Open Access Library Journal
2021, Volume 8, e7444
ISSN Online: 2333-9721
ISSN Print: 2333-9705

A Universal Equivalent Currency Hubee

Xianghao Nan

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

How to cite this paper: Nan, X.H. (2021) A Universal Equivalent Currency Hubee. *Open Access Library Journal*, **8**: e7444.
https://doi.org/10.4236/oalib.1107444

Received: April 22, 2021
Accepted: November 20, 2021
Published: November 23, 2021

Abstract

Universal digital equivalent currency is the equivalents of all negotiable instruments, including paper or electronic money, securities, bills, etc. This paper discusses the basic requirements of universal digital equivalent currency, that is, universality and advance; discusses the technical issues that must be solved for equivalent currency, such as the proof of authenticity of the identifier claimed by the subject, the proof of the attribution of currency and the prevention of duplication, the unification of payment currency and settlement currency, The design goal of equivalent currency is to overcome the defects of the previous negotiable instruments, integrate all advantages into one, which can be used in online and offline, universal in payment and settlement, convenient. This paper takes Hubee as an example to illustrate the whole operation process of digital equivalent currency. Only in this mode, an account can define a serial-no for preventing replication; can define the payee's account to prove the flow of funds; which makes currency not to be afraid of lost and make account book not to be afraid of theft.

Subject Areas

Information Technologies

Keywords

Currency, Authentication, Account, Payment, Settlement, Identifier

1. Introduction

In common sense, money is only an equivalent of wealth, and a tool of measurement of wealth, which facilitates the circulation and storage of wealth. The appearance of money gradually replaced barter and became an indispensable link for transactions. Money developed from copper coins to paper money, and from paper money to electronic money, electronic money is developing to digital money. Although electronic currency has not been fully formed into a complete

currency, electronic bills circulating on the Internet have long played the role of electronic currency and indicated the development direction of currency.

The transformation of currency existing form from paper media to electronic media has raised many new problems. The study of electronic currency and digital currency has become a common subject faced by the whole world in the era of digital economy, and has also become a focus of international competition. Digital currency will reflect a country's currency security technology level and will be an important field of new technology competition. If financial information security is compared to the crown, then electronic currency, digital currency is the pearl in the crown. Therefore, the research of universal digital equivalent currency is a severe challenge to information security workers.

In the history of monetary development, there have been various forms of equivalents, such as coupons, checks, securities, electronic bills, digital money, etc. Flexible and diversified operation methods have also emerged, such as network payment, third-party payment, and account cheque issuance. History offers us a lot of experiences, if we seriously analyze and study the past experience and lessons, it is possible by overcoming defects, bringing advantages together to design a equivalent currency that can be used online and offline, payment currency and settlement currency are shared, convenience and security are balanced, where accounts are not afraid to be stolen, the currency is not afraid to be copied.

The biggest difference between paper money and digital money is that paper money has a medium, while digital equivalents have no medium (logical). This has led to many different approaches. In terms of circulation and storage, the equivalent currency must be the unification of payment currency and settlement currency and must be a most convenient and safest currency without changing its form in the circulation and settlement. In the term of assignment for equivalent currency, there is no problem as long as it is equivalent to the original bill with authenticity proof. In the term of protection, it should address replication, because the problem cannot be solved by any logical method, while can only be solved by a issuing mechanism that can detect replication in time.

As a currency, it must have three elements: one is the claim item, the other is the assignment item, and the third is the protection item. The three elements of currency are to ensure the equivalence and authenticity of currency. Among them, the claim item is the issuing bank's authenticity certificate, stamped by the seal on the money, the assignment item is fixed value, the protection item is the anti-counterfeiting technology to ensure the authenticity of the paper money.

As an equivalent currency, it must have two functions: universality and advancement. The universality of equivalent currency means that it can be equivalent to bill, currency, coupon, RMB, or US dollar, and can be used by banks or enterprises. The advancement of the equivalent currency means that its performance and function must be better than the original one, and the equivalent currency must be able to solve the defects that the original notes cannot solve.

To this end, the digital equivalent currency Hubee is designed. First of all, it needs to realize the self-protection mechanism without the support of background system, the currency is not afraid of loss without wallet, and the accounts are not afraid of pilfer without vault.

The characteristics of equivalent currency just meet the needs of cloud banking. The payment of customer by equivalent currency is directly transferred to the cloud bank for settlement. Payment to settlement is automatic, while the equivalent currency stored in the cloud bank is safe and can be unattended. The emergence and development of equivalent currency will have an impact on the traditional currency management model.

