Open Access Library Journal
2022, Volume 9, e9324
ISSN Online: 2333-9721
ISSN Print: 2333-9705

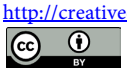
Realization Technology of Digital Currency Hubee

Xianghao Nan

CPK Laboratory, Beijing, China
Email: nanxianghao@bochtec.com

How to cite this paper: Nan, X.H. (2022) Realization Technology of Digital Currency Hubee. *Open Access Library Journal*, **9**: e9324.
https://doi.org/10.4236/oalib.1109324

Received: September 15, 2022
Accepted: October 22, 2022
Published: October 25, 2022



Abstract

The digital currency Hubee is an equivalent tool for all digital assets to provide a safe and convenient mobility and storage serve. Mobility (payment) or storage (settlement) of digital assets is easy to solve separately, even with traditional technologies, but when to solve both simultaneously, new technologies are needed. Therefore, in this paper, the necessary functions of digital currency are analyzed and discussed. The biggest technical difficulty in the design of digital currency is the authentication of the identifier claimed by the subject. As long as the identifier authenticity is solved, the subject and object authentication can be easily solved and a real digital signature can be realized. Until now, Identifier authentication technology is an international challenge. English-speaking countries separated the concept of identifier from the concept of identity only last year, but have yet to solve the problem of proving authenticity. On the basis of the Identifier authentication, a digital currency that is unified with payment and settlement currency and is not afraid of loss is realized. The currency does not need a wallet, and the account book does not need a Treasury, which can run in an unattended cloud bank. Hubee is an account-centered, non-centralized system that implements the information assurance policy of "my security is my decision". Hubee's scope can be controlled flexibly, it can be directly applied to a scope of a single commercial bank or a scope of a central bank, and can also be applied to different banks and commercial banks and different central banks in a way of mutual recognition. The appearance of Hubee and other digital money will break the traditional monetary management mode and create a new management mode adapted to the digital economy era.

Subject Areas

Information and Communication: Security, Privacy, and Trust

Keywords

Currency, Identity, Authentication, Bank

1. Introduction

The appearance of money gradually replaced barter and became an indispensable link for transactions. In the history of monetary development, various forms of equivalents have appeared from copper coins, paper currencies, electronic currencies, securities, electronic bills, etc. Flexible and diversified operation methods have also emerged, such as network payment, third-party payment, and user cheque issuance. Therefore, reference history provides a lot of referential experience in the study of digital currency [1].

Countries are developing digital currencies, of which there are more than 20, perhaps with different purposes and characteristics. However, in the era of digital economy, digital asset protection needs to address both mobile security and storage security. Mobility is bodied in payment, and storage is bodied in settlement. It is easier to solve mobile security and storage security separately, *i.e.* it can be solved by existing third-party signature technology and trust-based encryption technology. However, if the digital currency only applies to payment in circulation, digitalization will not have much significance, because the focus of digital asset protection is not on circulation such as payment, but on storage such as settlement. If Hubee wants to solve the mobile security and store security at the same time, it must get rid of the traditional trust logic, creating a new evidence-based truth logic to realize "one thing one proof" blocking any trust transfer, to provide proofs of authenticity, traceability, attribution, responsibility to make Hubee has a strong self-protection ability without being afraid of theft, further, to make the accounts are not afraid of theft, thus become a good digital asset protection tool.

2. Hubee's Core Technology

Hubee is composed of several authenticity proof items: firstly, the authenticity certificate of issuing bank's identifier must be solved; secondly, the relationship between issuing mechanism and anti-copy must be clarified; thirdly, the unification of payment currency and settlement currency must be solved.

2.1. Authenticity Proof of Issuing Bank's Identifier

2.1.1. Mapping of Identifier to Key-Pair

In CPK System [2], keys are generated by identifiers forming one to one mapping between keys and identifiers. CPK has a private matrix ($r_{i,j}$) and a public matrix ($R_{i,j}$). ($r_{i,j}$) is kept secret in KDC for private key generation, and the public matrix ($R_{i,j}$) is signed by KDC and published, so that everyone can calculate the public key. Its working principle is that the given identifier become to h pairs

matrix coordinates through the transformation of Hash function, and the indicated matrix variables are added to form keys. If the given identifier is Alice then

$$\mathrm{Hash}(\mathrm{Alice}) = (i, j)^h \rightarrow \begin{cases} \sum(r_{i,j}) = sk_{\mathrm{Alice}} \\ \sum(R_{i,j}) = PK_{\mathrm{Alice}} \end{cases}$$

where, the small slant sk_{Alice} represents the private key, and the large slant PK_{Alice} represents the public key.

