An advanced Decentralized Conditional Anonymous Payment System for Cryptocurrency using Blockchain

Kontham vinay kumar reddy
Department of Computer Science and Engineering
Lovely Professional University,
Punjab
konthamvinaykumarreddy76@gmail.com

Chavi Kapoor
Department of Computer Science and Engineering
Lovely Professional University,
Punjab
Ch.kapoor01@gmail.com

Veeravalli Shivadeepak
Department of Computer Science and Engineering
Lovely Professional University,
Punjab
Shivadeepak7@gmail.com

Mula Sai Charan
Department of Computer Science and Engineering
Lovely Professional University,
Punjab
mulasaicharan99@gmail.com

Gorentla sai yeshwanth
Department of Computer Science and Engineering
Lovely Professional University,
Punjab
yeshwanth.11702886@gmail.com

Rama Vishnuvardhan
Department of Computer Science and Engineering
Lovely Professional University,
Punjab
vishnuvardhanrama@gmail.com

Abstract— **Blockchain, a circulated record innovation, can possibly be conveyed in a wide scope of utilizations. Among these applications, decentralized payment frameworks (for example Bitcoin) have been perhaps the most developed blockchain applications with inescapable appropriation. While the early plans (for example Bitcoin) are regularly the cash of decision by cybercriminals, they just give pseudo-secrecy, as in anybody can de-anonymize Bitcoin exchanges by utilizing data in the blockchain. To reinforce the security insurance of decentralized payment frameworks, various arrangements, for example, Monero and Zerocash have been proposed. Notwithstanding, totally Decentralized Anonymous Payment (DAP) frameworks can be criminally misused, for instance in online coercion and illegal tax avoidance exercises. Perceiving the significance of guideline, we present a novel meaning of Decentralized Conditional Anonymous Payment (DCAP) and portray the comparing security necessities. To develop a solid DCAP framework, we first plan a Condition Anonymous Payment (CAP) conspire (in light of our proposed mark of information), whose security can be exhibited under the characterized formal semantic and security models. To exhibit utility, we contrast the presentation of our proposition and that of Zerocash under similar boundaries and testing climate.**

Keywords— decentralized conditional anonymous payment, blockchain, cryptocurrency, smart contract, anonymity, privacy regulation.

I. INTRODUCTION

Not at all like traditional e-money conspires a decentralized payment framework doesn't depend on believed gatherings such decentralized payment frameworks utilize a disseminated record. In Existing framework there is totally Decentralized Anonymous Payment (DAP) frameworks, which can't be successfully managed. At the end of the day, such frameworks can be abused for crimes, for example, illegal tax avoidance and in cybercrime cases (e.g., payment of payoff for ransomware/online coercion cases). Can be utilized for criminal activities. Anyone can without much of a stretch de-anonymize.

In the proposed work there is an effective Decentralized Contingent Anonymous Payment (DCAP) framework to find some kind of harmony between security assurance and guideline. Our Proposed Framework permits the presence of some confided in substances. We additionally give a solid development of the DCAP framework (upon the planned CAP-Condition Anonymous Payment plot) and examine how the proposition can fulfil security requirements. In this paper, we accomplished both obscurity and guideline properties in our decentralized restrictive anonymous payment (DCAP) system. Our proposed framework is profoundly secure and powerful.

Blockchain is a relatively recent trend, particularly fueled by the success of Bitcoin and its capability to build a trust ecosystem for satisfying economic activities in an environment of asymmetric information and uncertain identities (e.g., due to properties such as decentralization, immutability, verifiability, programmability) [6].