2. Authenticity Proof of Bank's Identifier

The identifier claimed by the issuing bank is only printed on the paper banknote, using the security properties of the physical medium to ensure that the authenticity is not tampered with. The proof of authenticity of the bank name in the claim item belongs to the subject authentication technique. Since there is no medium for the equivalent currency, it has been a difficult problem to prove the authenticity of the item. The subject authentication technology can be logically divided into two types: one is "peer authentication" based on trust, another is "identifier authentication" based on evidence.

Peer authentication works on the principle of "what you have, I have" or "what you encrypted, I can decrypt" to establish trust. There are two methods of peer authentication, one is symmetric and the other is asymmetric. Obviously, symmetry is only one factor in "multi-factor authentication" and cannot be used for the proof of the subject. DSS digital signature standard [1] provides a mathematical formula to prove the public-private key pairs, which uses the private-key to sign, and uses the public-key to verify, to prove that "I have a public-key, you have the corresponding private-key" of the principle of reciprocity, which only proves that the private-key and the public-key is a pair, but don't know whose signature it is, the proof has nothing to do with the subject authenticity. Anyone can generate a public and private key pair and sign it at will. If there is no restriction on the key pair, this signature cannot be used as a proof of the authenticity of the subject. Therefore, PKI certification system appears. "This is the public-key of Alice" is given in CA certificate, which provides the restrictive conditions for the key, but who proves the authenticity of CA? This will be an endless chain of evidence, which can only be resolved ultimately by administrative regulations. In the authentication method, the CA certificate is provided by the signer to the verifier. This saves the trouble of accessing the LDAP, but the proof logic is very regressive. The essence of this method is that the verification only carried out between the signer and the CA certificate, has nothing to do with the verifier, so the verifier can recognize or have the right not to recognize. The identifier claimed by the subject is not just the name of a person. Different occasions use different identifiers, such as claiming "I am XX" or "my

number is XX" when making a phone call. User name, account name, etc., can be used as identifiers, which should be reflected in a CA certificate. Although there are some problems, it can still be used as a method of subject authentication.

A new subject authentication technology is based on evidence to achieve subject authenticity through identifier authentication. According to the Truth Authentication Logic [2], an entity (or identity) is composed of identifier and ontology, so the identity authenticity should be composed of identifier authenticity and ontology authenticity. The identifier authenticity is that signed by the private-key of the claimed identifier (Alice) and verified by the public-key of the same identifier:

Identifier authentication: $k\mathrm{G} = (x,y) \to c$; $k^{-1}sk_{\mathrm{Alice}} \bmod n = s$; sign = (s, c),

Identifier verification: $s^{-1}PK_{\mathrm{Alice}} = (x, y) \to c'$.

If $c = c'$, then the identifier is true. Where, k is a random number, G is generator, sk_{Alice} is private-key derived from identifier Alice, PK_{Alice} is public-key derived from identifier Alice, n is te order of additive group, s is sign code and c is checking code. Suppose that the characteristic of ontology is h, then the subject authenticity is that a signature to the h with private-key of claimed identifier, and verification with public-key of the same identifier:

Subject authentication: $k\mathrm{G} = (x, y) \to c$; $k^{-1}(h + sk_{\mathrm{Alice}}) \bmod n = s$; sign = (s, c),

Subject verification: $s^{-1}(h\mathrm{G} + PK_{\mathrm{Alice}}) = (x, y) \to c'$.

If $c = c'$, then the subject is true, a signature certifies both identifier and ontology authenticity simultaneously.

Claiming is easy, but proving is hard, and verifying is even harder. The reason why it is difficult to prove the claimed identifier is that the proof has special requirements. In signature, the private-key must be derived from the claimed identifier, and there is a one-to-one mapping between the identifier and key. The verification is harder, because the public-key to be used for verification is calculated by the verifier from the claimed identifier. The public-key computing tool is published signed by the issuer to determine the scope. DSS can become a digital signature standard only when the key meets the above two conditions. In other words, a digital signature must be able to prove the authenticity of the identifier claimed by the subject. Only a digital signature can be used as evidence of authenticity. It is impossible to verify without evidence, so the authentication system is the unification of evidence showing system and verification system, the evidence provided by the proof system should be a direct evidence. An advanced technology of an authentication system is reflected in the evidence showing system.

This authentication system can only be established with an identifier-based public key. CPK [3] provides a general method for changing existing public keys, such as DLP of discrete logarithms, ECC of elliptic curves, RSA of factorization, BLP of bi-linear pairs, etc., into identifier-based public keys. Where, ECC has the shortest signature code and the fastest operation speed. CPK has also expe-

rienced 20 years of development, from the original type to smart type and timed type. The smart type overcame the "open problem" existing in the original type, while the timed type can solve the exhaustion of quantum computing. As equivalent currency issued today should be valid in the quantum age.

3. 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 equivalent 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 equivalent 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 equivalence currencies must have.

