Electronic cash systems : A Survey

Sharma Dewangini N.[1], Prof. Manoj B. Patel[2]
[1, 2] Department of Computer Engineering
[1, 2] Alpha College of Engineering and Technology, Khatraj, India

Abstract- *In digital world there are various websites presently has the situations where people transact with unknown agents and take decision for these agents for by considering the stature score. Central idea of this paper is to compare online Trust and stature models that are particularly suitable for the peer to peer network but uses different approaches for calculating for getting towards the trust of an entity. This paper describes how the trust for the entity is works of, their properties and various parameters advantages disadvantages. Finally, it concludes by comparison of all these protocols*

Keywords- component; formatting; style; styling; insert

I. INTRODUCTION

The term "electronic cash" often is applied to any electronic payment scheme that superficially resembles money. In fact, however, electronic cash is a specific kind of electronic payment scheme, defined by certain cryptographic properties.[1]

Generally any e cash system would take in account the agents as bank, customers/users and the stakeholder and the life cycle of electronic coin involves all the parties. User withdraws coin from the bank.

The coin then can be exchanged for some goods and services by the users to the merchants.

As even the merchant will not keep the coin with it rather the cycle is completed when the merchant/stakeholder deposits back the con to the bank.

From above steps the cycle can be said having 3 phases withdrawal phase, the payment phase, and the deposit phase.

Prior to process is the preprocessing step which requires deals with generating public keys, management of the account. electronic cash can be categorized as on-line and off-line. In an on-line electronic cash, the payment and deposit phases occur in the same transaction. So we can conclude that the coin is verified every by the bank at the time of payment so bank to be on-line for every coin exchanged between the spenders and the merchants.

In off-line electronic cash schemes, the coins are verified after the transaction at some convenient time for both merchants and the bank so that the bank does not have to be involved in every payment transaction. However, as the coins are not verified at the time of payment, there is a potential for dishonest spenders to double spend their coins. This is because digital cash, which is essentially a set of numbers, is easy to copy. Another requirement that can arise in electronic coins is the need for anonymity.

II. TERMINOLOGIES RELATED TO TRUST

Classification of electronic cash system

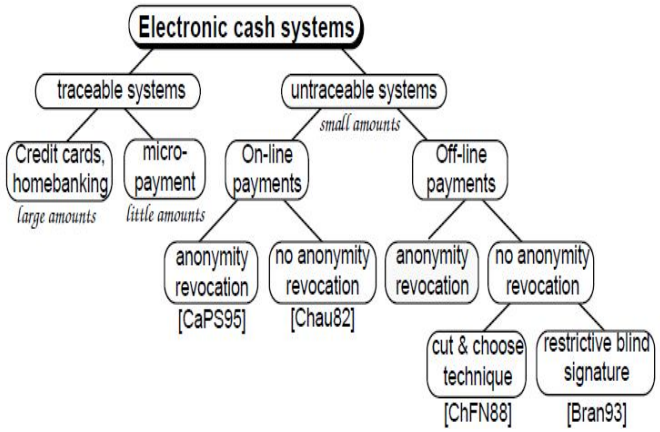


Figure 1. Classification of Electronic cash system[2]

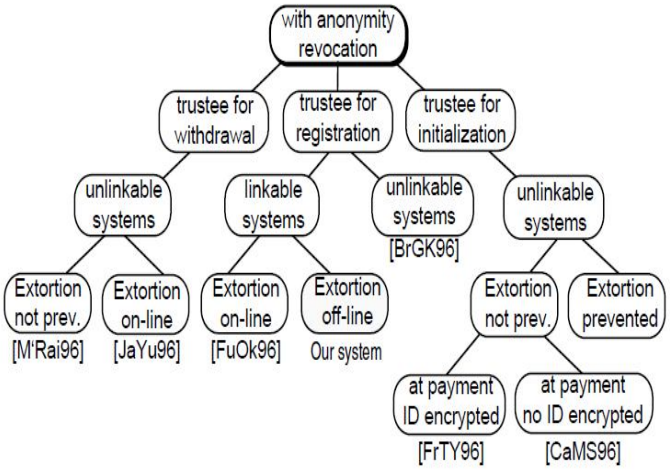


Figure 2. Classification of Electronic cash system with anonymity revocation[2]

