Cluster Computing (2021) 24:851–865
https://doi.org/10.1007/s10586-020-03163-6

Blockchain-based e-cheque clearing framework with trust based consensus mechanism

Nikita Singh[1] · Tarun Kumar[2] · Manu Vardhan[1]

Received: 21 January 2019 / Revised: 23 July 2020 / Accepted: 24 July 2020 / Published online: 31 July 2020

Abstract
The cheque based banking transactions are widely used all over the world. The reason is that it is a hustle free and trusted way of money transaction. The existing cheque settlement process involves manual processing of submitted cheques, and large amounts of time for clearance. This paper proposes a framework to automate the cheque settlement process. This framework proposes cheque generation, cheque processing and cheque settlement process through online and physical modes. The proposed framework is based on blockchain technology, where the blockchain network brings all different banks on a common platform i.e. the e-cheque issued from one bank can be submitted to any other bank in any mode of operation either physical or online. The proposed framework comprises a novel trust based consensus mechanism for block mining. The proposed consensus approach outperforms the existing proof-of-work based approach by reducing consensus time by 25%. The proposed framework can partially transform the current banking system over the blockchain. Security threats and vulnerability of the proposed framework is also discussed in this paper.

Keywords e-Cheque · Blockchain · Consensus mechanism · Multithreaded parallel transaction search · Trust management

1 Introduction

The evolution of information technology has brought notable growth and huge transformation in terms of accessibility, ease of doing business in almost all the sectors of different industries. Among these sectors, the banking sector shows major transformation by changing the way transactions are carried out. This sector uses information technology to provide ease of doing transactions. This sector has transformed its operations in centralized and online modes of operations. Real time gross clearance (RTGS), NEFT (National Electronic Funds Transfer) are technologies by which users can avail banking services of the respective banks from anywhere in the world. However, all the services provided by this sector is transformed by using information technology but cheque based transactions are still in its traditional forms. Only transformation in traditional cheque based transactions is the cheque truncation system (CTS). The financial institutions have introduced a CTS due to large volume of transactions for faster cheque clearance. In CTS, a magnetic ink character recognition (MICR) [11] coding is printed on all the cheques which is read by the MICR readers and the system automatically detects the drawer's bank and branch by scanning this MICR code. The cheques are transferred electronically (scanned images of cheques) to the drawer's bank. This process reduces the cheque clearance time. The CTS based cheque clearance process has its own vulnerabilities against forgery and counterfeits of cheques. Gjomemo et al. [8] discusses various ways of forgery in digital cheques such as replacing the duplicate signature of any person, changing the precision in cheque amount by using digital image processing techniques. Rajendra and Pal [18] propose a digital watermarking based approach for detection of any forgery in cheque. Anderson [1] proposes architecture of the e-cheque

✉ Tarun Kumar
ertarun123@gmail.com

Nikita Singh
nikitasinghk@gmail.com

Manu Vardhan
mvardhan.cs@nitrr.ac.in

[1] CSED, NIT Raipur, Raipur, India

[2] CSED, GLBITM, Greater Noida, India

framework. Chang et al. [5] propose an e-cheque system that is based on mutual authentication of drawer and payee. Blockchain based large e-governance applications such as blockchain based property transaction system [22] are gaining attention of researchers.

1.1 Blockchain

A concept of blockchain was first introduced by Satoshi Nakamoto in 2008. Nakamoto [15] proposed a crypto-currency based on blockchain technology. Blockchain is a kind of technology where all the transactions are stored in cryptographically linked blocks. These blocks form a linear connection chain called blockchain. The blockchain is distributed to the p2p network, where each peer stores a copy of complete and common blockchain. Before a transaction is committed to the blockchain, it has to be agreed upon by the active participants of the network in order to guarantee the trustworthiness of the information being incorporated into the blocks. This is where the consensus protocols become important and determines which state of the database is chosen to be valid and true. It is only when consensus is achieved that the new transaction is recorded into the block and is linked to the already existing chain of blocks using a cryptographic hash link to the previous block. The cryptographic link between blocks makes blockchain immutable in nature. Decentralization of blockchain removes the barrier of centralized ownership and limitation of centralized system i.e. single point of failure.

