Enhancing Privacy of e-Coins through Cryptographic approach

Dewangini Sharma[1], Prof. Manoj Patel[2]
[1, 2] Department of Computer Engineering
[1, 2] ACET Kalol GTU

Abstract- *Electronic transactions are common now days as almost everyone in this online world deals with the e cash. Bit coin was the initial and first cryptographic currency, which for the security reasons was replaced by zero coin the coin transfer by zero knowledge protocol so that no knowledge is passed for the minting the coin or redeeming the coin. We have proposed homomorphic[4] addition to secure the reward points. Simulation results are concluded in the paper.*

I. INTRODUCTION

The term "electronic cash" often is applied to any electronic payment scheme that apparently bear a resemblance to money. In fact, however, electronic cash is a precise class of electronic payment scheme, defined by firm 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.

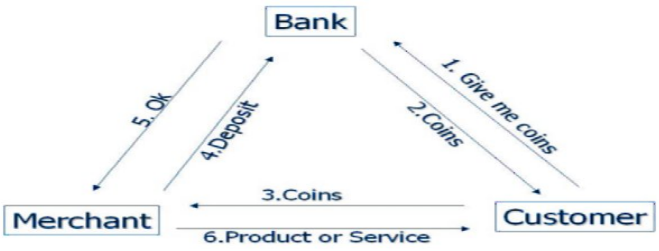

Figure 1: Life cycle of e cash [2]

From figure 1 cash has 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.

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 currency.

Bitcoins are created for the reward of task related to payments where users offers their computing power to verify and record payments termed as mining, individual as well as companies can be a part of this activity for exchange of the transaction fees and new created bitcoins. Except mining, they can be gained by the exchange for money, products, and services. Users can both send and receive bitcoins electronically for a way of transaction fee by using wallet software.

Bitcoin can also be termed as the e cash which is used as payment for products and service fees are less than that of by credit card processors. The European Banking Authority has warned that bitcoin lacks consumer protections. Unlike credit cards, any fees are paid by the purchaser not the vendor. Bitcoins can be stolen and charge backs are

impossible. As of July 2013 the commercial use of bitcoin was small compared to its use by speculators, which has contributed to price volatility.

Bitcoin has been a subject of concerns that it can be used for illegal activities, much like cash.

II. BACKGROUND

2.1 Classification of e cash system

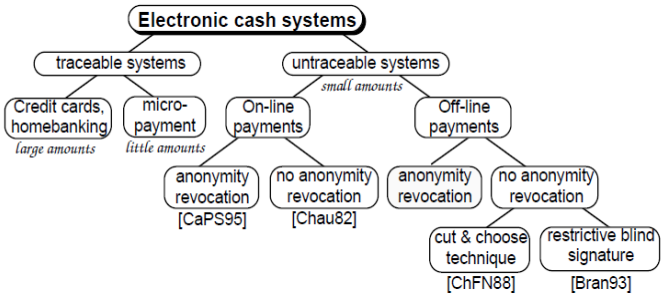

Figure 2: Classification of Electronic cash system[2]

Seven main events are distinguishable:

1.Initialisation: Choice of system parameters and keypairs 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: Shop deposits the digital coins at the bank and is credited accordingly.
7. Revocation: The trustee gets the coin from the withdrawal transcript or to compute the user's identity from the payment transcript in order to deter any perfect crime

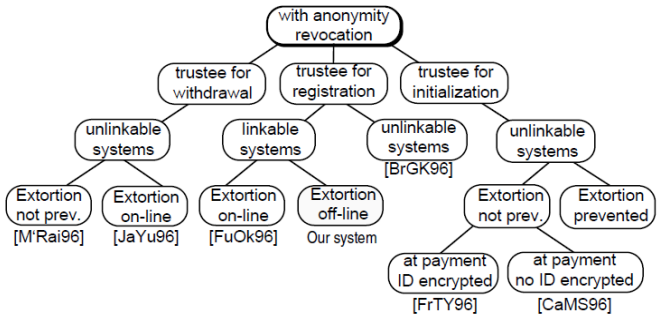

Figure 3: Classification of Electronic cash system with anonymity revocation[2]

2.2 Bitcoin Transactions

The electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

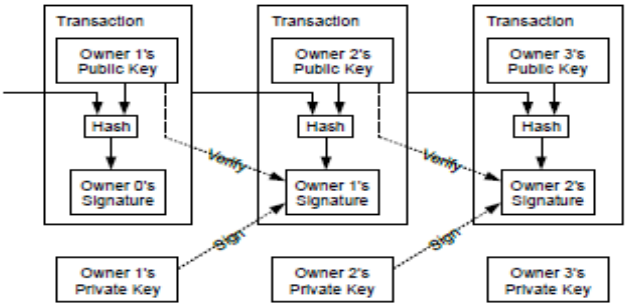

Figure 4: Transaction chain by hash key

2.3 Zero Knowledge Proof

The first efficient statistical zero-knowledge protocols to prove statements such as

(a) A committed number is a pseudo-prime.
(b) A committed/revealed number is the product of two safe primes
(c) A given value is of large order modulo that consists of 2 safe prime factors.