Cryptocurrency (also referred to as decentralized payment system) is, perhaps, the most mature Blockchain application at the time of this research, and other emerging applications include Internet of Things (IOT) and supply chain management. According to Coin Market Cap, 1 for example, there are 2,941 different cryptocurrencies on the market, with a market value of more than $219 billion. [5]

Unlike conventional e-cash schemes such as those described in, a decentralized payment system (e.g., Bitcoin) does not rely on trusted parties (e.g., a central bank). Such decentralized payment systems use a distributed ledger (i.e., blockchain) to record transactions instead. The blockchain is chronologically chained by a hash and largely replicated by mutually-distrustful nodes. To ensure the consistency of the blockchain ledger, transaction data (including addresses of senders and receivers, and transferred value) in early decentralized payment systems (e.g., Bitcoin, Ethereum and Mixcoin) is public. This has corresponding privacy challenges, for example in the privacy of identity and transferred value.

Although these systems have in place measures (e.g., pseudonyms2 or mixing3) to ensure identity privacy, an attacker can analyze transaction records in the blockchain to build the correlation between users' addresses and even obtain the user's real identity. [1]

Hence, security researchers have designed privacy-enhanced solutions at the protocol level, and examples include Monero and Zerocash. Specifically, Monero uses ring signatures to hide the sender's address together with the one-time payment mechanism to hide the relationship between the sender and receiver. One can only learn that some unknown numbers of coins have moved from one of these input public keys without the knowledge of the concrete one(s). In Zerocash, users can place the coins into a "shielded pool" and prove their right of spending these coins via a zero-knowledge method. It means that others can only validate the user's right of spending some specific coins in the pool, without knowing which particular coins. [7]

However, these completely Decentralized Anonymous Payment (DAP) systems cannot be effectively regulated. In other words, such systems can be exploited for criminal activities, such as money laundering and in cybercrime cases (e.g., payment of ransom for ransomware / online extortion cases). Thus, we posit the importance of designing a decentralized payment system that strikes a balance between achieving reasonable privacy protection and allowing regulation to prevent abuse / criminal exploitation. There has also been research along this line. For example, Wu et al. proposed a DAP system that takes into consideration regulation. That is, their proposal not only supports users to anonymously conduct transactions, but they also introduce an audit department to monitor the transaction records. [17]

The adopted blind signatures and key derivation mechanism ensure that their proposal achieves transferability, anonymity, and double-spending resilience. However, the construction in requires considerable interaction (in total about 14 times) during the mining, transferring, withdraw phases. In addition, the proposal also requires 1 blind signatures, 4 digital signatures, and 5 asymmetric encryptions. In other words, the complex and expensive communication and computing costs make it challenging to adopt such a system in practice. [17]

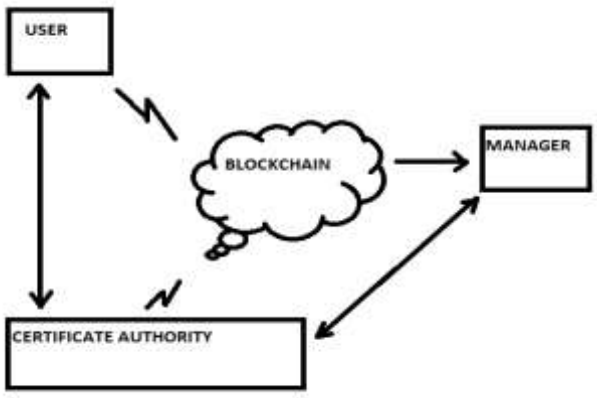

Figure 1. System Architecture of DCAP System.

II. LITERATURE REVIEW

Tomas Sander and Amnon Ta–Shma [1] A framework is auditable on the off chance that it permits to adequately control the cash supply. An electronic money framework that has this property and furthermore has a total report of exchanges permits checking a similar way the financial framework is observed today. We contend that auditable, non-inflexible frameworks protect against a large portion of the major known assaults and maltreatments of mysterious electronic money frameworks. The test is to construct a completely unknown yet auditable and non-unbending framework.

Dr. Gavin Wood Founder [2] Ethereum is an undertaking which endeavors to construct the summed up innovation; innovation on which all exchange based state machine ideas might be assembled. There are numerous objectives of this venture; one key objective is to work with exchanges between consenting people who might somehow have no way to confide in each other. Dealings in this proposed framework would have a few ascribes not regularly found in reality.