2.1.2. Identifier Authentication

Identifier is the name that a subject claims, so the identifier authentication technique is the most direct way to prove the authenticity of the subject. The identifier authentication protocol refers DSS digital signature standard [3].

The identifier proof code s is the product of the random number k and private key sk_{Alice}:

$$s = k^{-1} sk_{\mathrm{Alice}} \bmod n \tag{1}$$

The identifier check code c is the product of random number k and the generator G:

$$k\mathrm{G} = (x, y); c = (x + y)^2 \bmod 2^{16}$$

The identifier authentication code is $\mathrm{IAC} = (s, c)$

Where, G is the elliptic curve generator, n is the order of the additive group. The length of c is limited to two bytes to shorten the signature length. Identifier authentication function is marked by $\mathrm{SIG}_{sk\text{-Alice}}(0) = \mathrm{sign}$

The Identifier verification code is the product of proof code and public key

$$s^{-1} PK_{\mathrm{Alice}} = k\mathrm{G} \rightarrow c'$$

If $c = c'$, it proves that the private key used for signature and the public key used for verification are a pair. The authenticity of the key directly proves the authenticity of the identifier, because the key is directly derived from the identifier to form a one to one mapping. The identifier verification function is marked by $\mathrm{VER}_{PK\text{-Alice}}(0, s) = c'$.

Identifier authentication is independent and can represent the authenticity of the subject, it is rarely used independently, but it is the basis of identity authentication and object authentication.

2.1.3. Subject Authentication

Subject (or Identity) consists of identifier and ontology, so identity (ID) authentication is the authenticity proof of identifier and ontology. Ontology is represented by eigenvalues, which generally adopt biological features, such as fingerprints and facial features.

The sum of identifier private key and ontology eigenvalue constitutes the identity private key. Therefore, the ID authenticity proof code is:

$$s = k^{-1}(\mathrm{ontology} + sk_{\mathrm{Alice}}) \bmod n \tag{2}$$

Marked by $\mathrm{SIG}_{sk\text{-Alice}}(\mathrm{ontology}) = \mathrm{sign}$.

The verification is carried out by public key, so the public key of Alice is calculated first:

$$\text{Hash}(\text{Alice}) = (i, j)^h \to \sum(R_{i,j}) \to PK_{\text{Alice}}$$

So the identity public key is (ontology $*\,\text{G} + PK_{\text{Alice}}$), and the verification code is

$$s^{-1}(\text{ontology} * \text{G} + PK_{\text{Alice}}) = k\text{G} \to c'$$

marked by $\text{VER}_{PK\text{-Alice}}(s, \text{ontology}) = c'$.

If $c = c'$, it is proved that the authenticity of the key proves the authenticity of the ontology. And the identifier key proves that the ontology belongs to Alice.

2.1.4. Compound Authentication

The basic model of compound event is "A gives 50 yuan to B", where A is the subject, B is the slave, and 50 yuan is the object. Object authentication is the proof of the authenticity and responsibility of the subject to the object. It can also prove both ontology and object simultaneously, so the expression of compound authentication is:

$$\text{Object} = (\text{Bob} + 50) \bmod n$$

The sum of the identifier private key and object eigenvalue constitutes the object private key, so the object authenticity proof code is:

$$s = k^{-1}(\text{object} + sk_{\text{Alice}}) \bmod n \tag{3}$$

Marked by $\text{SIG}_{sk\text{-Alice}}(\text{object}) = \text{sign}$.

