# Enhancing Privacy of Electronic Coins through Cryptography

Palak Dave
Master of Technology
Department of Computer Engineering
Charotar University of Science and Technology, Changa

Ritesh Patel
Associate Professor
Department of Computer Engineering
Charotar University of Science and Technology, Changa

## ABSTRACT

In computerized world there are different sites without further ado has the circumstances where individuals execute and the exchange is for the most part done by the money and money is presently electronic. Focal thought of this paper is to think about Al the electronic money framework. This paper portrays how the every one of the conventions works, their properties and different parameters favorable circumstances inconveniences. At long last, it finishes up by correlation of every one of these conventions.

## Keywords

E-cash, E-coins, online transaction component

## 1. INTRODUCTION

The expression "electronic Cash" frequently is connected to any electronic installment conspires that externally takes after cash. Truth be told, be that as it may, electronic money is a particular sort of electronic installment conspire, characterized by certain cryptographic properties. [1]

For the most part any e trade framework would consider the operators as bank, clients/clients and the partner and the life cycle of electronic coin includes every one of the gatherings.

Client pulls back coin from the bank.

The coin then can be traded for a few products and ventures by the clients to the shippers.

As even the trader won't keep the coin with it rather the cycle is finished when the shipper/partner stores back the con to the bank.

From above strides the cycle can be said having 3 stages withdrawal stage, the installment stage, and the store stage.

Preceding procedure is the preprocessing step which requires manages producing open keys, administration of the record. Electronic money can be sorted as on-line and disconnected. In on-line electronic money, the installment and store stages happen in the same exchange. So we can reason that the coin is checked each by the bank at the season of installment so bank to be on-line for each coin traded between the spenders and the shippers.

In disconnected electronic money plots, the coins are checked after the exchange at some advantageous time for both shippers and the bank so that the bank does not need to be required in each installment exchange. Be that as it may, as the coins are not confirmed at the season of installment, there is a potential for tricky spenders to twofold spend their coins. This is in light of the fact that mechanized cash, which is basically an arrangement of numbers, is anything but difficult to duplicate. Another necessity that can emerge in electronic coins is the requirement for secrecy.

TERMINOLOGIES RELATED TO TRUST

A. Classification of electronic cash system

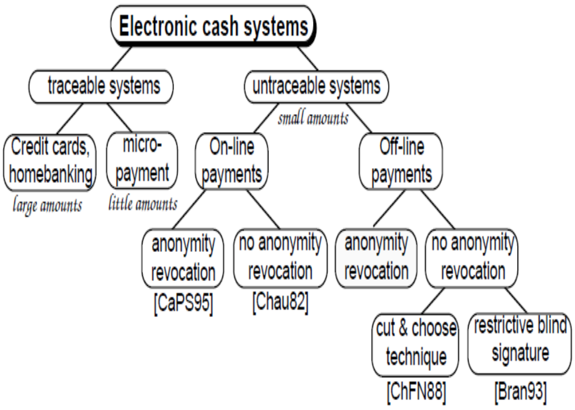

**Figure 1: Classification of electronic cash system**

B. Classification of electronic cash system

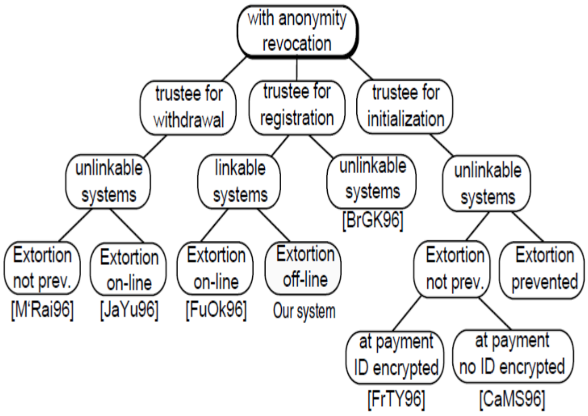

**Figure 2: Classification of electronic cash system**

In this setting seven headliners are discernable:

1. **Initialisation:** Choice of framework parameters and key sets of all elements.

**2. Opening account**: The bank opens a client record and registers his own information.

**3. Registration**: In the pseudonymous frameworks, the client registers at the trustee.

**4. Withdrawal**: The client pulls back computerized coins from his record onto his gadget.

**5. Payment:** The client pays at the shop utilizing the coins put away on his gadget.

**6. Deposit:** The shop stores the computerized coins at the bank and is credited likewise.

**7. Revocation:** The trustee can register either the state of the coin from the withdrawal transcript or to process the client's personality from the installment transcript keeping in mind the end goal to discourage any immaculate wrong doing.