Joseph Bonneau, Arvind Narayanan [3] Bitcoin offers just feeble anonymity by and by. This has prompted the ascent of blending administrations which guarantee to take a client's coins and arbitrarily trade them for other clients' coins to muddle their possession, however these accompany no security from burglary by the assistance. Objective is to empower solid anonymity in a straightforward plan that can be sent right away. Methodology is to expand on the current marvel of blends, however to add a free cryptographic responsibility layer.

Dorit Ron and Adi Shamir [4] On May 13th 2012 we downloaded the full freely available report of this framework in one of its two significant forms1, which comprised of around 180,000 HTML records. Subsequent to parsing and handling these records, we fabricated a chart of all the Bitcoin delivers and exchanges up to that date. An enormous equilibrium is either moved inside a couple of hours through many brief middle of the road records, or split into numerous limited quantities which are shipped off various records just to be recombined quickly a while later into basically a similar sum in another record.

Yukun Liu and Aleh Tsyvinski [5] The blockchain is increasing its attention day-by-day which may bring many benefits to the sectors. The information generally in the blockchain is public and cannot be modified. There are a lot of benefits but the risk factor takes all of its benefits. In fact, other than bitcoin there are other 1300cryptocurrencies that have been created under the blockchain. For the first time the policy is to have the identity card and the house verification by which you save a lot of time.

Valentina Gatteschi, Fabrizio Lamberti [6] Bitcoin is an open source for all which is not connected with any of the banks and payment companies and is trusted without any intermediates from one person to other. Now the bitcoin being one of the most expensive coin by holding the 50000dollar price range. Initially bitcoin have the agency problems from the centralized banking models to make the international transfer from one peer-other-peer.

Adam Mackenzie, the Monero Research Lab [7] This includes the method of hiding the transaction amounts in the strong DAC. Recall that in Bitcoin every group action is signed by the owner of the coins being sent and these signatures verify that the owner is allowed to send the coins. This can be entirely analogous to the signing of a check from your bank. In the conclusion the ring confidential transactions protocol gives a strong decentralized cryptocurrency with the most provable security estimates for the hiding amounts, the start ends and the destination end.

David Chaum [8] Computerization of the manner in which we pay for products and ventures is now in progress, as can be seen by the assortment and development of electronic financial administrations accessible to shoppers. A definitive design of the new electronic instalment's framework may generously affect individual protection just as on the nature and degree of criminal utilization of instalments.

Sourav Sen Gupta [9] Blockchain is an appropriated information base with highlights of decentralized, discernible, dependable highlights. It coordinates P2P (Peer-to-Peer) convention, advanced encryption innovation, agreement instrument, shrewd agreement and different innovations together.

Fergal Reid and Martin Harrigan [10] Bitcoin is a peer-to-peer electronic currency system, a shared electronic money framework, is a confused issue. Inside the framework, clients are explained by open keys as it were. An assailant wishing to remove anomality of its clients will endeavour to develop the one-to-many planning among clients and public-keys and partner data outer to the framework with the clients.

Satoshi Nakamoto [11] Business on the Internet has come to depend solely on monetary foundations filling in as confided in outsiders to handle electronic installments The expense of intervention builds exchange costs, restricting the base functional exchange size and removing the opportunities for little easygoing exchanges, and there is a more extensive expense in the deficiency of capacity to make nonreversible installments for no reversible administrations

Yuxiao Wang1, and Juntao Gao [12] In Bitcoin System in Bitcoin monetary framework, a client's security should be ensured through Anonymity. . In the plan, clients' characters are encoded by utilizing Access strategy and are contained in their exchange. At the point when an exchange is questioned to include Illegal exercises, the approved guideline hubs are fit for uncovering the clients' genuine personalities and add the illicit characters to a public boycott.

