Blockchain based Remittances and Mining using CUDA

Bhumika Ekbote, Vaishnavi Hire, Pratik Mahajan and Jignesh Sisodia

***Abstract*— A large number of people earn money in foreign countries and many of them have to send across the money back home in India. For every such transaction, multiple fees could be charged, varying from 3 to 12 percent. In this paper we offer a peer-to-peer settlement solution for such remittance on blockchain at negligible rates. Money transfers can be securely converted into crypto-currencies, which can easily be transferred across nations, and then again converted into local currencies. In this paper, we use Multi-chain for digital assets and peer-to-peer electronic cash systems where transactions take place between users directly, without an intermediary. These transactions are verified by network nodes and recorded in a public distributed ledger called the blockchain. Each block is verified and added to the blockchain (distributed public ledger), which includes all past transactions through a process known as Mining. Mining using CPU is unwise and has high cost of operation. We present an alternative approach using CUDA-enabled Graphics Processing Unit(GPU) for mining. The massively parallel nature of some GPUs majorly increases the mining power.**

***Index Terms*— Bitcoin, Blockchain, Blockchain Mining, CUDA, GPU acceleration for mining**

I. INTRODUCTION

Cross-border transactions relies almost exclusively on financial institutions and banks which serve as middleman. Bank 'A' at a place 'a' accepts money from customer 'C' and makes arrangement for payment of the same amount of money to either the customer 'C' or his "order" i.e. a person or entity, designated by 'C' as the recipient, through either a Branch of Bank 'A' or any other entity at place 'b'. In return for having rendered this service, the Banks charge a pre-decided sum known as exchange or commission or service charge. This sum can differ from bank to bank. This also differs depending upon the mode of transfer and the time available for effecting the transfer of money. Faster the mode of transfer, higher the charges.[1]

This financial system works well for almost all transactions but it still suffers from weakness of the trust based model. We cannot completely carry out non-reversible transactions, since financial institutions cannot avoid mediating disputes. The transaction cost increases because of cost of mediation, thus limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non- reversible services.These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party [2].

In this paper we use blockchain to propose a solution to reduce high cost of remittances.We have created a electronic payment system,SwiftPay, based on distributed consensus which will help us to transact directly without any middlemen. None the transactions in blockchain can be computationally reversed which protects the users from any fraud. The system is secure as we use a private blockchain to maintain all the records and the nodes which are controlling the blockchain are approved by the owner of blockchain.

The system is a web application which is built upon a private blockchain . It uses cryptocurrency to transfer actual currency across the borders.The use of blockchain gives security, speed and efficiency to the system.Blockchain is a distributed ledger which is a collection of immutable blocks. These blocks consist of all the transactions which happen in blockchain and are confirmed using a process called mining. Mining ensures that all transactions are authentic. As mining is a processor intensive course, it may result in delayed execution.. The system is made efficient by using GPU for mining process.

II. RELATED WORK

A. Blockchain

Blockchain is a global decentralized ledger which stores full history of all the transactions[2]. This blockchain is then verified and stored by every node in the network. Without any consensus being determined by central authority, every node in the network has the same version of blockchain . This is ensured by the blockchain protocol. Another key feature of blockchain is that any node can join or leave the network at any time, without disrupting the functioning of blockchain. New transactions can be created by any node and are propagated across the network in a peer-to-peer fashion. Any node can take a set of these pending transactions and create i.e. mine a new block containing them together with a link to the previous block. This new block is propagated across the network and transaction is confirmed. We can use blockchain to store any type of digital data.

B. Multi-chain

Multi-chain is the platform for creation and deployment of private blockchains. Private blockchains provide security and control over transactions. In Multichain , cryptocurrencies manage identity and security using public key cryptography[3].

Multichain solves the bitcoin blockchain problems , by giving privacy options and permission control to the users. In multichain, users generate random private key which

978-1-5386-0569-1$31.00

is mathematically related to a public address which is an identity to receive funds. Once funds are sent to that address, they can be only spent using the private key. Multichain node uses handshaking method to prove it owns a private key for its given public address.A node checks the public address of the receiving node in its permitted list. It sends the challenge message to the other node. The other node sends the signature of the challenge message referring that it has the private key of the given public address and hence completing the handshake.

C. Multichain Mining

In a private blockchain, addresses can be kept anonymous. Thus exchanges can be done without either party knowing identity of the counterparty. By restricting mining to a set of identifiable entities, MultiChain avoids the monopolizing of the mining process of the private blockchain.

Multi-Chain defines a parameter known as mining diversity which can vary from 0 to 1. Following scheme is used to validate a block:

- Permitted number of miners are identified.
- Multiply mining diversity with number of miners and round it off to get spacing.
- If the miner of this block mined one of the previous (spacing - 1) blocks, the block is invalid.
- This results in a round-robin schedule,where blocks are created in rotation by permitted miners.

The mining diversity parameter defines the strictness of this scheme.In general,higher values are safer, but a value too close to 1 can cause the blockchain to freeze up if some miners become inactive.Therefore a value of 0.75 as a reasonable compromise. Multichain mining is thus restricted to certain entities.