1.2 Contribution of this paper

This paper proposes a blockchain based solution to the cheque clearing system for banking transactions. Presently, some banks provide e-cheque facilities to their customers but the scope of e-cheque is limited to its own banking branches only since e-cheque issued by a bank cannot be deposited in another bank due to security and authentication issues. The proposed approach extends the scope of e-cheque from local to global banking. This paper analyzes the vulnerabilities of e-cheque against double spending and forgery. The analysis reveals that the proposed e-cheque system is not vulnerable to such threats. Hence, this paper proposes a novel solution to the e-cheque system. The proposed system is based on permissioned blockchain and is intentionally designed in such a way that any bank can see the cheque issued by its customer or deposited by any other bank. This enables a bank to validate the deposited e-cheque. Further, the information about any customer's such as personal details, balance information and frequency of transaction remains confidential to the concerned banks only. The proposed system only stores the issued and deposited cheque information into the blockchain. Aggregated balance of any customer is not visible to any other bank or its miners. Further a trust based consensus mechanism is proposed.

1.3 Organization of the paper

A brief literature survey of leading research papers that concerned this proposed approach have been researched in Sect. 2. Section 3 has six subsections that detail the proposed approach. Section 3.1 proposes network architecture for blockchain based e-cheque system. Section 3.2 proposes blockchain based e-cheque generation process. Section 3.3 proposes blockchain based e-cheque payout process followed by 3.4 that proposes consensus mechanism & leader election process along with analysis of results. Section 3.5 proposes multithreaded parallel transaction search algorithm followed by Sect. 3.6 that analyzes security threats & mitigation in the proposed approach.

2 Literature survey of leading related work

The global financial crisis that occurred in 2008 imposed strict and rigid banking norms and regulations worldwide with the view to prevent and deflect a crisis like this to ever happen again. Nguyen [16] attempts to bring into focus the role of blockchain technology in the development of a much more customer-centric and transparent banking system.SWOT analysis or SWOTM matrix, a short form for strength, weakness, opportunities and threats provides a structured planning method for the evaluation of various Blockchain against the SWOT parameters. The authors conduct an in depth analysis on the technologies that constitute the Blockchain, how the amalgamation of the technologies gave birth to Blockchain, analysis of various types of Blockchain and how the Blockchain functions along with its benefits and challenges [17]. Barclays becomes the first industry to adopt blockchain technology for its business [3]. Santander [19] also started to use blockchain technology for real-time trade transactions. InsurChain [10] is first blockchain application for insurance ecosystem. Starbase [23] also started to use crypto-tokens for crowd funding from various sources. Guo and Lang [9] in their paper describe how blockchain technology is the combination of several other existing computer technologies namely, distributed data storage, peer to peer systems, distributed consensus mechanism, and encryption algorithms. Cocco et al. [6] in their paper talk about the sustainable development and potential of blockchain as a banking technology by taking the bitcoin system under consideration. Eyal [7] discusses the role and potential of the blockchain technologies to fulfill the requirements. The

authors conduct an in depth study of the challenges of using Blockchain as a database operating in an Internet of Things environment (IOT). The research paper discusses the technology behind Bitcoin, the Bitcoin Backbone Protocol (BBP) and identifies how blockchain can be used as a database for IOT applications [25]. A decentralized authentication and access control mechanism has been proposed for lightweight IOT devices based on blockchain and fog computing to secure the huge amount of data generated by the IOT devices and provide a secure environment for the IOT systems to operate [12]. Daming et al. [14] carried out vulnerability analysis of blockchain against various intrusions. The study shows that the blockchain technology is more secure and robust to existing intrusion attacks. This proves that blockchain based application are more secure and fault tolerating as compared to client-server based architecture. The blockchain based technology can be adopted to banking system as well. Blockchain application are secured because its underlying consensus mechanism.