Paper money are implemented with a physical medium, copy-prevention to physical medium can only be solved by physical method, any digital logic method is powerless, and the digital equivalent currency is without medium, so theoretically, there can be no direct confrontation method, must find a new way where the copy can be allowed, but that doesn't work. Therefore, the properties of the equivalent currency and the prevention of duplication need to be solved by the issuing mechanism of the currency.

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 equivalent currency without special security methods. The equivalent currency is not only used for circulation, but also for settlement. As the information content of an equivalent 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 equivalent currency has a strong self-protection function, that is, it has the proof of the attribution, so the equivalent currency is not afraid of losing and its account books are not afraid of being stolen. The use of equivalent 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.

4. 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 payment, so the bank account book is the data with incomplete evidence and fear of loss. Therefore, the focus of equivalent 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 equivalent 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 an equivalent currency only satisfies the payment requirement without supporting settlement, there is no need to study such a equivalent currency.

5. Implementation of Equivalent Currency

In the above discussion, it is clear that the digital equivalent currency must have the proof of subject authenticity, the proof of the attribution and the proof of flowing direction. Only when the currency template is issued uniformly by the central bank, and the digital equivalent currency is opened by the account, can the crime of copying be effectively prevented.

Taking Hubee as an example, the realization of digital equivalent currency is described as follows.

5.1. Template Design of Hubee

For the convenience of illustration, take banks as an example. Institutions are divided into central bank, commercial bank and account, and their authorization relationship is as follows.

Authorization letter of the Central Bank to the commercial bank: signature of the central bank to the commercial bank, approving the amount to supervise overdraft.

Authorization letter of the commercial bank to the account: signature of the commercial bank to the account, approving the amount to supervise overdraft.

Authorization Letter for Hubee	
Name of central bank	$SIG_{sk\text{-}central\text{-}bank}$ (commercial-bank) = sign1
Name of commercial bank	$SIG_{sk\text{-}commercial\text{-}bank}$ (account) = sign2

Where SIG is the signature function, *sk-central-bank* is the private-key of the central bank, and *sk-commercial-bank* is the private-key of a commercial bank.

The template of equivalent currency can be copied and used repeatedly, and the bank uniformly stipulates the setting of data item format, such as serial number, payee, amount, linear sum, etc.

Hubee Template		
central	commercial bank	$SIG_{sk\text{-}central\text{-}bank}$ (commercial-bank) = sign1
commercial	account	$SIG_{sk\text{-}commercial\text{-}bank}$ (account) = sign2
payee	amount	$SIG_{payee's\text{-}account}$ (amount) = sign3
payer	amount	$SIG_{sk\text{-}payer's\text{-}account}$ (amount) = sign4
Serial-no	n	$Hash_{key}(n) = h$
Linear Sum	Lsum = (n + payee's account + amount) mod 2^{64}	$SIG_{sk\text{-}payer's\text{-}account}$ (lsum) = sign5

Item 1: signature of the central bank to the commercial bank, and attesting to the authenticity of the central bank and the commercial bank;

Item 2: the signature of the commercial bank to the account, certifying the authenticity of the commercial bank and the account;

Item 3: blank, signature of the payee's account to prove the authenticity of the receivable amount;

Item 4: blank, signature of the payer's account to prove the authenticity of the payment amount;

Item 5: blank, serial number, hash value under the key defined by the account;

Item 6: blank, linear sum, is the sum of serial-no, payee's account and amount;

The filling process is automatic, finally becomes Hubee.

Serial-no: Initial values are defined by the account and can be used sequentially or in the form of dynamic passwords. The serial-no n is Hashed into h, and the key used is defined by the account itself and fixed.

$$Hash_{key}(n) = h$$

The h acts as the account's signature to the serial-no n, only the account can generate and interpret h, and it is used for duplicate currency query and attribute proof. In the quantum age, even if all public-keys are cracked, and even if the central bank certificate, commercial bank certificate, payee's account certificate and payer's account certificate are all counterfeited, only the serial-no and hash value remain uncracked, which can still provide the attribute and anti-counterfeiting proof.

Payee: The payment process is characterized by "asking for money first, paying later". The payee sends the collecting notice first, in which the authenticity proof of the payee and amount is given:

$$\text{Collecting notice} = SIG_{sk\text{-}payee's\ account}(\text{amount}) = \text{sign}$$

The collection notice is the signature of the payee on the amount, where *sk-payee's account* is the private key of payee. A signature certifies the authenticity of both payee and amount.

The payer verifies the collecting notice: first, calculates the public-key of payee and verifies:

$$VER_{PK\text{-}PAYEE'S\ ACCOUNT}(amount) \rightarrow c'$$

where, VER is the verification function, and *PK-PAYEE'S ACCOUNT* is payee's public-key. After passing the verification, the payee and amount will be automatically filled into the template data item, and the payer also signs the amount to generate an equivalent currency:

$$SIG_{sk\text{-}account}(\text{amount}) = \text{sign4}$$

Lsum: Linear sum is used in bank settlement to establish an evidence-chain to ensure the integrity of the accounts.

$$\text{Lsum} = (\text{serial-no n} + \text{payee's account} + \text{amount}) \bmod 2^{64}$$

After the filling, the prompt will be displayed to send.