In this setting seven main events are distinguishable:

1. **Initialisation:** Choice of system parameters and key pairs of all entities.
2. **Opening account**: The bank opens a user account and registers his personal data.
3. **Registration**: In the pseudonymous systems, the user registers at the trustee.
4. **Withdrawal**: The user withdraws digital coins from his account onto his device.
5. **Payment:** The user pays at the shop using the coins stored on his device.
6. **Deposit:** The shop deposits the digital coins at the bank and is credited accordingly.
7. **Revocation:** The trustee is able to compute either the shape of the coin from the withdrawal transcript or to compute the user's identity from the payment transcript in order to deter any perfect crime

III. SOME STATURE BASED PROTOCOLS

A.

To protect the privacy of customers, each payment should be anonymous, and furthermore unlinkability should be satisfied. The unlinkability means that any other one except the trusted third party cannot determine whether two payments are made by the same customer.

STEP 1: Initialization:

Bank and trustee generate public and secret keys.
The public keys described in this setup protocol are assigned to a single monetary amount $w = 2^{\ell}-1$.

STEP 2: Withdrawal:

For withdrawing a coin, the e-coupon protocol, which corresponds to the issue of a membership certificate in the group signature scheme is conducted.

Payment:

Each shop owns a unique identifier.
m = concatenation of the identifier
the customer pays the shop any amount˜ w ($\leq w = 2^{\ell}-1$).
Let [˜ wℓ ・ ・ ・ ˜ w1] be the binary representation of ˜ w.

Payment protocol for a node $n_{j1}\cdots j_u$ is shown. By executing this payment protocol for multiple nodes parallel, the payment for any amount is accomplished.

F = paid node together with the group signature.
de.F values of a binary tree levels are illustrated in Figure 3.
*

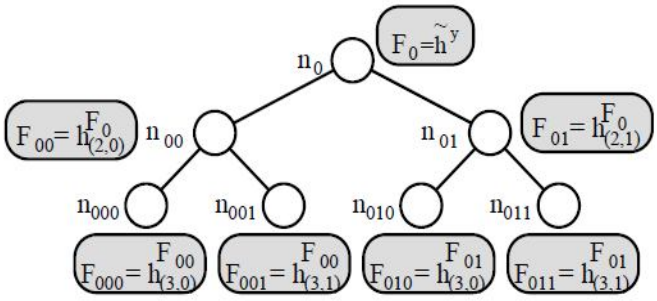


Figure 3: F values of a binary tree of 3 levels

Deposit:

Over-spending is checked on the divisibiliy rule. If it does not occur, the paid amount is deposited in the account of the shop. esle, the over-spender can be identified by owner tracing protocol.

Anonymity Revocation:

The owner tracing protocol is the same as the identification of the signer in the original group signature scheme. The coin tracing protocol is arranged from that of the e-coupon system.

B. Xcash

X-cash or executable digital cash for the common entity . A piece of X-cash consists of a signed certificate issued by the bank and a program which for generating the amount which the consumer is willing to pay for any tangible entity

Initially consumer C will get a certificate from bank authorizing to make payments to the consumer. The range will also be decided by the consumer for the payment based on that the offer function will be constructed and encoded in a piece of executable code. The consumer will then generate the X-cash by combining the signed executable code and the certificate issued by the bank. The executable is signed using e
skC = private key
pkC = public key contained in the signed certificate issued by the bank.
To buy something,
C sends X-cash to the merchant M.
M checks the correctness of the signature and evaluate offer by executing function.
M will contact C's bank if it get satisfied. By allowing the offer to travel in a common entity with corresponding goods or payments, the proposed architecture allows digital cash to be used in highly distributed settings while ensuring the security of conveyed funds. Although the basic scheme proposed in does not support anonymity, the authors claim

that it is possible to extend it to address such property. Not a multi-agent protocol, in a sense that interactions are limited to a merchant and a consumer, or a merchant and a bank.