Satoshi Nakamoto [13] In this proposed work they had projected a system for an electronic dealing while not hoping on the trust. And they commenced with the standard framework of coins made up of digital signatures, that provides sturdy management of the possession, however it is incomplete while not the simplest way to forestall double-spending. The network is strong in its unstructured simplicity. Any required rules and incentives will be enforced with this accord mechanism.

Blockchain Standards Committee [14] This standard characterizes the overall cycle of digital currency installment among customers and shippers. This cycle will be going to depicts how a buyer buys products or administrations with digital currency and how the shipper will get the fiat cash consequently. It includes different parts of, for example, digital currency installment administrators play a specialist job, shoppers claiming the cryptographic money, dealer getting to a cryptographic money installment stage, banks.

Matthew Green and Ian Miers [15] In this work it told the best way to develop unknown installment channels between two commonly suspicious gatherings in these papers they present procedures for building mysterious installment channels. In particular, it presents three channel recommendations, including a procedure that permits installments by means of an untrusted go-between. At long last, every one of their proposition will be started up proficiently utilizing very much considered procedures.

Mihkel Pajunen [16] The exertion put during this paper comprises of a quantitative report looking to manage the subject of client anonymity inside the Bitcoin network by utilizing a web review on one among the chief recognized Bitcoin discussions. The overview looks to make partner degree comprehension of client perspectives towards the side of anonymity by the technique for moving toward the investigating normal inclinations among the agents

III. MODULES

A. Certificate Authority (CA):

This entity is a trusted third party who is responsible for managing the certificates of Users' or Managers' public keys. Concretely, the CA first issues these certificates by embedding them into the transactions. Then, it builds the relationships between the issued certificates of public keys. This can help others to conveniently retrieve the relevant certificates from the blockchain, and the CA to efficiently update the certificates of all the participants.

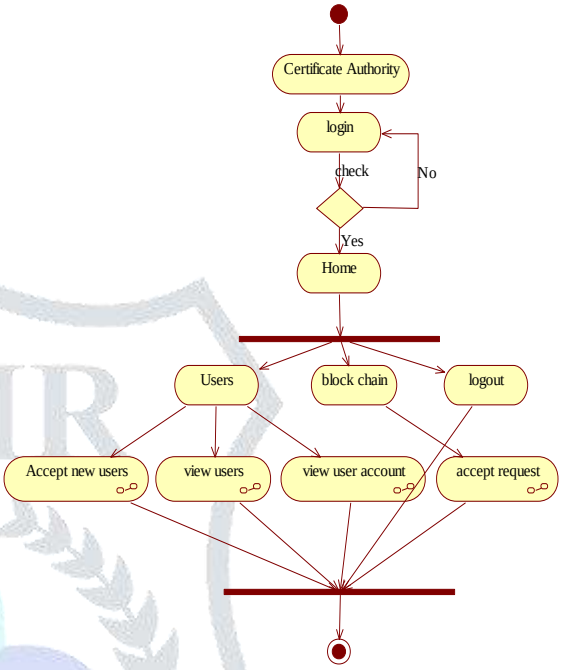

Figure 2. Working Model of Cetificate Authority in DCAP System.

B. User:

These entities are the main participants of a payment system. Who own their respective accounts (each account comprises an address and a private key)? The address is the User's identification and the private key is used to transfer amount from one address to another address.