The verification is carried out by public key, so the public key of Alice is calculated first:

$$\text{Hash}(\text{Alice}) = (i, j)^h \to \sum(R_{i,j}) \to PK_{\text{Alice}}$$

The object public key is (object $*\,\text{G} + PK_{\text{Alice}}$), and the object verification code is:

$$s^{-1}(\text{object} * \text{G} + PK_{\text{Alice}}) = k\text{G} \to c'$$

marked with $\text{VER}_{PK\text{-Alice}}(s, \text{object}) = c'$.

If $c = c'$, it is proved that the authenticity of the key proves the authenticity of the object. And the identifier key proves the responsibility of subject Alice to the object.

2.1.5. Encryption Technique

Hubee, which involves large and private amounts, needs to be encrypted. Suppose Bob sends encrypted data to Alice:

Bob first, randomly define the data encryption key and encrypt the data:

$$k\text{G} = (x, y) \to \text{key};\ \ \text{E}_{\text{key}}(\text{data}) = \text{code}$$

Bob calculates Alice's public key PK_{Alice}:

$$\text{Hash}(\text{Alice}) = (i, j)^h \to \sum(\text{R}_{i,j}) \to PK_{\text{Alice}}$$

And then encrypt the key:

$$k * PK_{\text{Alice}} = \beta$$

The key encryption is marked by $\text{ENC}_{PK\text{-Alice}}(\text{key}) = \beta$, Bob Sends (code, β) to Alice.

Alice decrypts the key with her private key:

$$sk^{-1} * \beta = \text{key};\ \text{D}_{\text{key}}(\text{code}) = \text{data}$$

The decryption is marked by $\text{DEC}_{sk\text{-Alice}}(\beta) = \text{key}$.

2.2. Attribution Proof and Anti-Copying Measure

Paper money itself has no attribute, it is embodied by possession. There are two forms of possession of paper money. One is to deposit it in the bank, and the other is to put it in one's wallet. To protect the possession, bank notes must be kept in safes, and the individual cash must be locked in wallets. The security of paper money is ensured by the maintenance of possession. With the development of online payment, there are more and more ways to deposit cash in the bank, but less and less ways to carry cash in wallet. After money is converted from tangible paper money to intangible digital currency, possession cannot be used to reflect the attributes of digital equivalents, because in the open network, possession is not enough to prove its attribution. There are two ways to prove the attribution of intangible assets. One is that they cannot prove their attribution, such as intellectual property rights, because anyone can sign and claim that the patent rights are theirs, while the patent itself cannot provide attribution proof, and can only rely on the notary institutions of patent rights to prove possession. If the digital currency does not provide its own attribute proof, it will be difficult for the law to determine its attribute when disputes occur. Thus it can be seen that the attribute proof is the function that the digital currencies must have.

If currency is issued by the central bank, after free circulation on the market, the currency finally returns to the deposit bank for settlement, the deposit banks spread all over the country, bring great trouble to find a copied currency, because the copied currency can only be found by means of comparison, so the central bank must set a platforms within its domain to record all the used currency. It should be a huge project. The serial number of the currency may be used as a segmentation method for the currency issuing to reduce the scope of comparison. It has a certain significance, but it is still a stupid method, and even if the copy is checked, no help to the further investigation of the case.

In the history of monetary development, the check system created a new issuing method. Because it is a paper template, the authenticity proof is very difficult, it takes several days to authenticate a check. But many people realize the advantages of electronic checks. In the early 1990s, the electronic finance just started, and the research of electronic check rose up all over the country.

If the currency is opened by the account like a check, then the currency will

naturally have its attribution. Because the payer's account can specify the payee's account when opening the currency, it will not have any significance for person even if he copied, so there is no fear of loss or theft. If duplication occurs, it is also easy to detect because the currency ends up back in the deposit bank for settlement, and it is easy to find out a copied currency within a account. It can be seen that the consistency of the starting point and destination of currency is the best way to detect the crime of duplication. The account can define its own serial number when opening a currency, that can only be generated and interpreted by the account, which can further prove the attributes, and provide a basis for identification of replication. This property has the function of resisting quantum exhaustion. The use of checks has been experienced for a long time, the advantages and disadvantages are clear, in the process of digitization, there will be no risk to overcome the defects and to carry forward the advantages.