## 2. SOME E CASH BASED PROTOCOLS

### 2.1 Mintcoin[5]

A few notoriety frameworks have been sent in down to earth applications or proposed in the writing. This paper portrays another framework called the beta notoriety framework which depends on utilizing beta likelihood thickness capacities to join input and infer notoriety appraisals. The benefit of the beta notoriety framework is adaptability and effortlessness and additionally its establishment on the hypothesis of measurements.

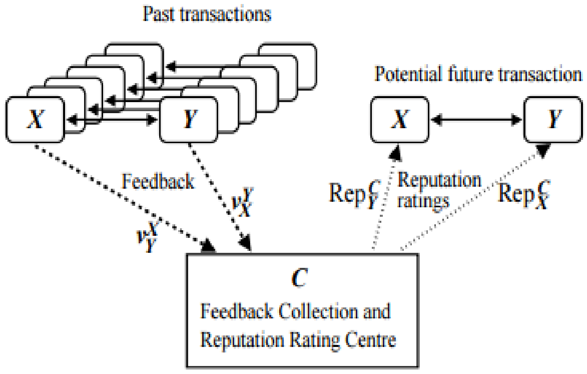

**Figure 3: F estimations of a paired tree of 3 levels**

Deposit:
Over-spending is kept an eye on the distinguishably run the show. In the event that it doesn't happen, the paid sum is saved in the record of the shop. Else, the over-high-roller can be recognized by proprietor following convention.

Anonymity Revocation:
The proprietor following convention is the same as the recognizable proof of the endorser in the first gathering mark conspire. The coin following convention is orchestrated from that of the e-coupon framework

### 2.2 Xcash[6]

X-cash or executable automated cash for the standard substance. A touch of X-cash involves a stamped verification issued by the bank and a program which for creating the entirety which the client will pay for any generous component.

At first client C will get a support from bank affirming to make portions to the buyer. The range will similarly be picked by the client for the portion considering that the offer limit will be produced and encoded in a touch of executable code. The client will then make the X-cash by uniting the stamped executable code and the validation issued by the bank. The executable is checked using e.

skC = private key PkC = open key contained in the marked endorsement issued by the bank.

To purchase something,
C sends X-money to the dealer M.

M checks the rightness of the mark and assess offer by executing capacity.

M will contact C's bank if it get satisfied. By allowing the offer to go in a run of the mill component with relating stock or portions, the proposed configuration grants mechanized exchange to be used out significantly scattered settings while ensuring the security of passed on resources. Disregarding the way that the fundamental arrangement proposed in does not support lack of clarity, the makers ensure that it is possible to extend it to address such property. Not a multi-authority tradition, it may be said that co operations are confined to a seller and a customer, or a dealer and a bank.

### 2.3 CyberOrg[7]

A model for various leveled coordination of asset proposed in , likewise permits the making of operators conveying e-money. The proposed approach concentrates more on the usage of specialists and their communications as opposed to tending to security necessities of e-cash installment.

Explores on utilizing multi-specialists frameworks for e-money installments are very later. A first clarification is that multi-operator setting makes an extra layer of challenges on top of an officially complex arrangement of issues. Later on, we should address a few challenges in this setting.

On one hand prevailing with regards to utilizing some fake specialists to arrange and direct installment exchanges for client sake may speak to an impressive lift for e-money innovation, however then again this might be the wellspring of noteworthy security challenges.

Subsequently, reasonable exchange offs must be made by considering these requirements, when outlining multi-specialists based e-money models.

### 2.4 Gupta et al. Debit Credit Computation[8]

Reason for a motivation framework and appropriate for interactive media transfer and download.

Three tunable framework parameters are there in this convention:

Document estimate consider f, f ∈ number, this parameters measures the level of MBytes information relying upon expanding the notoriety score.

Data transmission consider b, b ∈ genuine, distinguishes hubs for transfer speed

Time calculate hours t, t ∈ number. Period for the associate participation by sharing and remaining on the web is remunerated.

The notoriety is registered by the operator called notoriety calculation specialist to intermittently redesign to the input giving specialist's notoriety, and to guarantee that criticism esteem gave by them is kept locally with the goal that it can be recovered rapidly. Notoriety calculation operator does not assume any part while Reason for a motivation framework and appropriate for interactive media transfer and download.

Three tunable framework parameters are there in this convention:

Document estimate consider f, f ∈ number, this parameters measures the level of MBytes information relying upon expanding the notoriety score.

Data transmission considers b, b ∈ genuine, distinguishes hubs for transfer speed time calculates hour's t, t ∈ number. Period for the associate participation by sharing and remaining on the web is remunerated.