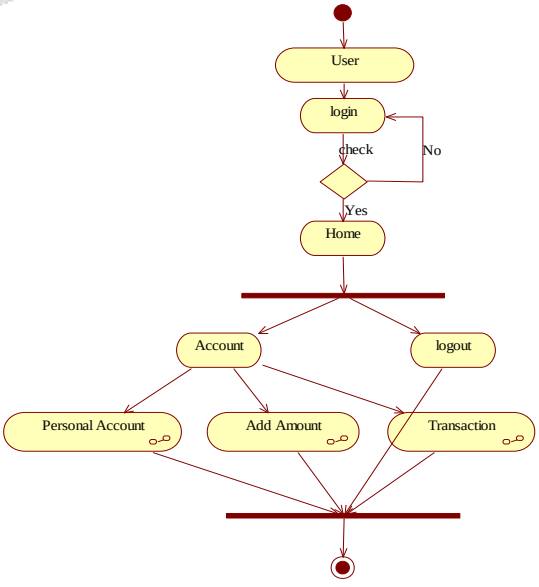

Figure 3. Working Model of User in DCAP System

C. Manager:

These entities are all trusted third parties, who are responsible for tracing the real identity of a suspicious transaction. Note that the Manager is the only entity who owns this authority to invert an anonymous address to the original long-term one. In addition, these entities maintain a common blockchain and own the right to allow or restrict another user to join the system. They can also publicly reveal the malicious users thus, resulting in a blacklist (i.e., these malicious users can no longer successfully issue transactions).

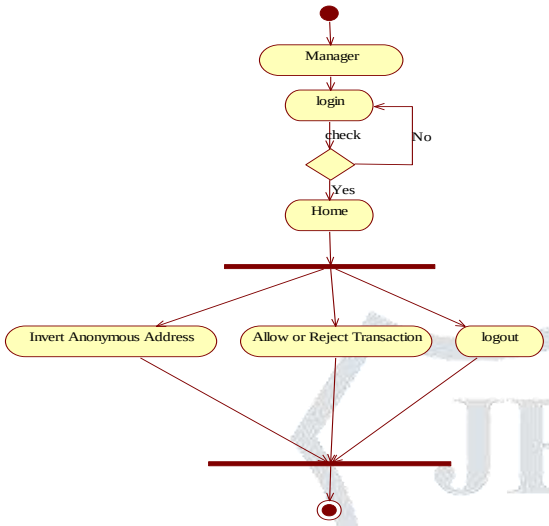

Figure 4. Working Model of Manger in DCAP System

D. Blockchain Network (BN):

This entity refers to the Blockchain Network, which provides an immutable, undeniable and verifiable data storage. The data structure is with a chain-based storage (i.e., the blockchain) comprising so-called transactions. In our proposal, it is realized as a permissioned blockchain, which is maintained by some permissioned nodes (i.e., Managers in our system). The public certificates are embedded into the transactions for the subsequent retrieval.

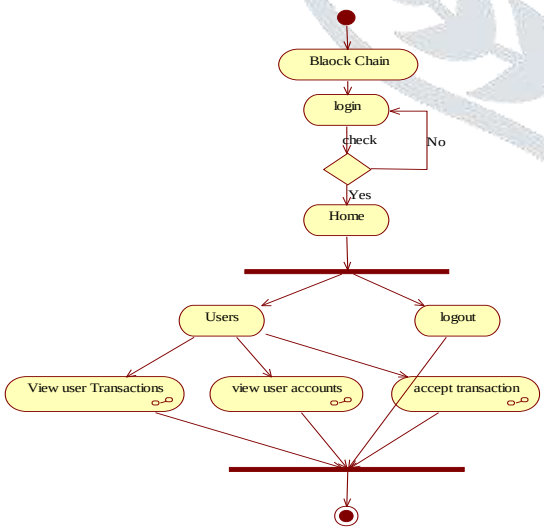

Figure 5. Working Model of Blockchain Network in DCAP System.

IV. DCAP SYSTEM:

The proposed DCAP system design consists of five phases namely:

A. System Initialization:

This phase mainly initializes Blockchain Initialization and Contract Deployment.

B. Register:

This phase involves registering two types of entity (i.e., User and Manager).

C. Transaction Issuance:

Assuming that user1 wishes to transfer amount to user 2; thus, user2 needs to provide its anonymous address to user1. Hence, user2 first invokes Update to generate anonymous account.

D. Chain Transaction:

This phase is executed by the managers to chain the pending transactions into the blockchain.