C. Gupta et al. Debit Credit Reputation Computation

Basis for an incentive system and suitable for multimedia upload and download.

Three tunable system parameters are there in this protocol:

File size factor f, f integer, this parameters measures the level of MBytes data depending on increasing the reputation score.

Bandwidth factor b, b real, identifies nodes for bandwidth . Time factor in hours t, t integer. Period for the peer cooperation by sharing and staying online is rewarded.

The reputation is computed by the agent called reputation computation agent to periodically update to the feedback providing agent's reputation, and to ensure that feedback value provided by them is kept locally so that it can be retrieved quickly. Reputation computation agent does not play any role while searching and retrieving so that it does become bottleneck for the normal operation of the P2P system:

Query-Response Credit (QRC)

Agents initially need to register then they receive credit for providing their feedback to the system processing the query-response messages.

On key pair i.e. public and private key are generated on the registration. The agent chooses to send these proof of process to the RCA for receiving the credits.

Then RCA uses the public key to verify the Process proof from the agent and encrypts stature score.

Upload Credit (UC):

Each agent gets credit for providing any content related to multimedia and gets credit, (public, private) key pair is denoted here {PKr, SKr} and sender peers by {PKs, SKs}.

At the time of the file download

For downloading {requester identity, file_name, file size, time stamp} and encrypt it with its private key and send to the up loader/sender agnates.

On receiving the information from the above step and decrypting it by using the requester's public key and then encrypts the receipt of the transaction by its private key.

Download Debit (DD)

While downloading a file an agent needs to debit for downloading the file. For negative reputation value, the RCA retains the negative scores in the form of debit state with itself until those peers send some credits for processing

Sharing Credit (SC):

This step allows the registered agents to for credit to be shared for staying online, based on the number of files they are sharing.

It can be achieved in two ways both the ways requires the RCA to do more work can also cause some amount of error in the stature computation procedure.

First way deals with transaction state being recorded by RCA to check the time period for which particular agent was online and total amount of data shared by an agent.

Second one periodic monitoring of the shared directories of agents by the RCA. But this method is more inaccurate Because the credit depends on the monitoring frequency.

Expiration and Consolidation of Reputation Scores:

The time stamp is not important for it as the debit is there in the reputation scores. The peers can periodically send their reputation scores to the RCA for consolidation and get one encrypted score back.

CyberOrg, a model for hierarchical coordination of resource proposed in [26], also allows the creation of agents carrying e-cash. The proposed approach focuses more on the implementation of agents and their interactions rather than addressing security requirements of ecash payment.

Researches on using multi-agents systems for e-cash payments are quite recent. A first explanation is that multi-agent setting creates an additional layer of difficulties on top of an already complex set of issues. In the future, we will have to address several difficulties in this setting. On one hand succeeding in using some artificial agents to negotiate and conduct payment transactions on user behalf may represent a considerable boost for e-cash technology, but on the other hand this may be the source of significant security challenges.

As a result, suitable trade-offs must be August 29, 2008 10:55 The International Journal of Parallel, Emergent and Distributed Systems survey 23 made by taking into account these constraints, when designing multi-agents based e-cash architectures.

D. A Multi-Agent Architecture for Electronic Payment[4]

The model has "autonomous payment clusters", in which only specialized users combine together to perform payment tasks. The proposed agent architecture is SAFER (Secure Agent Fabrication, Evolution and Roaming) is an agent framework designed to support and manage agents in e-commerce environments[5]