The notoriety is registered by the operator called notoriety calculation specialist to intermittently redesign to the input giving specialist's notoriety, and to guarantee that criticism esteem gave by them is kept locally with the goal that it can be recovered rapidly. Notoriety calculation operator does not assume any part while looking for and recouping with the objective that it gets to be bottleneck for the customary operation of the P2P system:

Question Response Credit (QRC)
Administrators at initially need to enlist then they get affirmation for giving their feedback to the system setting up the request response messages.

On key match i.e. open and private key are delivered on the selection. The administrator sends this confirmation of technique to the RCA for getting the credits.

By then RCA uses the overall public key to check the Process confirmation from the administrator and encodes stature score.

Upload Credit (UC):
Every specialist gets kudos for giving any substance identified with mixed media and gets credit, (open, private) key combine is indicated here {PKr, SKr} and sender peers by {PKs, SKs}.

At the period of the record download
For downloading {requester character, filename, record gauge, time stamp} and scramble it with its private key and send to the up loader/sender agnates.

On tolerating the information from the above walk and unscrambling it by using the requester's open key and a short time later encodes the receipt of the trade by its private key.

Download Debit (DD)
While downloading a document a specialist needs to charge for downloading the record. For negative notoriety esteem, the RCA holds the negative scores as charge state with itself until those companions send a few credits for preparing.

Sharing Credit (SC):
This progression permits the enrolled operators to for credit to be shared for remaining on the web, in view of the quantity of records they are sharing

It can be accomplished in two ways both the ways requires the RCA to accomplish more work can likewise bring about some measure of blunder in the stature calculation methodology.

To start with path manages exchange state being recorded by RCA to check the era for which specific operator was on the web and aggregate sum of information shared by a specialist.

Second one occasional checking of the mutual indexes of operators by the RCA. Be that as it may, this strategy is more wrong.

Since the credit relies on upon the checking recurrence.

Pseudonyms Generation
Each associate produces pen names enlisting with Bank. It just gives the irregular string for demonstrating Ownership of the alias.

P = f(r)

where f be one-route work, with zero-information evidence

p be the pen name r be arbitrary string. Advanced mark is utilized where for marking and the alias for confirmation.

RepCoin Withdrawal
Give B a chance to be the Bank. The U is companion and EC [6] be the e money. To begin with message is from client to bank, then bank confirms and afterward answers to the client in agreement to legitimacy. A wallet W of n repcoins has been pulled back. Repcoins are utilized to give namelessness. Also, one of a kind spending of the coins

Reputation Award
Can be just expressed notoriety giving as Two pen names there in this progression, it doesn't includes real characters rather two nom de plumes required as no immediate cooperation yet the nom de plume utilized so no data of personalities are uncovered.

Reputation Update
Happens when an associate needs to build notoriety having the repcoins gotten introducing itself to Bank.

What's more, different companions as a pen name. Yet, this can't be straightforward as companion U needs to store a got repcoin as pen name is unconscious aside from U the proprietor of PU. So other companion may attempt to store the repcoin by to Bank as U. in the event that associate's character kwon then obscurity is not safeguarded. So peer contacts Bank gets visually impaired consent been saved, then stores that visually impaired authorization.

Reputation Demonstration
For exhibiting ones notoriety to other companion, both interfacing with nom de plumes. For gathering G in light of certain notoriety levels, oversaw by Bank. For a companion to exhibit notoriety to associate verifier V, peer contacts the bank as the bank holds the gathering and registers in the gathering G.

Peer contacts a Group and registers to the gathering by giving expert open key the general population key of gathering and a zero information confirmation of learning that ace mystery key has a place with it has been made effectively and he is the proprietor.

Gather watches that companion's notoriety really has a place with that gathering or higher and afterward get to Grant for accreditation.

Peer communicates with the verifier P under his nom de plume demonstrates by executing Verify Credit having certification from gathering G. In particular, PU demonstrates that its proprietor has enrolled under a gathering of participation.

## 2.5A Multi Agent Architecture for Electronic Payment [9]

The model has "self-ruling installment bunches", in which just particular clients consolidate together to perform installment undertakings. The proposed specialist engineering is SAFER (Secure Agent Fabrication, Evolution and Roaming) is an operator system intended to bolster and oversee operators in internet business environments [5].

A SAFER people group is a self-ruling operator bunch that comprises of different substances. Five distinct elements are included in the electronic installment execution.

Interconnected Financial Institutions (IFI),
Installment Gateway,
Trusted Third Party (TTP),
Host and Agent.

Specialist gets demands from the proprietor and oversees and dispatches portable operators in like manner; the proprietor does not should be constantly online it can depend on the Agent.