The attribution proof and anti-copying measures require changes in the way the currency was issued or opened. The basic development trend is that, just like online payment, money is stored in the bank and users can use it freely without carrying cash. For the banks, there is no need to keep cash, but just to keep accounts of digital currency without special security methods. The digital currency is not only used for circulation, but also for settlement. As the information content of a digital currency is less than 300 bytes, it can be recorded in the form of array inside the machine, and printed out in the form of QR code outside the machine. As the digital currency has a strong self-protection function, that is, it has the proof of the attribution, so the digital currency is not afraid of losing and its account books are not afraid of being stolen. The use of digital currency does not impact the current banking system, but only simplifies and sublimates the form of account storage, so as to lay a good technical foundation for the transition of banks to fully automated unmanned banks.

2.3. Unification of Payment and Settlement Currency

Money is easy to circulate, because cash becomes electronic bills in circulation, and becomes electronic data in settlement. A cash has undergone several changes from electronic bill to electronic data in transmission and settlement, and the different security between different forms will produce the barrel effect. The weakest link is the bookkeeping in the form of data, because of the lack of verifiable evidence and the weak self-protection ability, the book and currency are separated and located in different places fearing of losing.

At present, electronic bills are the dominant form of money circulation, and its momentum is certain. Electronic bills indicate the sender and receiver in circulation, although they have not certificates, it has been an important guarantee of safety, which is an important guarantee of security, that is the reason why electronic payment can continue to exist. However, as electronic bills cannot support settlement, it still maintains the traditional practice with electronic data. Because electronic bills cannot provide authenticity for both sides of the pay-

ment, so the bank account book is the data with incomplete evidence and fear of loss. Therefore, the focus of digital currency security is on the storage link.

To ensure the safety of currency in circulation and storage, payment currency and settlement currency must be unified, the form of digital currency should not be affected by changes in circulation or storage, and should be consistent in all links. If equivalents are safe in circulation, they can remain safe in the settlement, which do not require additional protection. Payment activities in transactions directly cause changes in expenditure and income between bank accounts, without the need for additional intermediate links such as switching platforms. If a digital currency only satisfies the payment requirement without supporting settlement, there is no need to study such a digital currency.

3. Hubee's Authorization Letter

Hubee's authorization varies from scope to scope.

3.1. Letter of Central Bank

If Hubee is used at the scope of a central bank, it is scoped between a central bank and the subordinated commercial banks.

Authorization letter of the Central Bank to the commercial bank: signature of the central bank to the commercial bank, approving the quota and supervising overdraft.

Authorization Letter of Central Bank	
Central Bank's sign to commercial bank	$SIG_{sk\text{-central-bank}}(\text{commercial-bank}) = \text{sign}$

3.2. Letter of Commercial Bank

If Hubee is used independently in a commercial bank, it is scoped between the bank and the subordinated accounts. The Authorization letter is the signature of the bank on the account; It also approves the amount of the account and supervises overdrafts.

Authorization Letter of Commercial Bank	
Commercial Bank's sign to account	$SIG_{sk\text{-commercial-bank}}(\text{account}) = \text{sign}$

If a commercial bank is using Hubee at the central bank, the central bank's authorization must be included, e.g.

Authorization Letter of Commercial Bank	
Central bank's authorization letter	$SIG_{sk\text{-central-bank}}(\text{commercial-bank}) = \text{sign}$
Commercial bank's authorization letter	$SIG_{sk\text{-commercial-bank}}(\text{account}) = \text{sign}$

4. Hubee's Template

The template of digital currency can be copied and used over and over again, and the bank sets the format of data items uniformly.

Hubee templates with central bank scope are as follows:

Central Bank Template for Account		
Central Bank	Commercial Bank	sign1
Commercial Bank	Account (account number or name)	sign2
payee	Bob	
amount	50$	
currency	Chy (Chinese Yuan)	
Serial_no	0001	
Linear sum	(bob + 50 + chy + 0001) mod2^{64}	Sign3

Item 1: the signature of the central bank on the commercial bank certifying the authenticity of the two banks;

$$\mathrm{SIG}_{sk\text{-central\_bank}}\left(\mathrm{commercial\_bank}\right)=\mathrm{sign1}$$

Item 2: the signature of the commercial bank on the account to prove the authenticity of the bank and account;

$$\mathrm{SIG}_{sk\text{-commercial\_bank}}\left(\mathrm{account}\right)=\mathrm{sign2}$$

Item 3: payee sends the advice of collection in advance, including the payee and the amount. If the payer agrees, fill in the payee and amount in the template. The payer may also define the payee and the amount on its own initiative.