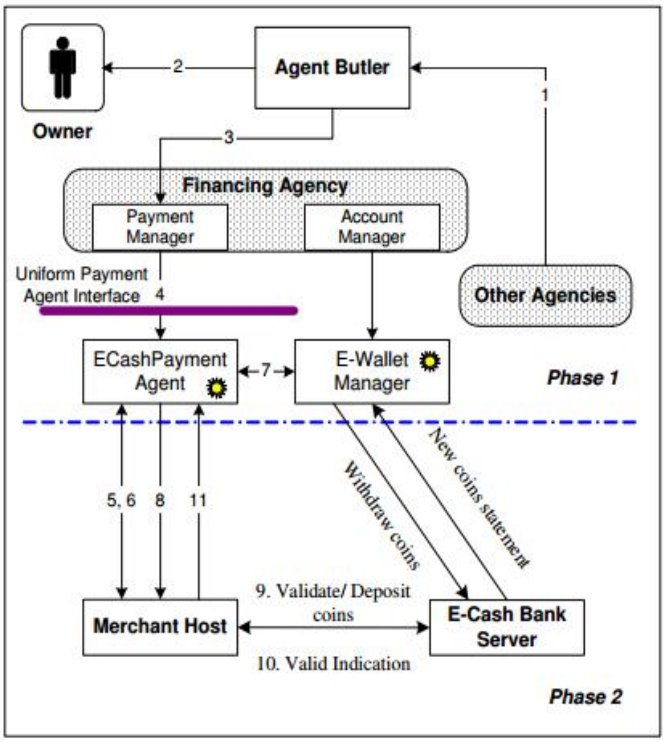


Figure 4: SAFER agent working community

A SAFER community is an autonomous agent cluster that consists of various entities. Five different entities are involved in the electronic payment implementation
Interconnected Financial Institutions (IFI),
Payment Gateway,
Trusted Third Party (TTP),
Host and Agent.

Agent receives requests from the owner and manages and dispatches mobile agents accordingly; the owner does not need to be always online it can rely on the Agent.

IFI consists of the network of banks involved in the transactions, including the customer's bank that issues the cash, the merchant's bank, and a clearing house that handles inter-bank transactions.

The payment gateway serves as front-end for the entities involved in the IFI.

TTP is neutral trusted certified host that handles trusted operations for specific purpose. It can be some Certificate Authority (CA) that is responsible for delivering trusted digital certificates agents are organized into a multi-layered structure referred to as "agency". Each "agency" represents a group of agents with specific functionality it allows agents to choose automatically the best payment option, which is a necessary task in order to make such framework useful in real-life applications.

E. Bitcoin[6]

Bitcoin as name suggests is a software-based online payment system by Satoshi Nakamoto in 2008 it was introduced as an open source software in 2009. Payments are stored in a public ledger using its account known as **bitcoin**. Payments work is person to other person and no central repository is there, so bitcoin a decentralized encrypted virtual currencyLike other proposed encrypted currencies, Bitcoin is fully decentralized and don't requires any central bank or authority. Rather, its security depends on a distributed architecture.

It deals with two assumptions:

a) The majority of its nodes are honest and so it I a sufficient proof that work can deter Sybil attacks. And, Bitcoin does not require any legal mechanisms to detect or punish any double spending nor trusted parties to be monitored.
b) It's decentralized design is responsible for Bitcoin's success, but it comes at a price: all transactions are publically conducted between cryptographically binding and random numbers

The bitcoins has to deal with the privacy weaknesses of currency. But, the available mitigations are very less. The most common suggestion is nothing but to make a laundry service in which user's exchanges different bitcoins. Many of these are used in the commercial operation today. But again these services have various limitations as the case may be: operators can steal the funds, track the easily by the generation of pattern of the coins, or even may go out of business, by having many users funds with themselves.

But the recognition of the risks bitcoins, there are many services offer short laundering periods, which lead to

minimal transaction volumes and hence for the lesser anonymity.

F. WhoPay [7]

A scalable and anonymous extension of PPay. provides security, anonymity, fairness, transferability, in addition to scalability.

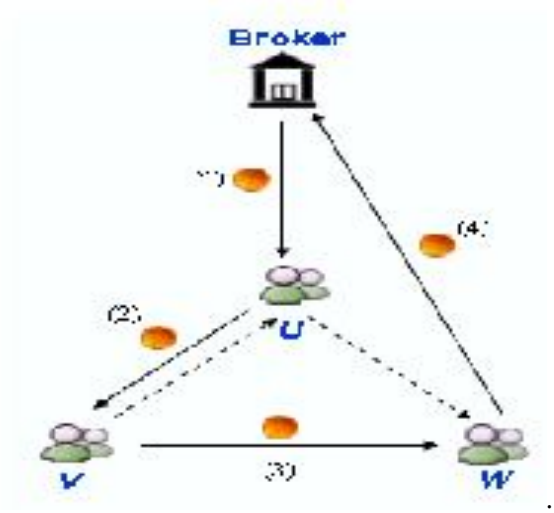
Trusted third party that plays the role of group manager for users. uses group signatures for fairness; every user is required to register with the group manager. coins are represented with public keys instead of serial numbers,transfer load is distributed across peers to ensure scalability,