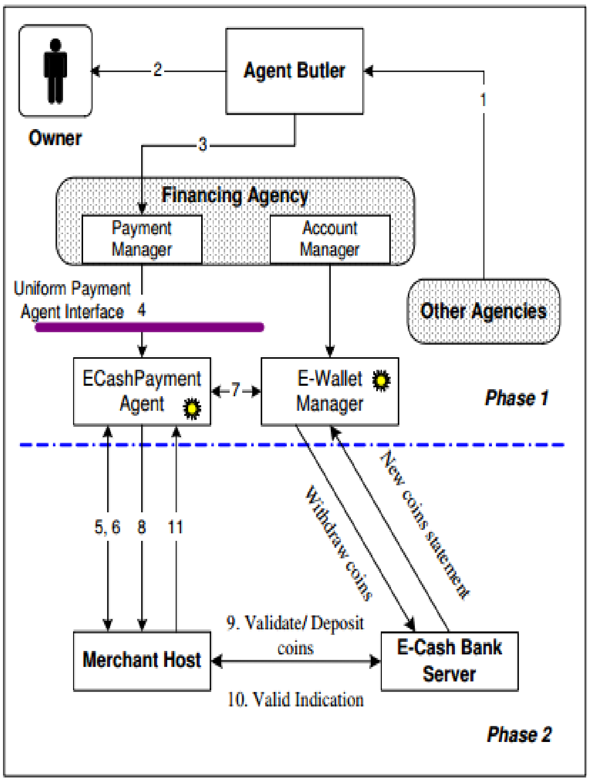

**Figure 4: SAFER agent working community**

IFI comprises of the system of banks required in the exchanges, including the client's bank that issues the money, the shipper's bank, and a clearing house that handles between bank exchanges.

The installment passage fills in as front-end for the elements required in the IFI.

TTP is nonpartisan trusted ensured have that handles trusted operations for particular reason. It can be some Certificate

Authority (CA) that is in charge of conveying trusted computerized declarations.

Specialists are sorted out into a multi-layered structure alluded to as "office". Every "organization" speaks to a gathering of operators with particular usefulness.

it permits operators to pick naturally the best installment choice, which is an important assignment with a specific end goal to make such system valuable, in actuality, applications.

## 2.6 Bitcoin[6]

Bitcoin as name recommends is a product based online installment framework by Satoshi Nakamoto in 2008 it was presented as an open source programming in 2009. Installments are put away in an open record utilizing its record known as bitcoin. Installments work is individual to other individual and no focal storehouse is there, so bitcoin a decentralized scrambled virtual currencyLike other proposed encoded monetary forms, Bitcoin is completely decentralized and don't requires any national bank or specialist. Or maybe, its security relies on upon a disseminated design.

It manages two suspicions:

a) The greater part of its hubs are straightforward thus it I an adequate confirmation that work can dissuade Sybil assaults. What's more, Bitcoin does not require any lawful systems to distinguish or rebuff any twofold spending nor confided in gatherings to be observed.

b) Its decentralized plan is in charge of Bitcoin's prosperity, yet it includes some significant downfalls: all exchanges are publically led between cryptographically official and arbitrary numbers.

The bit coins needs to manage the security shortcomings of cash. In any case, the accessible alleviations are less. The most well-known proposal is only to make a clothing administration in which client's trade's distinctive bitcoins. A large portion of these are utilized as a part of the business operation today. Be that as it may, again these administrations have different impediments by and large: administrators can take the assets, track the effectively by the era of example of the coins, or even may leave business, by having numerous clients' reserves with themselves.

Be that as it may, the acknowledgment of the dangers bitcoins, there are numerous administrations offer short washing periods, which prompt negligible exchange volumes and consequently for the lesser namelessness.

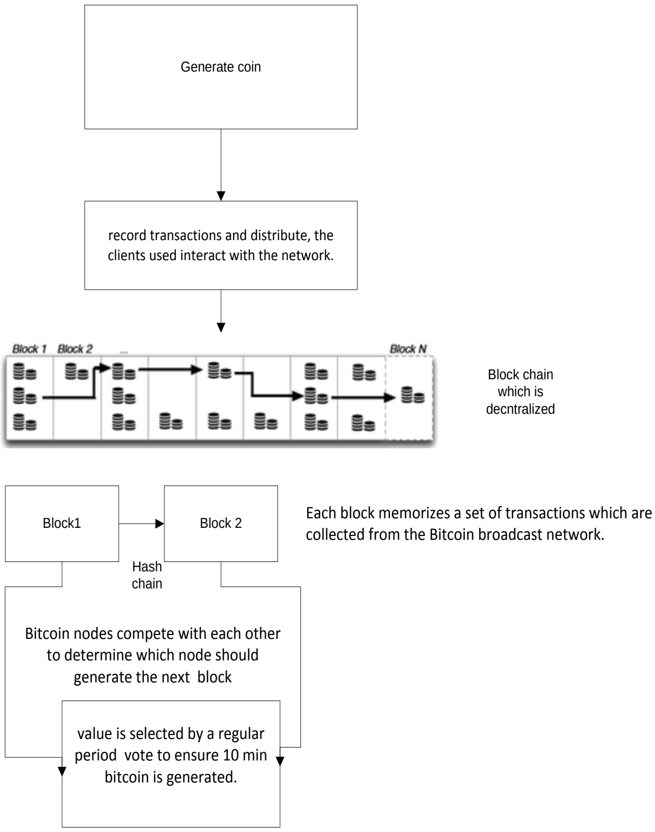
Generate coin
record transactions and distribute, the clients used interact with the network.
Block 1
Block 2
...
Block N
Block chain which is decntralized
Block1
Block 2
Hash chain
Each block memorizes a set of transactions which are collected from the Bitcoin broadcast network.
Bitcoin nodes compete with each other to determine which node should generate the next block
value is selected by a regular period vote to ensure 10 min bitcoin is generated.