In comparison to centralized database, multichain gives additional functionalities such as participant has full control over his assets through private key. Additionally, control in multi-chain is distributed across many entities, so that no individual or small group can unilaterally decide which transactions are valid or will be confirmed.

III. Shortcomings of Public Blockchain

The shortcomings to a public blockchain can be divided into two broad categories.

A. Scability

- Limited Capacity: A public blockchain has a limited capacity which is to be shared between all network users and is insufficient for financial applications. For example, a Bitcoin blockchain currently supports around 300,000 transactions per day[4] as compared to Visa which currently handles 150 million transactions in a day in the USA[5].
- Irrelevant Data: when using a public blockchain, all the users need to process and store large amount of information which is not relevant to the institution. Along with this, they have to verify all the new transactions and blocks created[3].

B. Privacy and Security

- Mining Risks: if using a public blockchain, there will be a global race to solve the difficult mathematical problem required to create a new block. It has several risks[3],
  - Unpredictable delay for transaction confirmation.
  - Risk of some miners refusing to confirm
  - The potential for 51% attack, where a group of miners controlling over half of the networks computational power collude to rewrite a significant period of the blockchains recent history[6]
- Lack of Privacy: All transactions are visible to all network nodes. The participants run the risk of their identities being revealed which can be used to track their entire transaction history[3].
- Openness: As anyone with Internet connection is able to connect to the blockchain, it can be used for illegal activities.[3]

IV. Why Private Blockchain ?

We have used a private blockchain to solve the problems of mining, privacy and integrated management of user permissions. A private blockchain enables us to[3]

- Ensure that blockchain activity is only visible to chosen participants.
- To control which transactions are permitted
- For securely mining the blockchain.
- In a Multi-Chain blockchain,there is no transaction fee or block reward.If the cost of mining a block in multi-chain is negligible as the miners need no compensation for providing this service beyond their general stake.Miners can also charge network participants a fixed annual service fee,paid by traditional off blockchain means. This reduces the cost of transactions in the remittance system.

V. System workflow

The system we built , works as a distributed ledger for funds transfer. As the blockchain created is a private blockchain created on multi-chain platform it adheres to its rules.

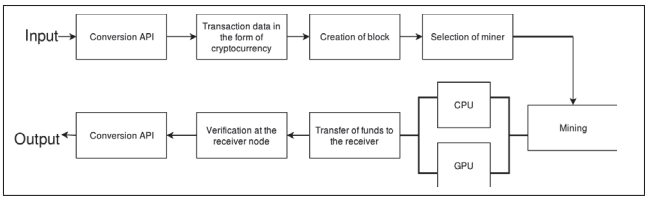

Fig. 1. System Architecture

A. Conversion API

The conversion API is used to convert the input currency into cryptocurrency. The cryptocurrency used for this system is Bolt. 1 Unit of Bolt is calculated using 8 different stable currencies. This ensures that the After the receiver is verified , the conversion API converts the cryptocurrency into desired currency.

B. Creation of Block

Transaction block is created which contains its unique id.Hash is generated which will have the information in the block. The permitted miners are calculated and using mining diversity, a block can be validated. The mining diversity used for this blockchain is 0.5.

C. Selection of miner

Here, the miner is selected using round-robin schedule. If the block validation gives invalid result, next miner will mine the block.

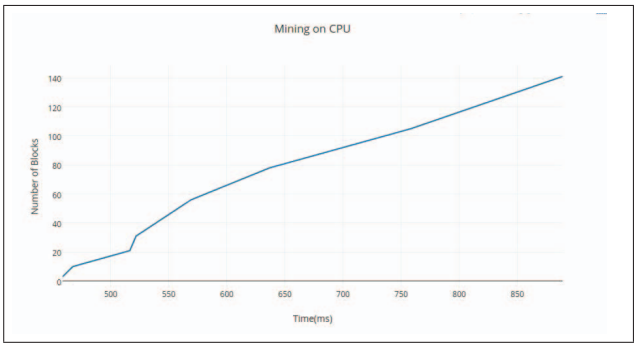

Fig. 2. Mining on CPU

D. Mining

Mining is a processor intensive activity.Therefore, to carry out effective mining, hash generation rates during mining are studied on CPU and GPU.

- Mining on CPU:
  Mining a private multi-chain blockchain on CPU includes following steps:
  - Allocation of resources in the RAM.
  - Generation of hash

  We have used Intel Core2 Duo CPU E7400
- Mining on GPU:
  Mining a private multi-chain blockchain on GPU includes following steps:
  - Allocation of resources on device using Anaconda/ PyCuda.
  - Generation of hash

  We have used NVIDIA GeForce GTX 780

E. Transfer funds to the Receiver

Receiver public address is stored in the block . Accordingly, funds are received by the receiver node.

F. Validation

The receiver node cannot spend the transferred funds unless it validates itself by responding to challenge message.This verifies that the receiver node has the private key for the given public address.Once the node is validated the the transaction is complete.