To obtain a coin,
H= user generates a pair of public and private key (pkH, skH), keeps secret skH and sends pkH to the coin's owner O the public key is sent without any identification of its owner. The transfer of the coin will follow the transferred coin will be

CH = SignskO(SignB(O, pkO), pkH, seq, expdate)),

expdate =expiration date for the coin; coins must be renewed before or by the expiration date to keep their value.

The scheme for WhoPay does not provides full anonymity; while coin holder is hidden, coin ownership is exposed



Solution by author to this problem is to remove the identity of the owner from the coin, and put the onus on the owner of a private key to prove her ownership of a coin.

Double spending can be detected by the group signature scheme, but it will be costly. To address this limitation, the WhoPay model provides real-time double spending detection by implementing a publicly viewable list of valid coins. This list can be read and updated by coins owners, and only be viewed by other peers. The authors suggest implementing the coins list as an access-controlled distributed hash table (DHT).

Te huge level of trust placed in a Centralized agene, which could as per security reason is not good for the system. It simply a variant of an online scheme, where the bank plays the role of the broker. Offline payments where peers can exchange coins among themselves without involving any external entity like a broker or a bank are not supported by PPay.

G. Androulaki et al. A Reputation System forAnonymous Networks[10]

This reputation system A peer agent is represented by a pseudonym and interact with each other by discarding pseudonyms such that their identity is not revealed to each other. These pseudonyms are unlikable the individual and the peers they share the same reputation score. The values of the reputation to each peer sum up to create that peer's reputation value which are publically made available, anonymous credential systems, e-cash, and blind signatures. Reputation is exchanged in the form of e-coins called repcoins. The higher the amount of repcoins received from other users, the higher is the reputation of the user. A centralized entity bank, maintains the three data bases first the repcoin quota database which gives repcoin one peer can give to another the reputation database: amount of repcoin earned by other peers and the history database to prevent for single time utilization of the points.

Pseudonyms Generation

Each peer generates pseudonyms without registering with Bank. It just gives the random string for proving Ownership of the pseudonym.

P = f(r)

where f be one-way function, with zero-knowledge proof p be the pseudonym and r be random string.

Digital signature is used where for signing and the pseudonym is for verification.

RepCoin Withdrawal.

Let B be the Bank. The U is peer and EC [6] be the e cash. First message is from user to bank, then bank verifies and then replies to the user in accordance to validity. A wallet W of n repcoins has been withdrawn. Repcoins are used to provide anonymity. And unique spending of the coins

Reputation Award

Can be simply stated reputation providing as Two pseudonyms are there in this step, it does not involves actual identities rather two pseudonyms are involved as no direct interaction but the pseudonym are used so no information of identities are revealed.

Reputation Update.

Takes place when a peer wants to increase reputation having the repcoins received presenting itself to Bank And other peers as a pseudonym. But this cannot be simple as peer U wants to deposit a received repcoin as pseudonym everyone is unaware except U the owner of PU. So other peer may try to deposit the repcoin by to Bank as U. if peer's identity kwon then anonymity is not preserved. So peer contacts Bank gets blind permission been deposited, then deposits that blind permission.

Reputation Demonstration

For demonstrating ones reputation to other peer, both interacting with pseudonyms. For group G based on certain reputation levels, managed by Bank. For a peer to demonstrate reputation to peer verifier V, peer contacts the bank as the bank holds the group and registers in the group G.

Peer contacts a Group and registers to the group by giving master public key the public key of group and a zero knowledge proof of knowledge that master secret key belongs to it has been created correctly and he is the owner.