**Figure 5: Working of Bitcoin**

## 2.7 Who Pay [7]

An adaptable and mysterious augmentation of PPay. Gives security, obscurity, decency, transferability, notwithstanding versatility.

Trusted outsider that assumes the part of gathering supervisor for clients. Utilizes assemble marks for decency; each client is required to enroll with the gathering director.

coins are spoken to with open keys rather than serial numbers, transfer load is conveyed crosswise over companions to guarantee adaptability, To get a coin,

H= client

Creates a couple of open and private key (pkH, skH),

Keeps mystery skH and sends pkH to the coin's proprietor O.

The general population key is sent with no distinguishing proof of its proprietor. The exchange of the coin will take after the exchanged coin will be

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

expdate =expiration date for the coin; coins must be reestablished before or by the termination date to keep their esteem.

The plan for WhoPay does not give full namelessness; while coin holder is shrouded, coin possession is uncovered.

coins are addressed with open keys as opposed to serial numbers,transfer load is passed on transversely over associates to ensure versatility,

To get a coin,

H= customer

makes several open and private key (pkH, skH),

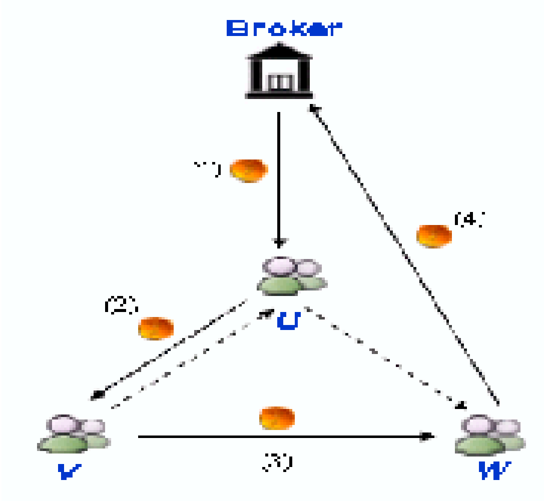

**Figure 6: WhoPay Broker**

Keeps puzzle skH and sends pkH to the coin's proprietor O.

The all inclusive community key is sent with no recognizing verification of its proprietor. The trading of the coin will take after the traded coin will be

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

expdate =expiration date for the coin; coins must be restored before or by the end date to keep their regard.

The arrangement for WhoPay does not give full anonymity; while coin holder is covered, coin ownership is revealed.

## 2.8 Androulaki et al. A Repcoin[10]

This notoriety framework A companion specialist is spoken to by a nom de plume cooperate with each other by disposing of nom de plumes that their character is not uncovered to each other. These nom de plumes unlikable the individual and the associates they have a similar notoriety score. The estimations of the notoriety to each associate total up to make that companion's notoriety esteem which are publically made accessible.

Unknown accreditation frameworks, e-money, and visually impaired marks. Notoriety is traded as e-coins called repcoins. The higher the measure of repcoins got from different clients, the higher is the notoriety of the client. A unified substance bank, keeps up the three information bases first the repcoin amount database which gives repcoin one companion can provide for another

the notoriety database: measure of repcoin earned by different companions and the history database to counteract for single time use of the focuses.

**Pseudonyms Generation**
Each associate produces pen names enlisting with Bank. It just gives the irregular string for demonstrating Ownership of the alias.

P = f(r)

where f be one-route work, with zero-information evidence

p be the pen name r be arbitrary string. Advanced mark is utilized where for marking and the alias for confirmation.

**RepCoin Withdrawal**
Give B a chance to be the Bank. The U is companion and EC [6] be the e money. To begin with message is from client to bank, then bank confirms and afterward answers to the client in agreement to legitimacy. A wallet W of n repcoins has been pulled back. Repcoins are utilized to give namelessness. Also, one of a kind spending of the coins.

