conversion between digital money and cash. In such cases, cash can be accepted by digital systems, while people can get cash easily from their digital accounts if necessary.

5 CONVERSION BETWEEN DIGITAL MONEY AND CASH

With the design principle in mind, we first sketch some basic ideas of how users can interact with the system (Figure 1). For example, when users want to use cash in a digital system, the payees can take a picture with the mobile phone to deposit it; or when users want to get some cash, they do not have to go to a bank or ATM but just print it by themselves.

To realize this design idea, our system needs to accomplish two requirements. First, the mobile phones (digital devices) can collect the information of cash and verify the authentication of the cash. Second, after the payee confirms the transaction, the original cash should be invalid and cannot be used again. We outline the process of generating cash and depositing cash in Figure 2. Each piece of cash has its own unique number and value and has been recorded in the system when
the user claims such a cash generation. The authentication of the cash can be then verified in the system and the information of the cash will be deleted after the verification.

Traditional cash is standardized in terms of its size, weight, and design, made of rigid and light-density material such as polymer or paper. People distinguish the authenticity of cash by their own experience of its physical properties. However, to ensure the generality of the CBDC system, we do not require the form, material, and presentation of the cash. Any cash that contains valid information can be verified in the system. Therefore, there is a risk of double-spending, while users can directly copy the information on the cash and generate a new one with the same information. Since we have no requirement for the physical material of the cash, we use asymmetric cryptography to ensure financial security.

Figure 3 shows the process of printing a physical cash from a digital account. When users want to print money, the local device will first generate a pair of asymmetric keys, i.e., a public key (pk) and a private key (sk) for the cash and send the user id, pk, and the value of the cash to the server. The server will verify the user identity like other digital payment systems and check whether the user has enough balance to generate such cash. If the user has enough money to generate the cash, the system will subtract the value from his account, create a unique identity for the cash, and store the information of the cash in the system, including its value, its pk, its creator, and its identity. The system will send back the cash identity to the user, indicating the success of generating such cash.

After receiving the cash identity, users can print the information (cash identity and private key) on paper (such as QR code) or in other physical medium (such as NFC tag). Figure 5 shows an
example of cash, which contains the identity and a private key. Payees who receive the cash can verify and deposit it in their own accounts.

Figure 4 shows how users redeem money into their digital accounts when they receive cash. Valid cash contains two information, i.e., the identity and the corresponding private key. The payee will first encrypt the payee’s id by the private key as ciphertext and send it to the server with the cash identity. Then, the server can use the cash’s public key to verify the redeem request’s validity. If the plaintext matches the payee’s identity, then the system will increase the payee’s account balance and invalidate the redeemed cash in the system.

6 OFFLINE PAYMENTS

The system we proposed in the previous section aims to solve the incompatibility of cash and digital money with in our CBDC system. However, the system still relies on online verification - although payers can use the printed cash to conduct the payment offline, payees still need to communicate with the online server to verify the cash.

This challenge has been discussed in previous studies [27]. DC/EP only considers that both payers and payees still keep their digital devices during offline transactions. However, as we have shown in Section 4, offline payment is also important in the scenarios where payers only have cash, i.e., the self-printed money, as some payers do not have access to digital devices, like children and the elderly.

Therefore, we consider addressing this challenge with merchant pre-authorization systems. In merchant pre-authorization systems, users will determine the merchant before making an offline payment. The server will generate such a merchant-specific cash in advance, and the cash can only be used at the specified merchant. Meanwhile, the merchant can verify the validity of the printed offline, demonstrating an offline payment scenario for both consumers and merchants.

The system generates a pair of asymmetric keys for each merchant. The system keeps the private key for generating the merchant-specific cash and sends the corresponding public key to the merchant. Merchant can verify the validity of the merchant-specific cash for offline payments using the public key.

Figure 6 shows how the system generates merchant-specific money. On top of generating the cash identity, the system will also encrypt the cash information with the private key of the merchant. Then the merchant is able to the public key to verify whether the cash is generated through the system. To make sure that this cash can only be spent by the user who prints the money, the system
will encrypt the message with the public key of the cash generated by the user. Users print the ciphertext \( C_t \) and the private key of the cash.

Figure 7 shows the process of receiving a merchant-specific cash. The merchants will first verify the cash’s validity with the private key of the cash provided by the consumer and the public key of themselves to make sure that the cash is generated with enough balance to pay the bill. After reconnecting to the network, merchants can submit all the cash they receive from users during the offline period, and the system will process all payment requests at that time.