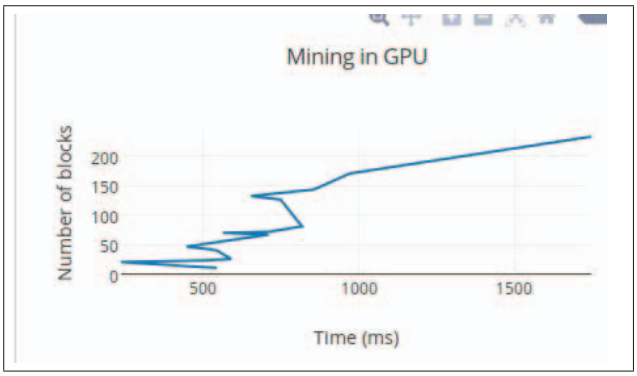

Fig. 3. Mining on GPU

VI. Implementation

For testing our system, two nodes, C1 and C2 were used.The CPU specification of both C1 and C2 was Intel Core2 Duo CPU E7400. C2 had an aditional NVIDIA GeForce GTX780 Graphics card.Both the nodes were connected through a private blockchain created on Multichain platform.Node C2 was given the mining permission. As the nodes increase in blockchain, multiple nodes will have mining permisions.

The wallet addresses of the nodes are linked with the coressponding user email ids. This makes it easier to identify wallet addresses.Every transaction between the nodes is identified by a unique transaction id. Djano framework is used for linking the frontend of the application to the blockchain.

During mining, SHA256 hash generation is carried out.The results were analysed in terms of increase in hash genration rates which affected the time required to mine the blocks.The graphs that were plotted based on these results showed that for limited number of blocks in the system, mining on CPU is efficient. GPU mining is beneficial when the number of blocks to be mined are large in numbers

VII. Conclusions

The system thus created has improved efficiency and takes considerably less time to remit money as compared to traditional systems. We have successfully reduced the time to remit money overseas from few days to few minutes. In traditional systems, when money is to be remitted, it goes through long procedures of back office checks and other regulatory checks. Our system uses Blockchain technology to solve this problem. The back office checks can be replaced by miners which work to validate the transaction. This can be done within minutes, thus improving the overall efficiency of the system as well as reducing the time required to carry out the procedures.

With the removal of back-office checks, we are able to reduce the transaction cost by a large extent. Thus, costs associated with this system is only the cost incurred while mining the blocks to the main blockchain. Thus we can vastly reduce the transaction cost associated We have also improved Blockchain mining efficiency and speed by using GPU (Graphical Processing Unit). This task is done on

the GPU with the help of CUDA. CUDA is a parallel computing platform and application programming interface (API) created by NVIDIA to allow software developers to use CUDA- enabled GPUs for general purpose processing also known as GPGPU (General Purpose Computing on Graphical Processing Units). Due to massive parallel computation, we see drastic increase in mining speed on GPU as compared to CPU.

It was observed that, when the number of blocks in the blockchain are less, i.e. less than threshold value (in this case 800 blocks), the CPU performs better than GPU. As the number of blocks increases, the GPU becomes more efficient. This is due to the fact that GPU has large number of small processing cores whereas CPU has less number of high frequency cores. The individual core performance of these high frequency cores is better than the processing cores in the GPU. Thus, when there are less number of blocks, the utilization of GPU cores is much less. As a result CPU performs better. We can consider this as, for eg. Consider a CPU having 4 cores and a GPU having 2300 cores. A process utilizes 4 cores when processing on CPU and same process utilizes 4 cores on GPU as well. As the individual core performance of CPU is better than that of GPU, the execution of this process will be faster on CPU than on GPU. Take another processing intensive process, in this case it can only utilize 4 cores of CPU, i.e. max number of cores on CPU. But this same process can utilize 2000 cores of GPU. This makes processing of this process on GPU much faster and efficient than on CPU. Similarly, when there are less number of blocks, the GPU cannot be utilized to its full efficiency, resulting in dismal performance on GPU when compared to CPU. But as number of blocks increase, the GPU utilization keeps on getting better. Thus we see that GPU performs better than CPU in mining.

REFERENCES

[1] www.banknetindia.com/banking/remitance.html

[2] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, Online, http://bitcoin.org/bitcoin.pdf

[3] Dr Gideon Greenspan, "MultiChain Private Blockchain White Paper", 2015, Online, http://multichain.com/download/MultiChain-White-Paper.pdf

[4] Analysis of maximum transaction rates: http://hashingit.com/analysis/33-7-transactions-per-second

[5] http://usa.visa.com/merchants/industry-solutions/retail-visa-acceptance.jsp

[6] Apart from the well-known 51% attack, some researchers argue that 33% of the network capacity would be sufficient: http://arxiv.org/abs/1311.0243. Either way, tokenized assets break the fixed relationship between the cost and potential reward of conducting such an attack, since the reward can contain more than just bitcoin.

[7] Jega Anish Dev, Bitcoin mining acceleration and performance quantification, 2014, Intl. Conf. on Advances in Computer Science and Electronics Engineering