Item 4: digital currency

Item 5: the initial value of Serial_no is defined by the account.

Item 6: linear sum, is the sum of payee, currency, serial_no and amount; Linear sum is used in bank settlement to establish an evidence-chain to ensure the integrity of the accounts.

$$\mathrm{Lsum}=\left(\mathrm{bob}+50+\mathrm{chy}+0001\right)\mathrm{mod}\,2^{64}$$

$$\mathrm{SIG}_{sk\text{-accoun}}\left(\mathrm{lsum}\right)=\mathrm{Sign3}$$

The filling process is automatic, and when the items are filled, they become Hubee, displaying the "send" prompt.

If Hubee's content is confidential or private, sends encrypted Hubee. Encrypts the key with public key, and sends (code, β).

5. Hubee's Payment

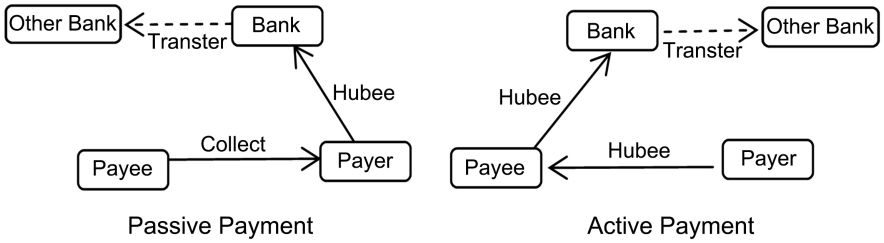
Hubee is filled in by the account:

Alice's Hubee

$$= \{\text{bank}, \text{account}, \text{sign2}, \text{payee}, \text{amount}, \text{currency}, \text{serial\_no}, \text{h}, \text{Lsum}, \text{sign3}\};$$

$$= \{\text{bank}, \text{Alice}, \text{sign2}, \text{Bob}, 50, \text{chy}, 0001, \text{h}, \text{lsum}, \text{sign3}\}$$

Hubee's payments occur between the account and the bank, and are also related to the recipient and the other bank. The diagram is as below:



There are two different layers in the delivery process of Hubee, one is the communication layer, and the other is the business layer.

5.1. Communication Layer Transmission

Hubee's communication authentication protocol implements GAP one-step protocol [4]. The subject authentication is implemented in GAP protocol in one step, so the password authentication and login registration mechanism are canceled. The links between accounts and banks are usually remote links, mainly telephone networks or the Internet. Therefore, the user name private key and phone number private key can be used to connect the remote account. For example, the Internet is identified by the user name alice.com. Alice.com sends Hubee to the banking side:

$$k\text{G} \to c;\ k^{-1}\left(\text{Hubee} + sk_{\text{alice.com}}\right) \to s;\ \text{sign} = (s, c)$$

The bank terminal calculates the public key $PK_{\text{ALICE.COM}}$ to verify the authenticity of the sender:

$$s^{-1}\left(\text{Hubee} * \text{G} + PK_{\text{ALICE.COM}}\right) \to c'$$

If $c = c'$, hands Hubee to the business layer.

5.2. Business Layer Acceptance

The first case: Hubee is submitted by the account of the Bank, and the payee also belongs to the bank.

If Hubee is encrypted, it is decrypted first. Then, the lsum's signature is verified, suppose the payer is Alice, then:

$$\text{Hash}(\text{Alice}) = (i, j)^h \to \sum\left(\text{R}_{i,j}\right) \to PK_{\text{Alice}}$$

$$s^{-1}\left(\text{lsumG} + PK_{\text{Alice}}\right) = k\text{G} \to c'$$

If $c = c'$, re-account check will be carried out, otherwise it will be rejected.