The key pair of each merchant can update regularly. If users want to revoke the printed money for a specific merchant, they just need to wait until the merchant changes the key pair or the merchants to be online and verify the money has not been spent. Then the old cash is not valid anymore, and users can withdraw the money back to their own accounts.

In current businesses, offline verification for merchants only occurs in extreme scenarios, especially in countries and cities where infrastructure is well developed. Moreover, we suggest that merchants may regularly update the pair of keys to ensure that attackers cannot hack the private keys to generate cash.

Moreover, if merchants do not trust the central system, i.e., the central bank, they may also establish a white-list of users. Only users with sufficient creditworthiness can generate merchant-specific cash. If a user is found to have falsified after online verification, the merchant can more easily trace the person responsible.

7 EXPERIMENTAL STUDY

Our prototype system can not be tested in real scenarios easily. It is hard to embed our system with the current money system without the permission of governments. Therefore, at this stage, we test our system in the laboratory. We focus on the system’s usability: Can this system bring convenience to users? Can this system solve the problems that users encounter in real life? What do users think of this new cash system? How do they feel when testing it?

Our experiments are held in two phases. In the first phase, we test the performance of our system under different payment scenarios. In the second phase, we invite users to complete the same payment tasks as in the first phase.

7.1 System Performance

In our prototype system, we consider two presentations of cash, i.e., printed QR code and NFC tag. Even though we have purchase the materials at retail stores, the cost (0.035 CNY and 0.42 CNY per note, respectively) is much less than the production cost of cash [12], which demonstrates that our system can be an appropriate substitute to current money system from the perspective of cost for central banks. A blue-tooth printer is used to print QR codes. The capacity of each NFC chip is 888 bytes.

We test our system performance with four different Android phones released between 2015 and 2020. We design six tests for measuring how the system performs under different payment scenarios.

- **Test 1**: Print five $10.0 in QR mode.
- **Test 2**: Receive one $10.0 with a QR code.
- **Test 3**: Print one $10.0 in NFC mode.
- **Test 4**: Receive one $10.0 with NFC.
- **Test 5**: Print one $10.0 in QR+NFC mode.
- **Test 6**: Offline verify one $10.0 in QR+NFC mode.
(a) Print cash with HUAWEI P20 through the blue-tooth printer.

(b) Write information into a NFC tag touch to the printed money.

(c) Scan the QR code to read the information on the printed money.

(d) Read the information stored in the NFC tag on the printed money.

Fig. 8. Examples of testing our prototype system with HUAWEI P20.

One of our researchers tests the system with four different Android devices (Figure 8), launched between 2015 to 2020. Each test has been conducted six times on every device. We take the average performance of each test and list it in Table 2. Each printing money operation with a single printer or a single NFC tag takes around 10 seconds, while if we use both paper and NFC tag to store the information of the money, it takes 15 seconds to print each money. When converting printed physical money to digital money, it takes users 10 seconds for the cash stored with a single material and 15 seconds for the cash in both QR code and NFC tag. Meanwhile, the process of making changes and offline payment validation does not consume additional time. Despite the different performance of the Android devices, the processing speed of our prototype system does not variance a lot. We can infer that our system can be adapted to different Android devices and has a relatively stable speed, which is much faster than the current conversion between cash and digital money (go to a bank/ATM for deposit or withdrawal operations).

7.2 User Experiments

After measuring the system performance, we invite six users to participate in our system design (4 female and 2 male, age from 20 to 32). Because of the COVID-19 situation, instead of inviting testing users to come to our lab, we deliver the system equipment (HUAWEI P20, blue-tooth printer,
Table 2. Performance of four Android devices on six tests on average. Each test has been conducted six times on every device.

| Test (sec) | MI 10  | HUAWEI P20 | RedMI K30 Pro | HUAWEI Mate 8 |
|------------|--------|------------|---------------|--------------|
| Test 1     | 41.21  | 35.45      | 38.63         | 40.79        |
| Test 2     | 12.28  | 8.67       | 10.12         | 11.19        |
| Test 3     | 12.45  | 13.22      | 11.83         | 16.22        |
| Test 4     | 6.84   | 8.16       | 11.05         | 9.70         |
| Test 5     | 14.82  | 18.02      | 14.72         | 17.55        |
| Test 6     | 12.16  | 18.88      | 16.95         | 17.14        |

Table 3. User experiments with HUAWEI P20.