The consensus process is responsible for selection of the leader for mining the new block, verifying the transaction in new block and achieving the consensus of other miners on new block before adding the block into blockchain. There exists various consensus mechanism to handle the byzantine failures such as Proof-of-work (PoW) [15], Proof-of-Stake (PoS) [13] etc. The PoW [15] handles the issues of Byzantine Generals Problem by imposing a puzzle to miners. The miners have to solve the puzzle in order to get the opportunity for elected as leader and mine the block. The new block is added to blockchain when majority i.e. 51% votes of miners are garnered. In PoS, the highest stake holder miner always get chance to mine the new block and other miners achieve the consensus on the new block

In any peer-peer systems or distributed systems, trust of nodes also plays an important role in selection of most efficient and secure node selection for various operations. Bano et al. [2] state that the important factor that distinguishes blockchains from traditional distributed databases is the ability to operate in a decentralized setting without relying on a trusted third party. Schwartz et al. [20] are of the opinion that several consensus algorithms exist for the Byzantine Generals Problem, few of which are suitably designed for decentralized and distributed payment systems. Tschorsch and Scheuermann [24] state that pioneering contributions of the virtual currency Bitcoin is achieving the degree of decentralization which was previously thought unachievable. Singh et al. [21] are of the view that each bank has to maintain a huge data center with expensive skilled manpower requirements and these data centers consume large energy, thus contributing to increased carbon emission.

3 Proposed blockchain-based e-cheque system

This research work proposes a novel and comprehensive electronic cheque transactions framework. The e-cheques generated by the system can be deposited to the bank either electronically or physically. The proposed system is based on the blockchain technology; hence all banks willing to implement the proposed system must join the proposed blockchain based framework in order to provide the e-cheque facility to the customers.

3.1 Proposed network architecture for e-cheque system

The network architecture of the proposed system comprises of entities such as different participating banks and their respective web servers that are replicated, miner nodes for each of these replicated web servers, cloud data center and some professional miners that may also be engaged as these miners carry state of the art hardware resources. All the miners are connected together with a common p2p swarm network as shown in Fig. 1 and a common blockchain exists that is used by all these participating banks. Each bank provides an interface for e-cheque generation and e-cheque deposit through online portal. The teller machine fetches information from miner of the bank and cloud data centre. Teller machines shall scan the barcode and read the e-cheque that is being deposited by any customer. All the e-cheques generated and deposited by the customers will be stored in the closed blockchain in the form of transactions.

A bootstrap server maintains the list of authorized miners. To join the p2p swarm network, each miner connects with bootstrap server by sending a request to join the p2p network. On receipt of any request from miner,

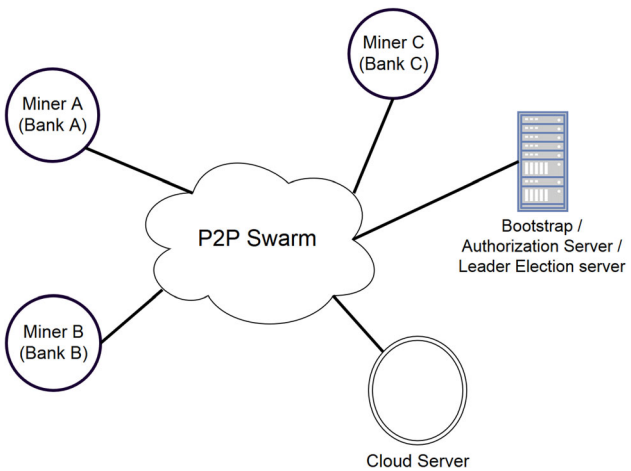

Fig. 1 Network architecture of DLT based e-cheque framework

bootstrap server replies back with the list of active miners as the response of the request. Now the incoming miner is able to connect with the all other active miners. Hence, p2p swarm is formed through the bootstrap server. This bootstrap server is also part of the p2p swarm network and participates in leader election process as discussed in Sect. 3.4. Each bank may have multiple miners as shown in Fig. 2 where mulitple miners of a bank are connected to the all servers of the bank. The miner local to a bank is called internal miner and these miners are connected to bank server via internal private network of that bank. The internal miners are connected to other bank miners via p2p swarm network. Master and secondary server handle banking application along with the role of web server. The next section discusses the process of the e-cheque generation, when any customer has to issue a cheque in favor of some other entity. It is important to note that two major activities of the proposed system for storing e-cheque transactions in blockchain are verification of:

i. e-cheque issued &
ii. e-cheque clearance.