E. Permission Update:

In this phase, the managers can trace the user's real identity (i.e., long-term address) of a suspicious transaction and revoke the authority of these identities.

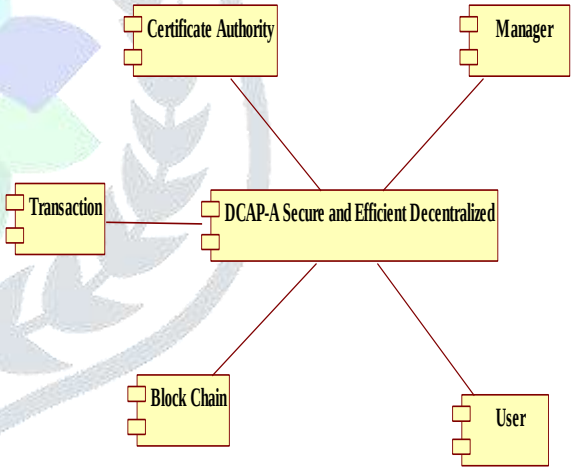

Figure 6. Component diagram of DCAP System.

V. RESULT ANALYSIS

This proposed work is done using HTML, CSS, JavaScript and Java and it is displayed using the web applications JDBD, Servlets, JSP. This can be easily worked by the processor Intel i3 or above with the hard-disk of 500GB or more. The minimum RAM required is 4GB or above.

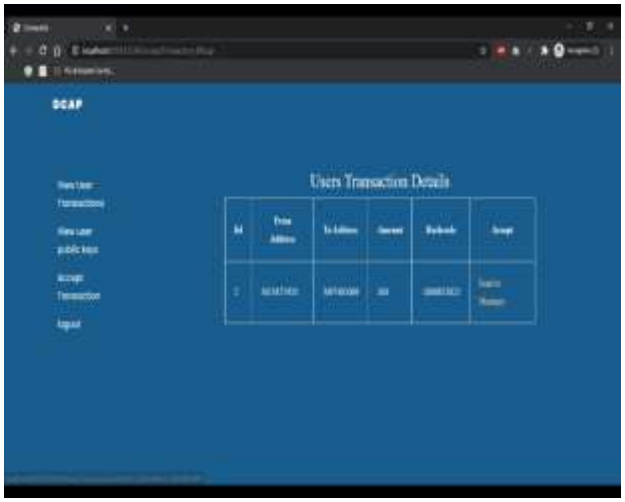

Figure 7. User Transaction details displayed in Blockchain module.

Firstly, the user will have account number of other users to make transaction. So, here in this image when the user1 initiates the transaction using the user2 account number our system will verify it with an OTP which will be sent to the user mail and then the user1 will verify the mail to make the transaction, then the transaction will be completed. Then our system will send the user transaction details to the blockchain system for verification. Then blockchain system will verify the transaction using the hash code given to it. Each and every transaction will have a unique hash code for future verification. Then our blockchain system will send this transaction details to manager for further verification. Here the role of blockchain will be finished. [FIG7]

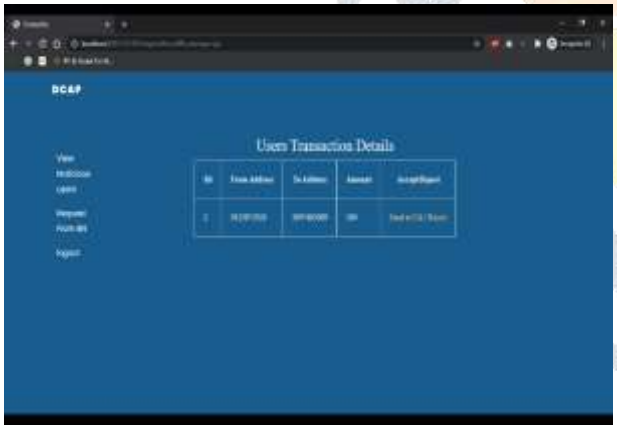

Figure 8. Verification phase in the Manager module.