| User (sec)   | 1    | 2    | 3    | 4    | 5    | 6    | average |
|--------------|------|------|------|------|------|------|---------|
| Test 1       | 42.12| 54.91| 65.05| 39.2 | 43.22| 46.4 | 48.48   |
| Test 2       | 10.43| 6.59 | 6.07 | 20.29| 11.4 | 6.52 | 10.22   |
| Test 5       | 19.06| 25.52| 25.45| 11.91| 46.62| 19.05| 24.60   |
| Test 6       | 17.6 | 37.9 | 27.89| 36.46| 48.66| 24.83| 32.22   |

and NFC tags) to each user and test the system in their familiar environment (e.g., home, office). We keep in contact with them through real-time video calls and record the conditions they encounter during the test.

During the testing session, users first read the instructions of the system. Then, they can try out the systems and ask questions to the researchers. Next, we asked the users to complete the four tests (test 1, 2, 5, 6) in Section 7.1, which cover all functionality of our system. We record the testing process and collect the testing issues. Finally, we discuss with them their feelings about our money system.

After a total of 15 minutes of reading and familiarizing themselves with the system, users independently complete the tests with the system. Their using time of each test is listed in Table 3.

7.3 Technical Challenges

Compared to our system performance tests with experienced users, the first-time users show a good understanding of the new system. We find two main challenges through our observation of the testing process: network connection and NFC practice.

Except for test 6, which is conducted offline, the remaining four tests require network connections during the testing period to send and receive messages with the server. Some users experience a long testing time (User 5, Test 5) because of the internet connecting issues. In fact, users consider this problem can be easily solved by moving positions. However, if the network interrupt happens when the merchant receives the money, it will greatly influence the business’s efficiency. Therefore, all users consider the offline payment design is useful in daily life, and they have not felt any inconvenience.

Another challenge for users is the NFC practice. In THE user study, all devices are provided by researchers, so users may feel that they are not familiar with the NFC practice. Different devices sense the signal from the NFC chip with a different part of the devices. Users 2, 4, and 5 encounter the failures of NFC write and read due to improper operations in Test 5 and 6. Since we only require one NFC read and write during the entire process for each cash, users are able to complete the test successfully after re-familiarizing themselves with the device. Meanwhile, our system ensures that
even though failures of NFC operation happen, users can still process the payment with a second attempt.

7.4 Loss or Theft
The most significant concern about our system from testing users is security. Several users (1, 2, 3, 4, 6) are curious about recovering the money after a loss or theft, and how to track thieves.

Our new money system has a remedies plan in case of cash stolen. The system allows users to destroy the cash they print, if it has not been used. The money will then go back to the users’ accounts, ensuring that thieves cannot use the cash anymore.

It is undeniable that the risk still exists if the thieves use the money before the users destroy the cash. However, we argue that our system is not more vulnerable than the traditional cash system. First, people also face the risk of losing cash or have cash stolen in the current money system. Because the cash in our system can be easily converted to digital accounts, users do not need to keep cash for a long time. In addition to the cash’s basic information, users can also make additional authentications of the people who pay with the cash, such as appearance, bio information, and other identity information. In such a case, attackers cannot use the money directly. Moreover, since the cash system is anonymous if cash is lost or stolen, it is almost impossible for users to trace the money flow of their lost money. In our system, each cash’s usage history is through the central system, making it possibly better to track the flow of lost or stolen money.

7.5 Usability Challenges
Another concern mentioned by testing users is managing change money. In our qualitative study, participants also mentioned that in retail scenarios, almost surely, the cash value does not perfectly match the money that payers have to pay to the merchants. Based on different user preference, we consider two possible mechanism.

First, User 3 wants to keep the cash as the change. The most intuitive solution is to generate a new cash by the merchants. The newly printed cash is considered as the credential of the money change. However, such a mechanism has pitfalls of security. Both the merchant and the consumer have the identity and the private key of the cash. Therefore, there is a possibility that the merchant embezzles the money. We discuss this security issue with User 3, and he does not consider it a big problem for him. Because the system has a record of the cash generation and deposit, he does not worry too much about the merchant stealing the money. He also said that he would prefer to use such a mechanism at a large and trusted merchant.

Another mechanism is designed to solve the problem proposed by our interviewees that they do not want to manage small change. Rather than generating new cash, the change money will directly return to the user’s digital account. If the total value of paid cash is equal to or larger than the total amount of the bill, then the system will deposit the bill’s amount in the merchant accounts and return the change to the account which creates the cash. This solution addresses not only the inconvenience when carrying large amounts of small change but also the security issue of the first mechanism. However, this mechanism is not suitable for offline payers who want to use the change money to conduct a second-round payment. Such a system may change how people prepare cash: instead of considering the total amount they might use, people should consider the number of times they use money.