Group checks that peer's reputation actually belongs to that group or higher, and then access Grant for credential. Peer interacts with the verifier P under his pseudonym PU proves by executing Verify Credit having credential from group G. Specifically, PU proves that its owner has registered under a group of membership.

H. Zerocoin

Zerocoin, as the bit coin is a decentralized e cash system that uses cryptographic techniques for breaking the linked individual Bitcoin transactions without adding any trusted parties. Function and security requirements of zerocoin is that

a) A decentralized e-cash scheme.
b) A concrete instantiation and prove it secure under standard cryptographic assumptions.
c) The specific extensions required to integrate protocol into the Bitcoin system and evaluate the performance of a prototype implementation derived from the original open source bitcoind client.

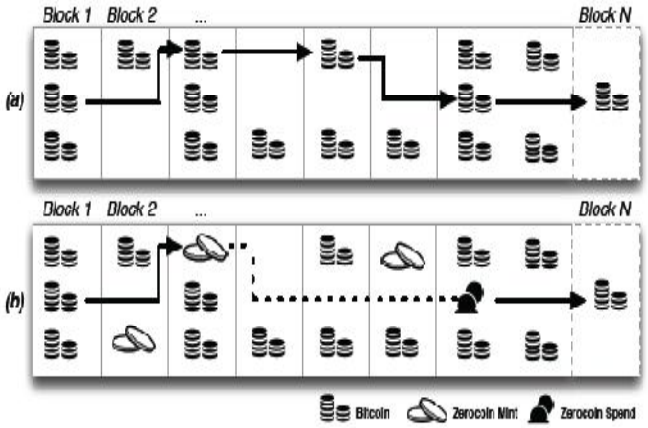


Figure 5: Two example block chains[2]

(a) Normal Bitcoin transaction history, with each transaction linked to a preceding transaction.

(b) A Zerocoin chain. The linkage between mint and spend (dotted line) cannot be determined from the block chain data.

Intuition behind the construction :

To understand Zerocoin, consider the pencil and paper protocol with example.

Consider a system where each user has the access to a physical bulletin board present. To mint a zerocoin of fixed value of a bitcoin to be added is 1,

User A first generates a random coin for which S= serial number, then commits to S using a secure digital commitment scheme.

C= commitment for coin, only opened by a random number **r** to reveal the serial number S.

A commits to the public bulletin board, along with 1 bitcoin of physical currency.

All users will accept C only if it's correct has the correct sum of currency. To redeem coin C, scanning of the bulletin board is done to obtain the set of valid commitments $(C_1, , , C_N)$ by all users in the system.

A non-interactive zero-knowledge proof is generated for the following two statements:

(a) C 2 $(C_1, , , , C_N)$ commitment are known

(b) r is hidden value when the commitment C opens to S. so for all the other users the user A, using a disguise a spend transaction has (S, _). All the others users verify this proof check S has not previously spent in any of the other transaction.

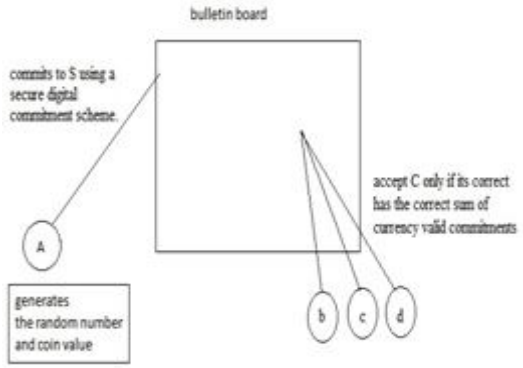


Figure 6: bulletin board scheme intuition of the proposed protocol

If above condition are satisfied then user a is allowed to make transaction of course, the But the above stated protocol is not workable:

Bulletin boards are centralized for storing the e cash and critical information. Serial numbers removed or cash may be stolen to allow spending double. To protocol work over a network, user A requires a distributed digital backing currency. The first and most basic contribution, the core of the Bitcoin protocol is the decentralized calculation.