So, here in this phase when the blockchain sends the transaction details to the manager for verification, the manager firstly verifies the user whether the user is a genuine user or not by viewing the malicious user's option. Here in this option the manager will confirm whether the user is genuine or not. Later when the manager confirms it, the manager will decide whether to send the transaction details to Certificate Authority [CA] or just reject the transaction. If the user is genuine the manager will send the transaction to the CA or if the manager has found any malicious users then the manager will reject the user. So here the user is genuine so the manager will send it to the CA for the completion of the transaction.[FIG 8]

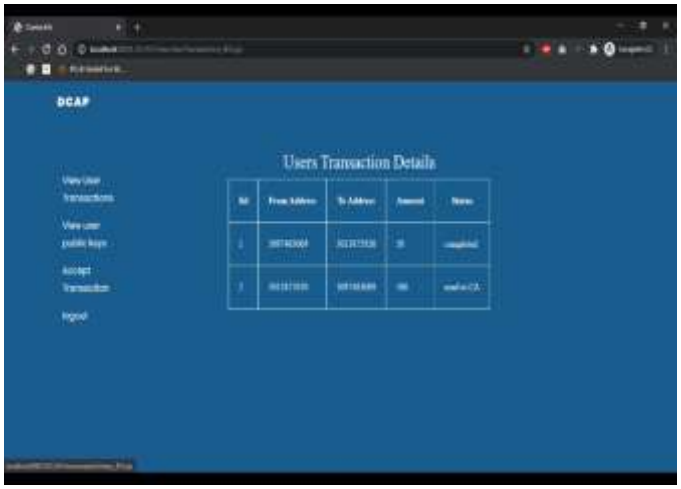

Figure 9. Status of the user Transaction in Blockchain module.

Here in this phase, the blockchain can see the user transaction status, when the manager has sent the transaction for the completion to CA, here in blockchain system we can see the status of the transaction. It is showing that it is send to CA means now the transaction is with CA and he will accept the transaction to complete it.[FIG 9]

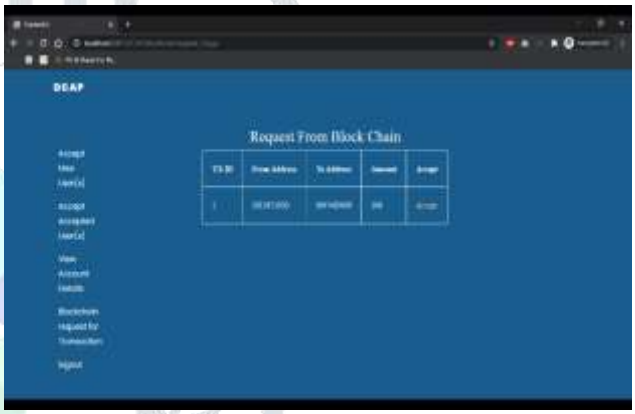

Figure 10. Request from Blockchain to Certificate Authority for completion of transaction.

Here in this image the Certificate Authority will get the request from the blockchain for completing the transaction. Now the CA will accept the transaction as it is fully verified by our manager. After accepting the transaction money will be deducted from user1 and money will be credited to the user2. By this we can assure that the transaction is completed successfully. So here the transaction was too transparent and genuine because there were no malicious users as all the users were genuinely registered and verified users.[FIG 10]

VI. CONCLUSION & FUTURE ENHANCEMENT

The proposed work has achieved both anonymity and regulation properties in our decentralized conditional anonymous payment (DCAP) system. Before constructing our DCAP, we defined a conditional anonymous payment (CAP) scheme with the formal semantic and security models. Also, it will provided a concrete design of CAP based on our proposed signature of knowledge scheme, and proved it secure in the defined security model. Building on the proposed CAP, we constructed our DCAP and demonstrated how it can satisfy the related security requirements. Then, it will be evaluate the performance of our prototype by comparing it with that of Zero cash under the same parameters and testing environment. Findings suggested that our proposal is practical for real-world deployment. A follow-on work is to collaborate with a real-world organization to customize our proposal and implement it in a real-world setting. This will also allow us to identify

additional features or properties that need to be included in future version.