8 SECURITY LEVELS
During our design process, we find that the most critical issue for money systems is how to convince a payee to accept a payment. In an online scenarios (with access to the Internet), a payee can
directly verify the validity of a payment. The difficulty of the design is in an offline scenario. We provide a spectrum of trust levels to allow for offline payments:

- **On the most basic level**, the QR code represents money sitting in the account of the payer. Whoever scans that QR code first, will be the receiver of the money. Today’s physical equivalent is a personal check. It may be okay for a relative to give a child a (decorated) personal check as a present, since the relation between payer and payee is strong, and as such trustful. If the check fails to be cashable, the parents may have a word with the relative that gave the check. Even a retail store may accept such a form of payment, if the payer is a well-known return customer. One may carry such a personal check along for emergency situations, possibly simply in an NFC enabled application like Google pay, or in printed form.

- **On the next higher security level**, the paying account is not a personal account, but it belongs to a trusted third party such as a commercial bank. Today’s physical equivalent is a banker’s check. A retail store may accept such a banker’s check even if the customer is unknown, as it is guaranteed to be valid by the bank that issued the check. A fraudulent customer may copy such a banker’s check in an attempt to double spend. However, the issuing bank will go after such a fraudulent customer the same way it does already today. Moreover, such a check could be difficult to copy by having some printed security elements, similarly to banknotes today. Banks may be willing to issue digital money in the form of such banker’s checks as a business. In contrast to banknotes, such a banker’s check will be more secure: If we are in an emergency situation, the validity of such a check can be verified simply by caching the check.

- **There is an even more secure level**: this is known as colored money in the cryptocurrency world. Today’s physical equivalent is a gift card of a particular store. The idea is that the money is printed such that there is only one possible receiver, for instance a retail store. In this case, the retail store can be sure that there is no double spend, as the store is the only possible receiver for the money. In some sense, the money was already promised to the store when being printed, the customer only waits for an opportunity to spend it. In contrast to today’s gift cards, colored money can be reverted back into the payer’s account.

We believe that these three trust levels should handle all emergencies and exceptional situations that we learn from qualitative studies. Our system is able to handle these levels, and possibly others.

9 CONCLUSION

This paper considers upcoming challenges coming with the development of digital payments. When central banks are promoting and developing digital payments, how should we design the central bank digital currency systems to enable all social members to access financial services as much as public utility access?

We start with the existing experiences from countries where digital payments have been widely accepted and propose three design principles of our digital payment systems: keeping both digital and physical presentations of money, enabling convenient conversion between two presentations, and supporting offline payment. We implement and test our prototype system on different devices for different scenarios and discuss their skepticism with users. Our work is a pilot study of digital money systems in the context of CBDC and potentially will inspire implementations of CBDC design of central banks.

REFERENCES

[1] Niklas Arvidsson, Jonas Hedman, and Björn Segendorf. 2018. När slutar svenska handlare acceptera kontanter. Handelsrådet, Forskningsrapport 1 (2018).

[2] Bank for International Settlements. 1996. Implications for central banks of the development of electronic money. Bank for International Settlements.
Christian Barontini and Henry Holden. 2019. Proceeding with caution-a survey on central bank digital currency. *Proceeding with Caution-A Survey on Central Bank Digital Currency* (January 8, 2019). BIS Paper 101 (2019).

Morten L Bech and Rodney Garratt. 2017. Central bank cryptocurrencies. *BIS Quarterly Review September* (2017).

Harumi Befu. 1968. Gift-giving in a modernizing Japan. *Monumenta Nipponica* 23, 3/4 (1968), 445–456.

Ole Bjerg. 2017. Designing new money-the policy trilemma of central bank digital currency. (2017).

Codrula Boar and Andreas Wehrli. 2021. Ready, steady, go?: Results of the third BIS survey on central bank digital currency. (2021).

Vitalik Buterin et al. 2014. A next-generation smart contract and decentralized application platform. *white paper* 3, 37 (2014).

Benoît Coeuré and Jacqueline Loh. 2018. Central bank digital currencies. *Committee on Payments and Market Infrastructures BIS Report* (2018), 34.