3.2 Proposed blockchain-based e-cheque issue

In the proposed system, for e-cheque issue, the drawer generates e-cheque from online banking portal of the bank. In the proposed system, each customer is issued with a pair of public and private keys and to generate the e-cheque, customer needs to digitally sign each transaction using his private key. The public key of all customers of all the banks is known to all miners. The generated e-cheque has unique barcode and its number printed on it. During verification of this newly created e-cheque, the digital signature of the drawers is verified by at least two internal miners. Hence, the server multicasts this transaction to two least loaded miners to verify this transaction. Upon verification of digital signature, the transaction is added to transaction pool and verified e-cheque is generated as discussed in Sect. 3.2.1. The banking portal now allows the drawer to download this e-cheque as valid e-cheque. Set of these verified transactions are stored in a block by an internal miner. Figure 3 illustrates the process at each end of the proposed system along with work flow of e-cheque generation request when any account holder requires a cheque for making any payment. This verified e-cheque is downloaded by drawer and may be sent electronically (mail/sms etc.) to the payee. Payee can download this e-cheque sent by drawer and deposit the same physically into its own banker's teller machine or electronically by payee's banking portal.

3.2.1 Transaction format for e-cheque issue

Before all the verified e-cheques issued by various entities can be cleared, these verified e-cheques should be recorded into the blockchain in form of transaction so as to validate