VII. References

[1] Sander, T., & Ta-Shma, A. (1999). Auditable, anonymous electronic cash. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 1666(June), 555–572. https://doi.org/10.1007/3-540-48405-1_35

[2] Wood, G. (2014). Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 1–32.

[3] Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J. A., & Felten, E. W. (2014). Mixcoin: Anonymity for Bitcoin with Accountable Mixes BT - Financial Cryptography and Data Security. International Conference on Financial Cryptography and Data Security, 486–504. Retrieved from https://link.springer.com/chapter/10.1007/978-3-662-45472-5_31#enumeration

[4] Ron, D., & Shamir, A. (2013). Quantitative analysis of the full Bitcoin transaction graph. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7859 LNCS, 6–24. https://doi.org/10.1007/978-3-642-39884-1_2

[5] Liu, Y., & Tsyvinski, A. (2020). Risks and Returns of Cryptocurrency. The Review of Financial Studies. https://doi.org/10.1093/rfs/hhaa113

[6] Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough? Future Internet, 10(2), 8–13. https://doi.org/10.3390/fi10020020.

[7] Noether, S., Mackenzie, A., & Research Lab, T. M. (2016). Ring Confidential Transactions. Ledger, 1, 1–18. https://doi.org/10.5195/ledger.2016.34

[8] Reid, F., & Harrigan, M. (2011). An analysis of anonymity in the Bitcoin system. Proceedings - 2011 IEEE International Conference on Privacy, Security, Risk and Trust and IEEE International Conference on Social Computing, PASSAT/SocialCom 2011, (July), 1318–1326. https://doi.org/10.1109/PASSAT/SocialCom.2011.79

[9] Fan, C. I. (2006). Ownership-attached unblinding of blind signatures for untraceable electronic cash. Information Sciences. https://doi.org/10.1016/j.ins.2004.10.010

[10] Gupta, S. Sen. (2017). Blockchain - The foundation behind Bitcoin. Indian Statistical Institute, Kolkata.

[11] Altshuler, Y., Elovici, Y., Cremers, A. B., Aharony, N., & Pentland, A. (2013). Security and privacy in social networks. Security and Privacy in Social Networks, 1–253. https://doi.org/10.1007/978-1-4614-4139-7

[12] Monti, M., & Rasmussen, S. (2017). RAIN: A Bio-Inspired Communication and Data Storage Infrastructure. Artificial Life, 23(4), 552–557. https://doi.org/10.1162/ARTL_a_00247

[13] Wang, Y., & Gao, J. (2018). A Regulation Scheme Based on the Ciphertext-Policy Hierarchical Attribute-Based Encryption in Bitcoin System. IEEE Access, 6(c), 16267–16278. https://doi.org/10.1109/ACCESS.2018.2814620

[14] Standards, B., & Electronics, C. (2020). IEEE Standard for General Process.

[15] Green, M., & Miers, I. (2017). Bolt: Anonymous payment channels for decentralized currencies. Proceedings of the ACM Conference on Computer and Communications Security, 473–489. https://doi.org/10.1145/3133956.3134093

[16] Pajunen, M. (2017). A n Evaluation of U ser A ttitudes Tow ards A nonym ity in B itcoin. Retrieved from http://his.diva-portal.org/smash/get/diva2:1141672/FULLTEXT01.pdf

[17] Lin, C., He, D., Huang, X., Khan, M. K., & Choo, K. K. R. (2020). DCAP: A Secure and Efficient Decentralized Conditional Anonymous Payment System Based on Blockchain. IEEE Transactions on Information Forensics and Security, 15, 2440–2452. https://doi.org/10.1109/TIFS.2020.2969565