Christian Decker and Roger Wattenhofer. 2015. A fast and scalable payment network with bitcoin duplex micropayment channels. In *Symposium on Self-Stabilizing Systems*. Springer, 3–18.

Federal Reserve Board. 2020. 2020 Federal Reserve Note Print Order. https://www.federalreserve.gov/faqs/currency_12771.htm [Online; accessed 06-April-2020].

Hill Gates. 1987. Money for the Gods. *Modern China* 13, 3 (1987), 259–277.

Deepti Kumar, David Martin, and Jacki O’Neill. 2011. The times they are a-changin’ mobile payments in India. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 1413–1422.

Gerardo Licandro. 2018. Uruguayan e-Peso on the Context of Financial Inclusion. *Banco Central del Uruguay, November 16* (2018).

Michael. 2020. China’s National Digital Currency DCEP / CBDC Overview. https://boxmining.com/deep/ [Online; accessed 29-July-2020].

David C Mills, Kathy Wang, Brendan Malone, Anjana Ravi, Jeffrey Marquardt, Anton I Badev, Timothy Brezinski, Linda Fahy, Kimberley Liao, Vanessa Kargenian, et al. 2016. Distributed ledger technology in payments, clearing, and settlement. (2016).

Changchun Mu. 2019. DC/EP is ready to use a two-tier operating system. Remarks by Changchun Mu at China Finance 40 Forum, Yichun, China.

Satoshi Nakamoto. 2019. *Bitcoin: A peer-to-peer electronic cash system*. Technical Report. Manubot.

Jill M Norvilitis and Michael G MacLean. 2010. The role of parents in college students’ financial behaviors and attitudes. *Journal of economic psychology* 31, 1 (2010), 55–63.

Jill M Norvilitis and Yingmei Mao. 2013. Attitudes towards credit and finances among college students in China and the United States. *International journal of psychology* 48, 3 (2013), 389–398.

Jacki O’neill, Anupama Dhreshwar, and Srijhari H Muralidhar. 2017. Working digital money into a cash economy: The collaborative work of loan payment. *Computer Supported Cooperative Work (CSCW)* 26, 4-6 (2017), 733–768.

Joyojeet Pal, Priyank Chandra, Vaishnav Kameswaran, Aakanksha Parameshwar, Sneha Joshi, and Aditya Johri. 2018. Digital payment and its discontents: Street shops and the Indian government’s push for cashless transactions. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–13.

Gary Pritchard, John Vines, and Patrick Olivier. 2015. Your money’s no good here: The elimination of cash payment on London buses. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 907–916.

Richard Orange. 2019. Sweden: how cash became more trouble than it’s worth. https://www.theguardian.com/money/2019/mar/09/sweden-how-cash-became-more-trouble-than-its-worth [Online; accessed 09-March-2019].

Sveriges Riksbank. 2017. The Riksbank’s e-krona project–Report 1. *E-krona reports* (2017).

Hong Shen, Cori Faklaris, Haojian Jin, Laura Dabbish, and Jason I Hong. 2020. ‘I Can’t Even Buy Apples If I Don’t Use Mobile Pay?’ When Mobile Payments Become Infrastructural in China. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 1–26.

James Tobin. 1985. Financial innovation and deregulation in perspective. *Bank of Japan Monetary and Economic Studies* 3, 2 (1985), 19–29.

John Vines, Mark Blythe, Paul Dunphy, Vasilis Vlachokyrilos, Isaac Teece, Andrew Monk, and Patrick Olivier. 2012. Cheque mates: participatory design of digital payments with eighty somethings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1189–1198.

John Vines, Paul Dunphy, Mark Blythe, Stephen Lindsay, Andrew Monk, and Patrick Olivier. 2012. The joy of cheques: trust, paper and eighty somethings. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work*. 147–156.

Wikipedia contributors. 2020. Renminbi — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Renminbi&oldid=967027927 [Online; accessed 15-July-2020].
[32] Qian Yao, Huifeng Li, Xinxiang Wen, Liansan Li, Dongbing Wang, Hao Liu, Xin Zhao, Xiaoxue Tang, and Wenshu Liu. 2017. The method and system of offline electronic payment are carried out using digital cash chip card. CN107230079A.

[33] Chuanhui Zan, Xu Wan, Chengzhan Song, and Yanu Liang. 2019. Offline payment method, terminal and agent delivery equipment based on digital currency. CN109493016A.

[34] Viviana A Zelizer. 1989. The social meaning of money:” special monies”. American journal of sociology 95, 2 (1989), 342–377.