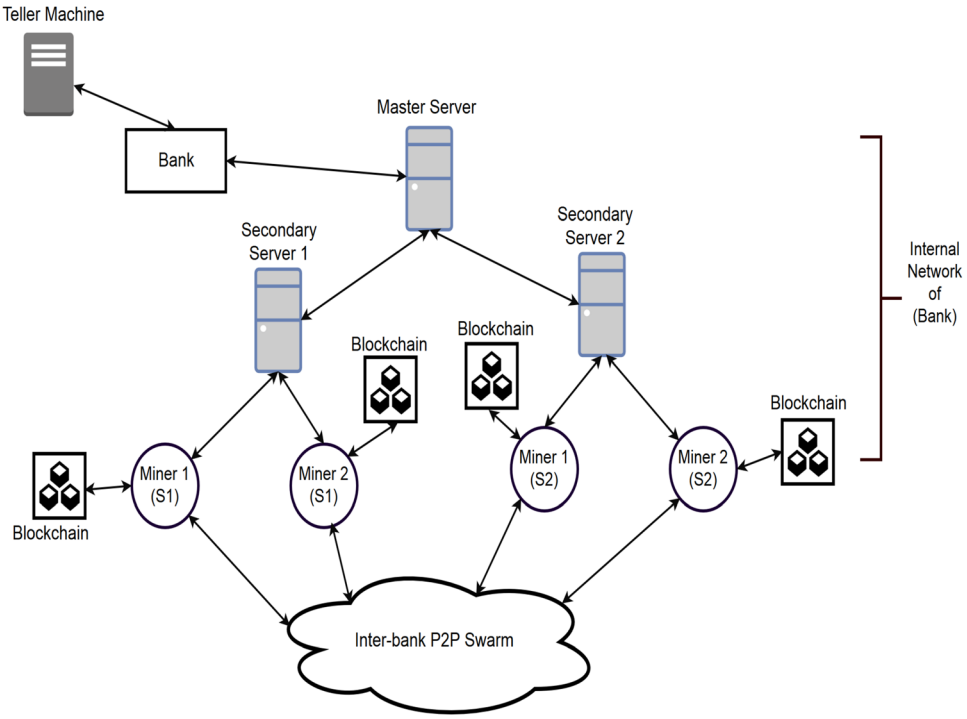

Fig. 2 Intra-bank p2p network and banking server architecture

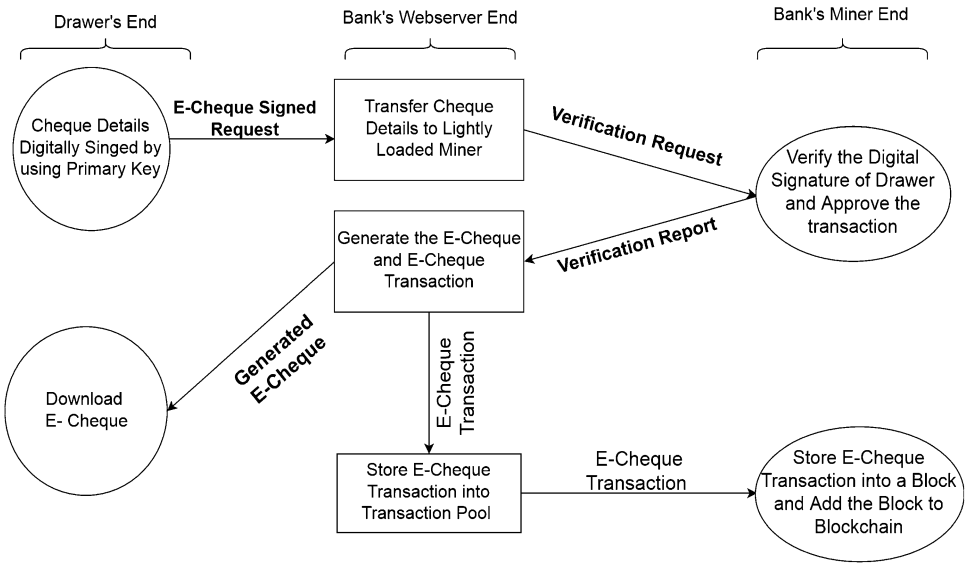

Fig. 3 e-Cheque issue process

whether these e-cheques are eligible for being honored. Eleven different attributes that constitute an e-cheque are:

$Request\_Type$:	type of the transaction, {set to value to "e-cheque issue"}
B:	the unique barcode number assigned to the e-cheque,
D_N:	name of the drawer,
B_N:	name of the drawer's bank,
B_B:	name of the bank branch where the drawer's account exist,
D_A:	drawer's account number,
C_{qn}:	cheque number,
C_{qt}:	is the cheque type i.e. banker's cheque, account payee cheque etc.,
P_N:	name of payee,
A_t:	amount and
C_{qd}:	cheque issue date

These e-cheque attributes are defined by a set EC.

$$EC = \{Request\_Type, B, D_N, B_N, B_B, D_A, C_{qn}, C_{qt}, P_N, A_t, C_{qd}\}$$

To secure the set EC, secure hash of this set is computed before the set EC is digitally signed by the customer. $SHA256$ algorithm is used to compute the hash of this set EC.

$$Hash_{EC} = SHA256(EC)$$

Drawer signs the set EC and hash of this set EC with its private key. Drawer's private and public key are represented by DS_K and DP_K. The digital signature is obtained using $ECDSA$ algorithm as:

$$digital\_signature = ECDSA(DS_K, Hash_{EC}, EC)$$

After obtaining the digital signature, the same is verified by internal miners and a copy of verified e-cheque is generated and provided to the customer. At the server side, hash of the generated e-cheque is also recorded into the transaction. The generated e-cheque is represented by a file 'E' and the hash of this file is computed as:

$$Hash_E = SHA256(E)$$

Now the complete transaction is represent by set T_X as:

$$T_X = \{EC, Hash_{EC}, digital_signature, Hash_E\}$$

This transaction as illustrated in Fig. 4 is stored in the global transaction pool and placed into the block during the mining process.

3.2.2 Block creation for e-cheque issue transactions

In the proposed framework, a block contains only one kind of transaction based on 'Request Type'. This is because during e-cheque generation, only internal miners shall perform verification whereas for payout, all the miners participate in verification of details of e-cheque payout. Hence, the proposed blockchain has two types of blocks i.e. the block that contains transactions with "Request_Type" as "e-cheque issue" and the blocks that contain transactions having "Request_Type" as "e-cheque payout". This is defined in 'block_type' field in each block.