5.2. Settlement of Hubee

Digital equivalent currency always does not change its form in transfer and accounting. A bank account is made up of two parts: one is record of equivalent currency, and the other is a record of bank settlement, such as:

Hubee Record									
Bank1	Bank2	Amount	payee	amount	payer	serial	Hash	lsum	payer
Sign1	Sign2		Sign3		Sign4	n	h	lsum	Sign5
sign1	Sign2		Sign3		Sign4	n	h	lsum	Sign5
sign1	Sign2		Sign3		Sign4	n	h	lsum	Sign5

Settlement		
Balance	Bank's sign	E-chain
Balance	Sign6	$Ecode_1$
Balance	Sign6	$Ecode_2$
Balance	Sign6	$Ecode_n$

The settlement process in the bank is as follows:

After the verification for equivalent currency, first calculates the new balance and signs to the balance:

$$SIG_{sk\text{-}bank}(\text{balance}) = \text{sign}$$

Ecode: The evidence-chain is the accumulative of lsum:

$$Ecode_1 = lsum_1$$

$$Ecode_n = lsum_1 + lsum_2 + \ldots + lsum_n$$

Each time a new record is added, the bank first checks the evidence-chain $ecode_1..ecode_{n\text{-}1}$:

$$Ecode_{n\text{-}1} = (lsum_1 + lsum_2 + \cdots + lsum_{n\text{-}1}) \bmod 2^{64}$$

If $ecode_{n\text{-}1} = ecode'_{n-1}$, the data is proved not to have been lost or tampered with, allowing the addition of a new $record_n$. If $ecode_i \neq Ecode'_i$ occurs in the i^{th}

position, it indicates that there is a problem with the i^{th} position. Then, the balance of the $i-1$ position and $i^{th}+1$ position is used to extrude the amount of the i^{th} position, and the linear equation is listed by lsum.

$$\text{Lsum} = (n + \text{payee's account} + \text{amount}) \bmod 2^{64}$$

In the equation, the amount and serial-no is known factor, so the payee's account can finally be worked out. Thus, the main elements of the i^{th} lost digital equivalent currency can be recovered.

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

5.3. Checkout Notice of Hubee

After the settlement, the commercial bank sends the settlement notice to the payee and the balance notice to the payer.

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

$$\text{Data} = \{\text{bank, payee, amount}\}$$

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

The commercial bank sends the data and sign to the payee.

The balance notice is composed of the bank,payer, amount and signed by the bank

$$\text{Data} = \{\text{bank, payer, amount}\}$$

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

The bank sends the data and sign to the payer.

5.4. Privacy protection of Hubee

When the amount needs privacy protection, it provides key encryption function.

Assuming that Alice sends encrypted data to Bob, Alice first defines data encryption key, key = r*G, where r is a random number and G is the base point of elliptic curve.

Alice encrypts data with the symmetric key:

$$E_{key}(\text{data}) = \text{code}$$

where E is symmetric encryption function.

Alice computes Bob's public key, encrypts the key with the public-key,

$$\text{ENC}_{BOB} = \text{beta}$$

where, ENC is asymmetric encryption function, *BOB* is Bob's public-key. Alice sends {code, beta) to Bob.

Bob uses his private key to decrypt:

$$\text{DNC}_{bob}(\beta) = \text{key}$$

$$D_{key}(\text{code}) = \text{data}$$

where, DNC is an asymmetric decryption function, *bob* is Bob's private-key, and D is a symmetric decryption function.

6. Summary

Digital equivalent currency unifies the payment currency and settlement currency, realizing the subject authenticity proof and currency attribution proof, and forming an evidence chain among the payer, payee and bank. Bank does not need a vault, and person does not need a wallet. The issuance way where bank uniformly issues templates and the account opens the currency minimizes risks and costs. The serial-no that is defined by an account also provides authenticity and attribute proof, the quantum exhaustive is powerless about this. The characteristics of the equivalent currency meet the technical requirements for cloud banking. It is applicable to the payment and settlement of bulk funds among commercial banks under the same central bank.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] National Institute of Standards and Technology (1994) NIST PUB 186, Digital Signature Standards.

[2] Nan, X.H. (2020) CPK Solution to Cyber Security: Theory and Practice. Publishing House of Electronic Industry, Beijing.

[3] Nan, X.H. and Chen, Z. (2003) A Profile to Network Security. Defense Industry Publishing House, Beijing.