Apart from the validity of the computation, no other information about the modulus e.g., a generator which order equals the modulus or any other operand is given. In spite of the Bitcoin's user base seemed to be anonymous[7] risking their money and paying transaction fees. One illustration of this is the existence of laundries that for a fee will combine together different users' funds in the hopes that shuffling makes them difficult to trace. Because such systems require the users to trust the laundry to both

(a) not record how the mixing is done
(b) Give the users back the money they put , use of these involves a fair amount of risk.

2.4 Decentralized Ecash

The decentralized e cash scheme is **to anonymize the Bitcoin network** uses a type of cryptographic electronic currency's the name suggests decentralization means it does not requires any kind of central authority to issue the coin.

Table 1 Presents the comparison within the literature survey done with various papers C-centralized system D is decentralized system. pros, cons, and the scenario its is suitable for.

	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 DebitCredit Computation	Short term misuse of cash cannot be done.	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. 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

IV. PROOF OF PROPOSED WORK

4.1 Base Work

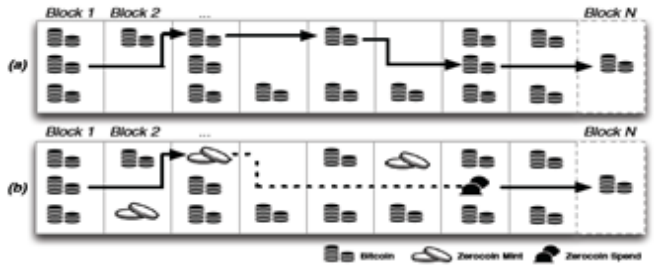

Figure 5 bitcoin and zerocoin working

Algorithm of the zerocoin:

1.	Setup(1λ): parameter.	AccumSetup (1λ) gives the output (N, u). generate prime numbers p, q where p = 2w q + 1 for w ≥ 1 choose random generators g, h G = (g) = (h) and G ε Zq* output of step 1 = (N, u, p, q, g, h)
2.	Mint(parameter) : (c, skc).	input = Select S,r ← Zq* c ← gS hr mod p such that {c prime | c ∈[A , B]} Set skc = (S, r) output (c, skc)
3.	Spend (parameters; c; skc, R, C):	(Π, S). If c not belongs C output ⊥. Compute A ← Accumulate((N, u), C) ω ← GenWitness((N, u), c, C). Output (π, S) where π IS signature of knowledge: π = ZKSoK[R]{(c, w, r): AccVerify((N, u), A, c, w) = 1 ∧ c = gS hr }
4.	Verify (params, π, S, R, C) → {0, 1}.	π= proof, S serial number C = set of coins, A ← Accumulate((N, u), C).

Verify that Π is the signature of knowledge on R using the known public values.
If the proof verifies successfully, output 1, otherwise output 0.

The zerocoin assumes a trusted setup process for generating the parameters. The accumulator trapdoor (p, q) is not used subsequent to the Setup procedure and can therefore be destroyed immediately after the parameters are generated.