**Reputation Award**
Can be just expressed notoriety giving as Two pen names there in this progression, it doesn't includes real characters rather two nom de plumes required as no immediate cooperation yet the nom de plume utilized so no data of personalities are uncovered.

**Reputation Update**.
Happens when an associate needs to build notoriety having the repcoins gotten introducing itself to Bank

What's more, different companions as a pen name. Yet, this can't be straightforward as companion U needs to store a got repcoin as pen name is unconscious aside from U the proprietor of PU. So other companion may attempt to store the repcoin by to Bank as U. in the event that associate's character kwon then obscurity is not safeguarded. So peer contacts Bank gets visually impaired consent been saved, then stores that visually impaired authorization.

**Reputation Demonstration**
For exhibiting ones notoriety to other companion, both Interfacing with nom de plumes. For gathering G in light of certain notoriety levels, oversaw by Bank. For a companion to exhibit notoriety to associate verifier V, peer contacts the bank as the bank holds the gathering and registers in the gathering G.

Peer contacts a Group and registers to the gathering by giving expert open key the general population key of gathering and a zero information confirmation of learning that ace mystery key has a place with it has been made effectively and he is the proprietor.

Gather watches that companion's notoriety really has a place with that gathering or higher and afterward get to Grant for accreditation.

Peer communicates with the verifier P under his nom de plume demonstrates by executing Verify Credit having certification from gathering G. In particular, PU demonstrates that its proprietor has enrolled under a gathering of participation.

## 2.9 Zerocoin [13]

Zerocoin, as the bit coin is a decentralized e money framework that utilizations cryptographic strategies for breaking the connected individual Bitcoin exchanges without including any put stock in gatherings. A capacity and security prerequisite of zerocoin is that a decentralized e-money plot.

A solid instantiation and demonstrate it secure under standard cryptographic suppositions.

The particular augmentations required to coordinate convention into the Bitcoin framework and assess the execution of a model usage got from the first open source bitcoind customer.

Authority (CA) that is in charge of conveying trusted computerized declarations.

Specialists are sorted out into a multi-layered structure alluded to as "office". Every "organization" speaks to a gathering of operators with particular usefulness.

it permits operators to pick naturally the best installment choice, which is an important assignment with a specific end goal to make such system valuable, in actuality, applications.

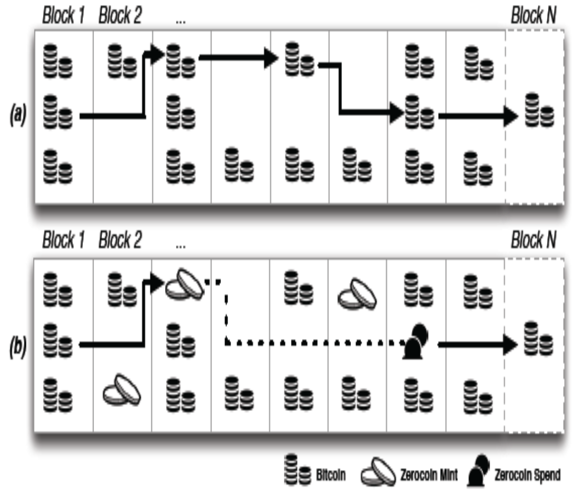

**Figure 7: Two example block chains**

(a) Ordinary Bitcoin exchange history, with every exchange connected to a first exchange.

(b) A Zerocoin chain. The linkage amongst mint and spend (specked line) can't be resolved from the square chain information.

Intuition behind the construction:
To comprehend Zerocoin, consider the pencil and paper convention with case.

Consider a framework where every client has the entrance to a physical release board show. To mint a zerocoin of settled estimation of a bitcoin to be included is 1,

Client A first creates an arbitrary coin for which S= serial number, then focuses on S utilizing a safe advanced duty plot.

C= responsibility for coin, just opened by an irregular number r to uncover the serial number S.

A focuses on general society announcement board, alongside 1 bitcoin of physical cash.

All clients will acknowledge C just if it's right has the right entirety of money. To reclaim coin C, filtering of the notice board is done to acquire the arrangement of substantial responsibilities (C1, , CN) by all clients in the framework.

A non-intuitive zero-learning verification is created for the accompanying two articulations:

(a) C 2 (C1, , CN) responsibility 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.