Solution can be:

A trusted, append only bulletin board where storing the information and processing the financial transactions is done known as block chain . user A add her commitments and coins by putting them in the block chain being sure that strict protocol conditions determine when her committed funds may be accessed.

Block chain when integrated with the Bitcoin has practical challenge. As it may be difficult to prove that a commitment C is in the set (C_1, , , C_N) . Solution can be to prove the disjunction ($C = C_1$) v ($C = C_2$) v , , v ($C = C_N$). But again the proofs known as OR proof have size O(N),

This makes them impractical for small values of N.

Else it can also be solved by producing the proofs the not grow linearly as according to the size of the N.A public one-way accumulator can be used to decrease the size of this proof. One-way accumulators, allow parties to combine many elements into a constant-sized data structure, and prove one specific value is contained within the set. , the Bitcoin network computes an accumulator A over the commitments (C_1, , , C_N) with the appropriate membership witnesses for each item in the set. The spender need only prove knowledge of

One such witness. Which can reduce the cost of the spender's proof to O (log N) or even constant size.

Properties required by accumulator for the proposed protocol. No trusted third parties, the accumulator and its associated witnesses must be publicly computable and verifiable. The accumulator must combine computing party to the values in the set. The accumulator must support an efficient non-interactive witness inseparable or zero-knowledge proof of set membership. But such accumulators do exist. In our concrete proposal of Section we use a construction based on the Strong RSA accumulator

I. Mixcoin

Mixcoin is the protocol extension of the bitcoin which provides anonymous payments in Bitcoin and other similar cryptocurrencies. As the name suggests mixcoin so it mixes the coin currency and also has the accountability mechanism which exposes the case when the coin is theft.

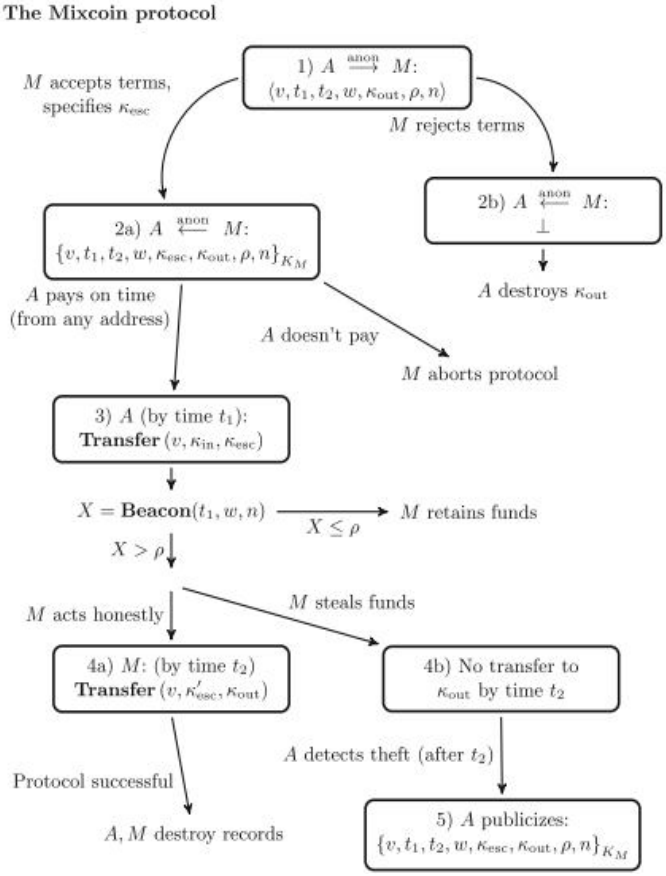


Figure 7. Working of mixcoin protocol

v = "chunk" of Alice's funds whose sizes should be standardized,

Alice will need to split her funds into multiple chunks and perform multiple sequential rounds of mixing for each.

Step 1:

Alice contacts mix by using an anonymous channel
Decides v = chunk size to be mixed
t1= deadline for Alice to send funds to the mix
t2 =deadline by which the mix must return funds to Alice
κout = where Alice wants to transfer funds Deadlines are specified as block numbers and not clock times,
ρ = mixing charge to be paid by Alice
n= nonce, for randomized mixing
w= the number of blocks mix requires to confirm Alice's payment

Step 2:

Kesc= escrow generated sends back a warranty containing all of Alice's parameters
Kesc= signed using KM.