6. Hubee's Settlement

Hubee's bank account consists of two parts: one is Hubee's statement and the other is the bank's statement. Hubee's bookkeeping does not change the form of Hubee. Because Hubee stipulates the payer and payee, which has no meaning for the third party, so it is not afraid of loss. Hubee's accounting forms are as follows:

Alice's Account								
Bank	Sign	Payee	Amount	Currency	Serial_no	Hash	lsum	Sign
	Sign_1				n	h	lsum	Sign_2
	Sign_1				n	h	lsum	Sign_2
	Sign_1				n	h	lsum	Sign_2

Bank's Statement of Alice		
Balance	Sign	E-chain
Balance	Sign_4	Ecode_1
Balance	Sign_4	Ecode_2
Balance	Sign_4	Ecode_n

The bank settlement process is as follows:

First calculate the balance and sign the balance

$$\text{SIG}_{\text{Bank}}\left(\text{balance}\right)=\text{sign}_4$$

To establish Ecode: The evidence-chain is accumulation of Lsum:

$$\text{Ecode}_1=\text{lsum}_1$$

$$\text{Ecode}_n=\text{lsum}_1+\text{lsum}_2+\cdots+\text{lsum}_n$$

Each time when a new record is added, check the evidence-chain of ecode1. ecoden-1:

If $\text{ecode}_{n-1}=\text{ecode}'_{n-1}$, the data is proved not to have been lost or tampered with, allowing the addition of a new record$_n$. If $\text{ecode}_i \neq \text{Ecode}'_i$ occurs in the i^{th} position, it indicates that there is a problem with the i^{th} position. Then, the balance of the $(i-1)^{\text{th}}$ position and $(i+1)^{\text{th}}$ position is used to extrude the amount of the i^{th} position, and the linear equation is listed by lsum.

$$\text{Lsum}=\left(\text{payee}+\text{currency}+\text{amount}+n\right)\bmod 2^{64}$$

In the equation, the amount and serial_no are known, and the payee can be

finally calculated. So far, the payee and amount of the i^{th} lost Hubee can be recovered.

In bank books, balances are private and should be stored encrypted.

The second case: the payee belongs to another bank. If the other bank belongs to the unified Hubee system, it is ok to re-encrypt Hubee and forward it.

Third case: if the receiver does not have the Hubee function, the original provisions shall be implemented.

7. Hubee's Checkout Notice

After the settlement, the bank will send the settlement notice to the payee and the balance notice to the payer.

The settlement notice is composed of bank name, amount, payer, and signed by the bank:

$$\text{Data} = (\text{bank} + \text{amount} + \text{payer}) \bmod n$$

$$\text{SIG}_{\text{bank}}(\text{data}) = \text{sign}$$

The bank sends the bank name, amount, payer and signed data to the payee.

The balance notice is consists of the bank name, amount, payee, and signed by the bank

$$\text{Data} = (\text{bank} + \text{amount} + \text{payee}) \bmod n$$

$$\text{SIG}_{\text{bank}}(\text{data}) = \text{sign}$$

The bank sends the bank, amount, payee and signed data to the payer.

Suppose the bank sends encrypted data to Bob. The bank encrypts plain data: $E_{key}(data)$ = code, E is a symmetric encryption function. The bank computes Bob's public key, and encrypts key:

$$\text{ENC}_{\text{BOB}}(\text{key}) = \text{beta}$$

the bank sends {code, beta) to Bob.

Bob decrypts the key with his private key:

$$\text{DEC}_{\text{bob}}(\text{beta}) = \text{key};\ \text{D}_{\text{key}}(\text{code}) = \text{data}$$

where, DEC is asymmetric decryption function and D is symmetric decryption function.

8. Hubee's Form of Existence

Hubee has two kinds of existence forms: the form of inside-machine or outside-machine.