All the attributes listed in Sect. 3.2.1 require about 1400 bytes of storage. Hence this implementation has been done with a block size of 50 KB with each block containing 30 transactions. Selection of the miner for mining the new block is always controlled by the consensus algorithm. Before this block becomes part of blockchain, miners of all

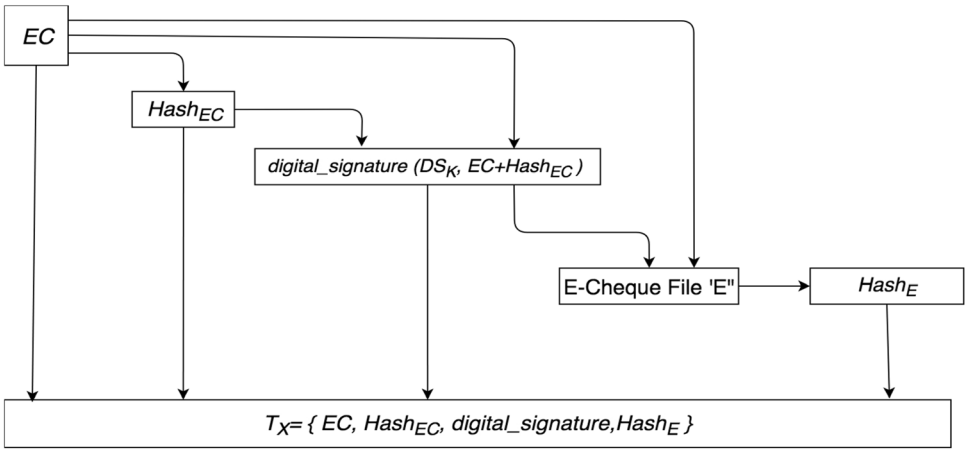

Fig. 4 Generation of transactions for e-cheque deposit request

the participating banks only verify the digital signature of this miner during consensus process.

The block generated by the miner contains following attributes:

- hash of previous block,
- timestamp,
- hash of all the transaction,
- list of the transactions and
- digital signature of the miner.

The hash of previous block is defined by PB_{Hash}, and set of the transaction is defined as T where:

$$T = \{T_{X1}, T_{X2}, T\,\mathrm{X3}, \ldots, T_{Xn}\}$$

Each T_X represent the transaction defined in previous section. Hash of the transaction is computed as:

$$Hash_T = SHA256(T)$$

Value of attribute 'block_type' is set to "e-cheque issue" as all the transactions stored are for issuing an e-cheque. The time instance when a block is created is denoted by TS. Finally the miner has to sign the all the transaction with its private key. Let the private and public key of the miner be represented by MS_K and MP_K. Finally, digital signature is obtained using $ECDSA$ algorithm as:

$$M_{digital\_signature} = ECDSA(MS_K, Hash_T, block\_typeT, TS) \quad (1)$$

The content of the block is represented as set B_L where:

$$B_L = \{PB_{Hash}, TS, Hash_T, block\_type, T, M_{digital\_signature}\}$$

This newly created block is broadcast to all the miners of every bank to achieve consensus only on digital signature of miner which create the block using respective public key. This is necessary to ensure that the block is being generated by authorized miner and block is added to the block in their blockchain if found valid.

3.3 Proposed blockchain-based e-cheque clearance

The payee can deposit the e-cheque electronically through the online banking portal or physically by depositing the print copy of the e-cheque in the teller machine. The server accepts this e-cheque and performs a search operation for corresponding transaction on blockchain for verifying validity and authenticity of it. The e-cheque clearing request is approved by the banking system once the validity and authenticity of the e-cheque is proved; otherwise it is rejected. In physical deposit process, teller machine scans the barcode of the e-cheque and extracts the respective transaction corresponding to this cheque that is stored in the blockchain with block type "e-cheque issue". The clearance request is generated by the teller machine after verification of the e-cheque. Once the e-cheque is cleared by the system, the details of the e-cheques are again stored in blockchain in the form of the transaction in block type "e-cheque payout". Figure 5 shows the process flow of e-cheque deposit request and clearance process. Once the payee's bank server receives e-cheque deposit request during clearing process, the request is forwarded to the miners in the p2p network. These miners search for corresponding transaction in the blockchain and verify its validity and authenticity. The search is based on the proposed Multi-threaded Parallel Transaction Search Algorithm (MPTSA) that reduces the search time considerably. The payee's bank server generates the clearance request to the drawer's bank on valid e-cheques otherwise it rejects the request and notifies the customer accordingly.