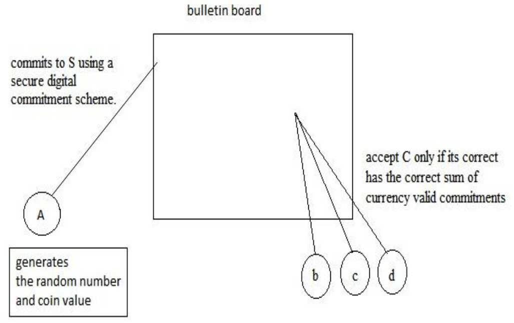
bulletin board
commits to S using a secure digital commitment scheme.
accept C only if its correct has the correct sum of currency valid commitments
A
generates the random number and coin value
b
c
d

**Figure 8: bulletin board scheme intuition of the proposed protocol**

In the event that above condition are fulfilled then client an is permitted to make exchange obviously, the But the above expressed convention is not workable:

Release sheets are unified for putting away the e money and basic data. Serial numbers expelled or money might be stolen to permit spending twofold. To convention work over a system, client A requires disseminated advanced support money. The first and most essential commitment, the center of the Bitcoin convention is the decentralized figuring.

Arrangement can be:

A trusted, attach just notice board where putting away the data and preparing the money related exchanges is done known as piece chain. Client an include her responsibilities and coins by placing them in the piece chain being certain that strict convention conditions decide when her submitted assets might be gotten too.

Square chain when incorporated with the Bitcoin has handy test. As it might be hard to demonstrate that a promise C is in the set (C1, , CN). Arrangement can be to demonstrate the disjunction (C = C1) v (C = C2) v, v (C =CN). In any case, again the confirmations known as OR evidence have measure O(N), This makes them illogical for little estimations of N.

Else it can likewise be illuminated by creating the evidences the not develop straightly as indicated by the span of the N.A open one-way aggregator can be utilized to diminish the measure of this proof. . One-way aggregators, permit gatherings to consolidate numerous components into a consistent estimated information structure, and demonstrate one particular esteem is contained inside the set. , the Bitcoin organize figures a gatherer An over the duties (C1, CN) with the proper enrollment witnesses for everything in the set. The high-roller require just demonstrate learning of

One such witness. This can decrease the cost of the high-roller's confirmation to O (log N) or even consistent size.

Properties required by aggregator for the proposed convention. No trusted outsiders, the aggregator and its related witnesses must be freely calculable and evident. The gatherer must join processing gathering to the qualities in the set. The aggregator must support a productive non-intelligent witness indistinguishable or zero-learning evidence of set enrollment. In any case, such collectors do exist. In our solid proposition of Section we utilize a development in view of the Strong RSA collector.

## 2.10 Mixcoin[15]

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.

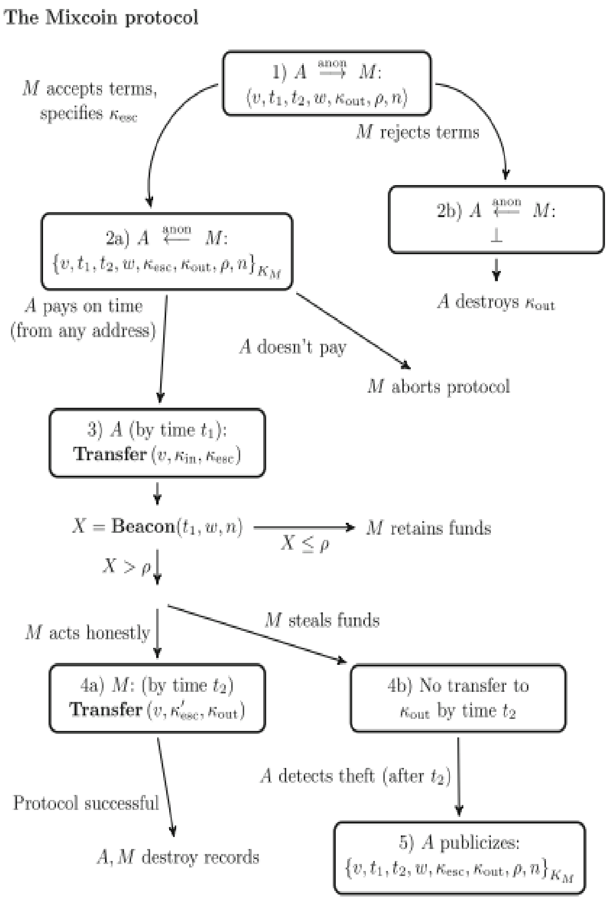
The Mixcoin protocol
1) $A \overset{\text{anon}}{\longrightarrow} M$: $(v, t_1, t_2, w, \kappa_{\text{out}}, \rho, n)$
$M$ accepts terms, specifies $\kappa_{\text{esc}}$
$M$ rejects terms
2a) $A \overset{\text{anon}}{\longleftarrow} M$: $\{v, t_1, t_2, w, \kappa_{\text{esc}}, \kappa_{\text{out}}, \rho, n\}_{K_M}$
2b) $A \overset{\text{anon}}{\longleftarrow} M$: $\perp$
$A$ destroys $\kappa_{\text{out}}$
$A$ pays on time (from any address)
$A$ doesn't pay
$M$ aborts protocol
3) $A$ (by time $t_1$): Transfer $(v, \kappa_{\text{in}}, \kappa_{\text{esc}})$
$X = \textbf{Beacon}(t_1, w, n)$
$X \leq \rho$
$M$ retains funds
$X > \rho$
$M$ acts honestly
$M$ steals funds
4a) $M$: (by time $t_2$) Transfer $(v, \kappa'_{\text{esc}}, \kappa_{\text{out}})$
4b) No transfer to $\kappa_{\text{out}}$ by time $t_2$
$A$ detects theft (after $t_2$)
Protocol successful
$A, M$ destroy records
5) $A$ publicizes: $\{v, t_1, t_2, w, \kappa_{\text{esc}}, \kappa_{\text{out}}, \rho, n\}_{K_M}$