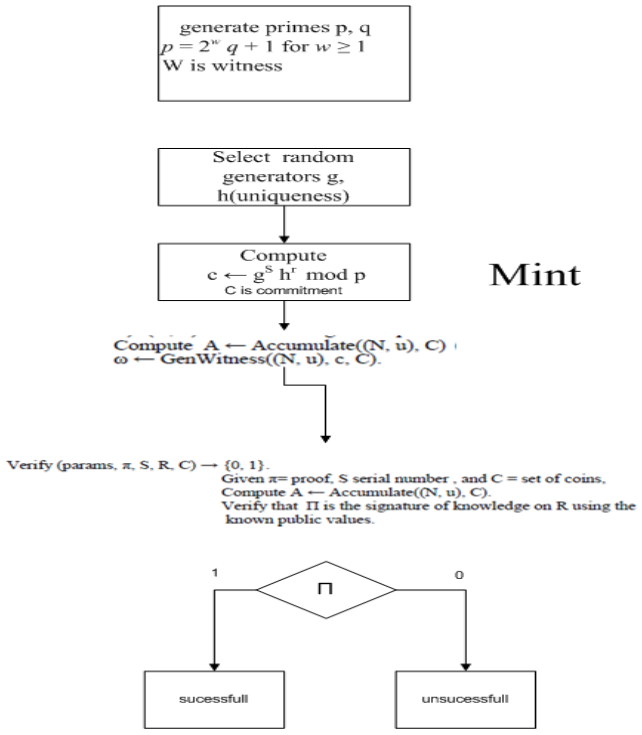

Figure 6 Working Of Zerocoin

4.2 Proposed work

Homomorphic crypto systems[4] have the property that given only the ciphertexts of two numbers, the ciphertext of the sum of those two numbers can be computed.

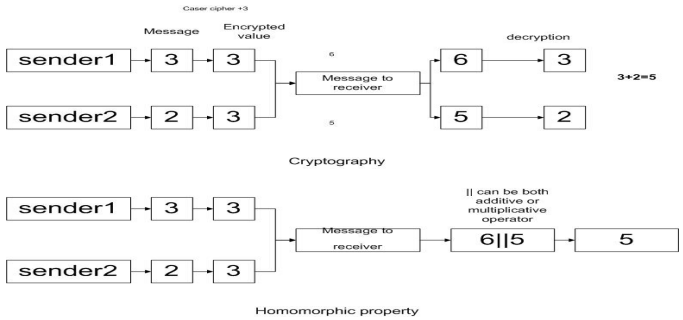

Figure 6 Idea of proposed scheme

Here both the normal cryptographic addition and the homomorphic addition[4] is compared in the figure 6. We are going to used this work in the any system where we can get rewards for the purchase and that reward will be added back to the website in the homomorphic way. Figure7 shows the working flow of the proposed scheme. figure 8 shows the values with the mathematical proof

Algorithm

1. User gets purchase Article AR
2. Reward per article R(AR)
3. When R(AR)>25
4. If(redeem in coin on purchase)
   select any two prime numbers say p and q
   Say N = p * q. where p and q being confidential and N is public.
   Decrypted algorithm Dg is M=b× (ax)-1 (mod p).
   Calculate y = gx mod p. use this y for the encryption
5. else
   Reward = reward + current reward