3.3.1 Transaction format for e-cheque clearance

To ensure that only valid e-cheque get deposited and used only once, the proposed system generates a transaction for each e-cheque issued. The miners first search the corresponding e-cheque transaction in the blockchain and

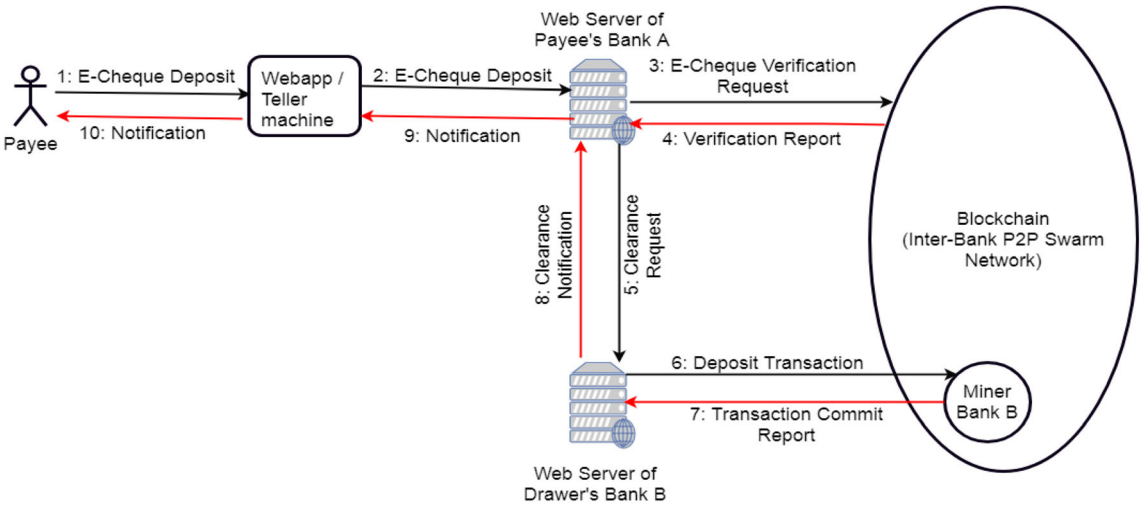

Fig. 5 e-Cheque deposit and clearance process in the proposed system

generate the validity report for the e-cheque based on its attributes. The transaction that matches the requested attributes and has newest timestamp value is picked up for validity check. The requested e-cheque would be valid only when the value of "Request_Type" field of searched transaction is "e-cheque issue" else e-cheque is considered as invaild.

The value of attributes "Request_Type" is set to the "e-cheque payout" as this transaction is prepared for commit operation. The attributes defined for the e-cheque deposit request are:

$Request\_Type$: type of the transaction, {set to value to "e-cheque payout"}
S_{id}: Clearance request identifier,

$B, D_N, B_N, B_B, D_A, C_{qn}, C_{qt}, P_N, A_t, C_{qdt}$ are the attributes that are same as defined in Sect. 3.2.1.

C_{qdd}: cheque deposit date,
P_{BN}: name of the payee's bank,
P_{BB}: name of the payee's bank branch, name

All the above attributes are part of the set P. Therefore, the e-cheque deposit attributes are represented by set EC.

$$EC = \{Request\_Type, S_{id}, B, D_N, B_N, B_B, D_A, C_{qn}, C_{qt}, P_N, A_t, C_{qd}, C_{qdd}, P_{BN}, BB\},$$

To secure EC, secure hash of this set is computed using $SHA256$ before the set EC is digitally signed by the payee's bank server which initiates clearance request.