Form of Inside-machine: array of character string: such as:

$$\text{Hubee}: \{\text{bank}, \text{account}, \text{sign1}, \text{payee}, \text{amount}, \text{currency}, \text{n}, \text{Lsum}, \text{sign2}\};$$

$$\sum = \{24\text{B} + 24\text{B} + 36\text{B} + 24\text{B} + 16\text{B} + 3\text{B} + 8\text{B} + 8\text{B} + 36\text{B}\} = 179\text{B};$$

Form of outside-machine: Printed table and QR-code, such as:

Alice's Hubee (24B)	
Bank name	Character string (24B)
Bank sign to account	Array of digit (36B)
Payee	Character string (24B)
Amount	Integer (16B)
Currency	Character (3B)
Serial_no	Integer (8B)
Lsum	Integer (8B)
Account's sign to Lsum	Array of digit (36B)

QR-Code
(187Bytes)

9. Hubee's Action Scope

Hubee runs on the CPK authentication network. CPK authentication network is a boundless horizontal logical network, which can provide a verifiable connection at any two ends. In such a plane without a center, a different network form can be flexibly set up, such as simulated star network with a center, hierarchical tree network, flat grid network, blocked LAN, etc. It can be opened or closed between different networks or between different blocks. Decentralized operation is guaranteed by the key management center in the form of distribution of private keys. This decentralized network operation is guaranteed by the key management center in the form of private key distribution. The KMC is only the key distribution center, not the network operation center. If each user has a private key, the autonomy of the network is in the hands of each user, forming a user-managed network without a center.

When the CPK system publishes the public matrix, it is signed by the issuer (KMC), and its scope is very clear. Telephone network, Internet, 5G network, satellite network and other global networks, etc., all can be included in a CPK authentication network, only they constitute different identifier classes.

Hubee will operate in a global network. The global network includes telephone network, Internet, 5G network, satellite network, etc. In the global network, telephone system is takes phone number as its identifier, Internet takes user name as its identifier, banking system takes account as its identifier, only the classification of identifier is different. Hubee's accounts all have account private keys, just as they do on the web, forming a network of flat transactions centered around each account.

Hubee's scope is determined by matrix variables and mapping keys. If a central bank defines matrix variables and mapping keys uniformly, a unified Hubee will be used across the central bank's affiliated commercial banks, forming a central bank-wide scope. If a commercial bank operates independently, that is, separate matrix and mapping key are defined to form an independent private network within the range of a bank. Private networks are incompatible with pri-

vate networks. When mutual recognition is required, it is necessary to have the mapping key of the other party, and there is no need to set an independent matrix. However, between central banks, independent matrices are generally adopted. When mutual recognition is needed, each central bank has the other bank's public matrix. When the key length is 256 bits, one public key matrix is 4k bytes. A bank can install multiple public key matrices. Therefore, Hubee scope extension, whether centralized or decentralized, all are practicable.

As a test, select a bank and set up a Hubee bank scoped to a bank-wide. Bank only need to issue authorization letters and templates, and accounts can be opened only with private keys. Hubee system can run in parallel with the original system without affecting each other. In the digital asset protection, the bank is still not at ease, and the settlement table can be established between the bank and the account synchronously. Its technical realization is also easy, but under the Hubee condition, it appears redundant.

10. Summary

Hubee is account that mastered digital currency in which only the account has the right to handle funds, and no one else has the right to handle. Hubee will attack the bank-centered money operation mechanism and shift to the account-centered new money operation mechanism. Hubee realizes the subject authenticity proof and currency attribution proof, so that it has a strong self-protection function, not afraid of loss, individuals do not need wallets, banks do not need vaults. Hubee's security responsibility rests solely with the account. Recently, France, Russia, China and other countries have put forward the request to study digital currency, brewing a storm of currency reform. Because Hubee solves the key technology of subject authentication, it lays a good technical foundation for designing digital currency that is convenient to use, safe to store and easy to supervise.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Katz, Y. (2019) Society and the Digital Gap. *Advances in Applied Sociology*, **9**, 60-69. https://doi.org/10.4236/aasoci.2019.91005

[2] Nan, X.H. (2022) CPK Public Key and Its Basic Functions. *Open Access Library Journal*, **9**, 1-12. https://doi.org/10.4236/oalib.1108287

[3] National Institute of Standards and Technology (1991) NIST PUB 186, Digital Signature Standards.

[4] Nan, X.H. (2021) GAP Universal One-Step Authentication Protocol. *Open Access Library Journal*, **8**, 1-8. https://doi.org/10.4236/oalib.1108061