**Figure 9: Working of mixcoin protocol**

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

Alice should part her assets into various pieces and play out numerous successive rounds of blending for each.

Step 1:

Alice contacts blend by utilizing an unknown channel

Chooses v = lump size to be blended

t1= due date for Alice to send assets to the blend

t2 =deadline by which the blend must return assets to Alice

κout = where Alice needs to exchange reserves Deadlines are indicated as piece numbers and not clock times,

ρ = blending charge to be paid by Alice

n= nonce, for randomized blending

w= the quantity of squares blend requires to affirm Alice's installment.

Step 2:

Kesc= escrow produced sends back a guarantee containing the greater part of Alice's parameters

Kesc= marked utilizing KM.

On the off chance that Alice transfers the concurred esteem v to κesc by the due date t1

Step 3: Mix is exchanges κout by time t2

At that point both sides ought to crush their records to guarantee forward namelessness against future information ruptures.

In the event that the blend neglects to exchange the esteem v to κout by time t2 then Alice distributes her guarantee on the grounds that the guarantee is agreed upon.

**TABLE 1. Comparison of Trust models**

| System/<br>Protocol | Pros | Cons |
|---|---|---|
| Bitcoin | Fully decentralized | Untrusted nodes can enter/exit network. |
| Xcash | Extends cash by anonymity | Not multi agent |
| Cyberorg | The discrete logarithms unlinkability | Heuristic assumption |
| Gupta et al Debit Credit Computation | Short term misuse of cash cannot be done. | Less secure receipt off the message |
| Multiagent | Extensible and scalable. | Specialized use participate |
| Whopay | Scalable and anonymous | Entity like a broker or a bank are not supported |

| | | |
|---|---|---|
| Zerocoin | Zero knowledge | Minting is not accurate |
| Androulaki et al. [10] A Reputation System for<br>Unknown Networks | Represented by a pseudonym | Bank, which is a centralized<br>Entity. No negative feedback |
| Zerocoin | Imposes zero knowledge | -- |
| Mixcoin | Effective with Bitcoin<br>randomized blending charges | Careful consideration of higher-level side channels |

## 3. 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.therefor enhancing security by hiding origin, destination or amount of the payment through transaction. Privacy can be enhanced in electronic cash system both in terms of functionality & efficiency. So reward coin that made suggest gift can be applied in zero knowledge proof for securing currency in payment transaction.

## 4. ACKNOWLEDGMENTS

Wish to express deep Sense of gratitude to Prof.Ritesh Patel & faculty of Computer Engineering, Charotar University of Science and Technology, changa under whose valuable Guidance, constant endeavor, continuous encouragement, Unceasing interest and constructive great suggestions made this task success.

## 5. REFERENCES

[1] Erl, H-P. (1996) The Emergence of Electronic Commerce and Electronic Forms of Money. Munich: Technical University of Munich.

[2] Hayes, D.G. et.al. (1996). Towards Electronic Money and Banking: The Role of Government. A Conference Sponsored by the United States Department of the Treasury. Washington, DC. September 19-20.

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

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

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

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

[7] Jamali, Nadeem, Xinghui Zhao, and Gul A. Agha. "Decentralized resource control for multi-agent systems." Proceedings of the Third International Joint Conference on Autonomous Agents and Multiagent Systems-Volume 3. IEEE Computer Society, 2004.

[8] Gupta, Minaxi, Paul Judge, and Mostafa Ammar. "A reputation system for peer-to-peer networks." Proceedings of the 13th international workshop on Network and operating systems support for digital audio and video. ACM, 2003.

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

[10] 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.

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

[12] 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

[13] Miers, Ian, et al. "Zerocoin: Anonymous distributed e-cash from bitcoin."Security and Privacy (SP), 2013 IEEE Symposium on. IEEE, 2013.

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

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