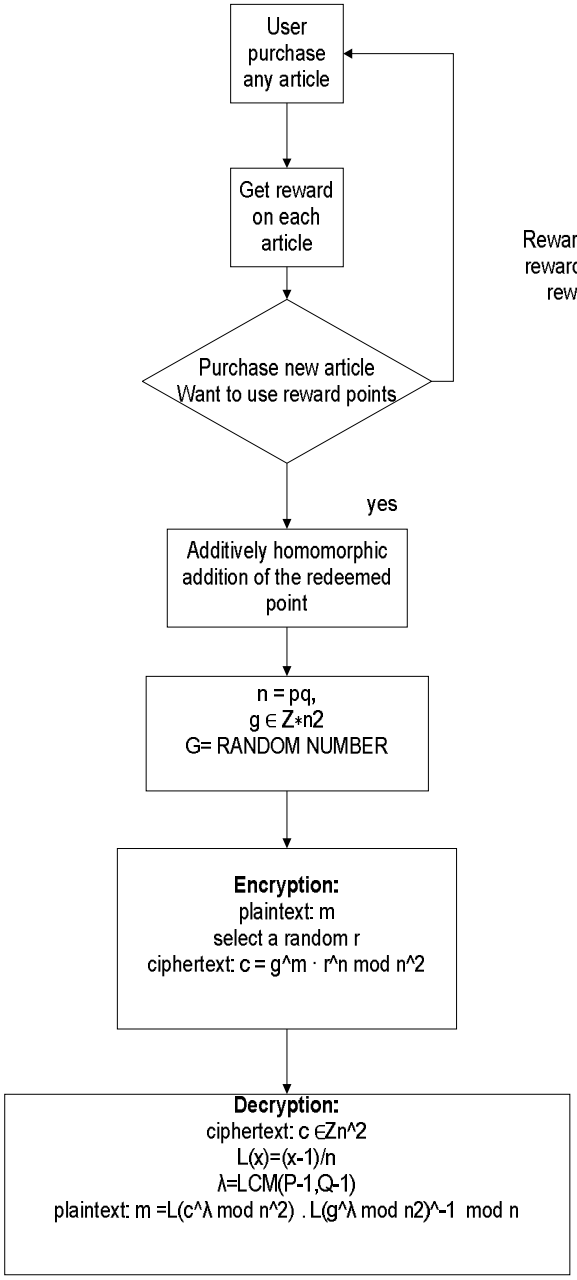

Figure 7 Working of proposed scheme

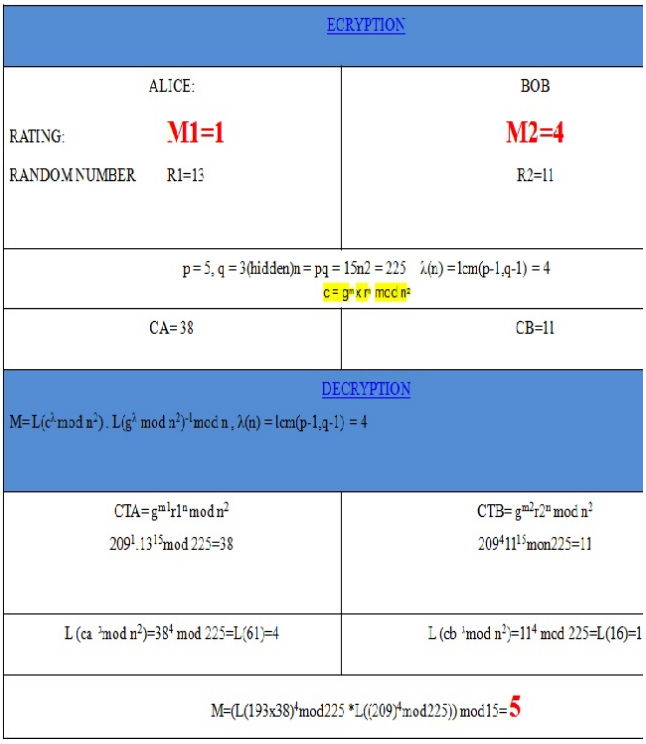

Figure 7 Mathematical proof of proposed scheme

V. EXPERIMENTAL EVALUATION

The dataset[5] holds “38,100 Having id ie anonynimity The dataset consists of 2 files.”

Figure 8 shows the comparison of both the approaches in terms of storage space

Ratings data ratings_data.txt.bz2 (2.5 Megabytes): it contains the ratings given by users to items[3][6].

Every line has the following format:

user_id	item_id	redeem value[6]
1	1000	4

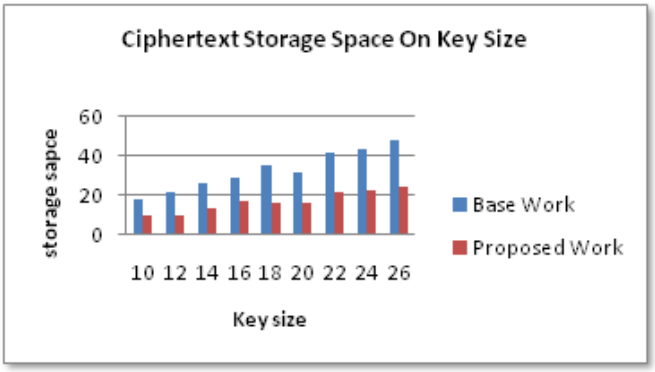

Figure8 comparison of zerocoin and homomorphic addition

VI. CONCLUSION

We conclude that proposed modification it better as

1. Proposed method provides security to the reward points.
2. Proposed method provides more security as it impose the genuine user to the system.
3. Proposed method can be used to construct a threshold cryptosystem
4. Takes less Storage

REFERENCES

[1] Newsome, James, et al. "The sybil attack in sensor networks: analysis & defenses." Proceedings of the 3rd international symposium on Information processing in sensor networks. ACM, 2004.

[2] Levien, R. "from Advogato Website." Advogato Trust Metric, URL: http://www. advogato. org/trust-metric. html.

[3] Tran, Dinh Nguyen, et al. "Sybil-Resilient Online Content Voting." NSDI. Vol. 9. No. 1.

[4] Thadani, Ankita, and Vinit Gupta. "Enhancing Privacy Preservation of Stature System Through Homomorphic System." Emerging Research in Computing, Information, Communication and Applications. Springer India, 2015. 439-449.

[5] Xue, Jilong, et al. "Votetrust: Leveraging friend invitation graph to defend against social network sybils." INFOCOM, 2013 Proceedings IEEE. IEEE, 2013.

[6] http://www.trustlet.org/wiki/Downloaded_Epinions_dataset

[7] Quercia, Daniele, and Stephen Hailes. "Sybil attacks against mobile users: friends and foes to the rescue." INFOCOM, 2010 Proceedings IEEE. IEEE, 2010.