If Alice does transfer the agreed value v to κesc by the deadline t1

Step 3:

Mix is transfers κout by time t2 then both parties should destroy their records to ensure forward anonymity against future data breaches.

If the mix fails to transfer the value v to κout by time t2 then Alice publishes her warranty Because the warranty is signed

IV. CONCLUSION

This paper has surveyed the literatures on reputation models across diverse disciplines. The centralized as well as decentralized different aggregation methods for peer to peer network. Disadvantage of each of the protocol has been pointed out. We have attempted to integrate our understanding across the surveyed literatures any tried to find out the one system proving the privacy and with strong cryptography building blocks.

	System/ Protocol	Pros	Cons	Suitable for
3.1	bitcoin	fully decentralized available mitigations are very less	network model, which had of many untrusted nodes which enter and exit the network. Moreover, the problem of choosing long term trusted parties, in the legal and regulatory grey area	decentralized
3.2	xcash	Extends cash by anonymity	Not multi agent	cen
3.3	cyberorg	the discrete logarithms unlinkability among all payments	heuristic assumption	cen
3.4	Gupta et al[7] Debit Credit Reputation Computation	Short term misuse of reputation	Less secure for the receipt off the message	de
3.5	multiagent	extensible and scalable. Real life application	Only specialzed user can participate	de
3.6	whopay	scalable and anonymous	entity like a broker or a bank are not supported	cen
3.7	Zerocoin	Zero knowledge	Minting is not accurate	de
3.8	Androulaki et al. [10] A Reputation System for Anonymous Networks	represented by a pseudonym	bank, which is a centralized entity. no negative feedback	de
3.9	zerocoin	Imposes zero knowledge		de
3.10	Mixcoin	efficient and fully compatible with Bitcoin randomized mixing fees, and an adaptation of mix networks to Bitcoin	careful consideration of some of the higher-level side channels	cen

TABLE 1. comparison of Trust models

ACKNOWLEDGMENT

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g.” Avoid the stilted expression “one of us (R. B. G.) thanks ...”. Instead, try “R.B.G. thanks...”. Put sponsor acknowledgments in the unnumbered footnote on the first page.

REFERENCES

[1] Law, Laurie, Susan Sabett, and Jerry Solinas. "How to make a mint: the cryptography of anonymous electronic cash." Am. UL Rev. 46 (1996): 1131.

[2] Petersen, Holger, and Guillaume Poupard. "Efficient scalable fair cash with off-line extortion prevention." Information and Communications Security (1997): 463-477.

[3] Nakanishi, Toru, and Yuji Sugiyama. "Unlinkable divisible electronic cash."Information Security. Springer Berlin Heidelberg, 2000. 121-134.

[4] Jakobsson, Markus, and Ari Juels. "X-cash: Executable digital cash." Financial Cryptography. Springer Berlin Heidelberg, 1998.

[5] Guan, Sheng-Uei, and Feng Hua. "A multi-agent architecture for electronic payment." International Journal of Information Technology & Decision Making2.03 (2003): 497-522.

[6] Zhu, F., Guan, S.-U., and Yang, Y. Internet Commerce and Software Agents: Cases, technologies and Opportunities. IDEA Group Publishing, 2000, ch. SAFER E-Commerce: Secure Agent Fabrication, Evolution & Roaming for E-Commerce, pp. 190–206.

[7] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system."Consulted 1.2012 (2008): 28.

[8] Wei, K., Smith, A. J., Chen, Y.-F. R., and Vo, B. Whopay: A scalable and anonymous payment system for peer-to-peer environments. In Proc. 26th IEEE International Conference on Distributed

[9] Computing Systems (ICDCS 2006) (Lisboa, Portugal, 2006), IEEE Computer Society, p. 13.

[10] Bonneau, Joseph, et al. "Mixcoin: Anonymity for Bitcoin with accountable mixes." Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2014. 486-504.