$$Hash_{EC} = SHA256(EC)$$

Now, payee's bank server signs the set EC and hash of the set EC with its private key. The payee's bank server's private and public key is represented by SS_K and SP_K respectively. The digital signature is obtained using $ECDSA$ algorithm as:

$$digital\_signature = ECDSA(SS_K, Hash_{EC}, EC)$$

Finally, the complete transaction is represented by set T_X as:

$$T_X = \{EC, Hash_{EC}, digital\_signature\}$$

The clearance request is only approved by the drawer's bank server when the generated e-cheque payout transaction request is stored in the blockchain. All the valid e-cheque clearance transactions are added in the block before these become part of block chain. This is elaborated in the next section.

3.3.2 Block creation for e-cheque clearance transactions

To store these transactions into blockchain, leader miner creates a block and adds verified transactions that has "Request_Type" value as "e-cheque payout" and sets the "block_type" field to "e-cheque payout". To add this block in the blockchain, all peers must verify all transactions in the newly created block. Once all the transactions of newly created blocks are verified by each miner, the consensus process is started to obtain the final consensus to add this block into blockchain. A novel approach for consensus mechanism is proposed in the next section.

3.4 Proposed scalable trust based consensus approach

The proposed e-cheque transactions framework comprises of two types of miners; one that are part of the bank and the other being outsourced or private. The nodes that are part of the banking system are termed here as Banking System Miners (BM). The other are Authorized Professional Miners (AM) that have investments in state of the art infrastructure (farms) and offer their services so as to encash their investments in these farms. Based on the number of transactions, we classify BSM into heavily loaded BSM (RHBM) and lightly loaded BSM (RLBM).

3.4.1 Leader election process

To maintain the blockchain consistency, the process of block mining needs to be synchronized. The leader election mechanism holds this responsibility and by synchronizing mining process, consistency in blockchain is maintained. The leader election mechanism elects a leader miner among several miners for mining process for each block. This leader miner mines the new block and broadcasts it to all miners for consensus process. In the proposed system, the bootstrap server maintains the list of all active miners. Hence, allocation of mining slots to miners is handled by bootstrap server.

3.4.2 Proposed trust based consensus algorithm (TCA)

Most of the existing blockchain applications demand 51% of votes in order to add a block to an existing blockchain. This can be very demanding when the application being developed involves real time transaction processing. To overcome these issues, a hybrid efficient consensus mechanism based on the load of the node and its trust value is proposed here. Objective of proposed consensus algorithm is to reduce the overhead of message exchange and time required to achieve the consensus. In the proposed approach, each miner maintains the status table of other miners as shown in Table 1.

Each node will maintain information about each miner as given in Table 1. In this table, the attributes like UF and TF are computed each time before addition of new blocks in the blockchain. The value of trust factor is used in the selection of the consensus agents for the consensus process. This trust factor (TF) is computed based on following these attributes of each node:

Computation capacity factor (CCF): Its value is defined based on the infrastructure of a node. If the node is equipped with state-of-the-art computing resources then its value is set to 1 else its value is set to 0.5.
Utilization factor (UF): Its value depends on the current utilization of the available resources at each node and response time factor (RTF) of the node in the previous transaction verification process. The RTF is given by:

$$RTF = \begin{cases} 1.0 & if \ \ response\_time < 0.3\,sec. \\ 0.5 & if \ \ 0.3\,sec. < response\_time < 0.6\,sec. \\ 0.1 & if \ \ response\_time > 0.6\,sec. \end{cases} \tag{2}$$

And UF is given by

$$UF = \begin{cases} 1.0 & if \ \ current\_utilization < 0.3 \\ 0.5 & if \ \ 0.3 < current\_utilization < 0.6 \\ 0.1 & if \ \ current\_utilization > 0.6 \end{cases} + RTF \tag{3}$$

Trustworthiness factor (TWF): is the most important factor as its value increases every time by 2, if nodes perform correct verification and decrease by 5 if any node performs incorrect verification due to any malicious activity or whatever the reason. If node did not participate in the consensus then its value is increased by 1 to maintain the scope of this node in future consensus.

Now, overall trust factor of any node is given by:

Table 1 Proposed attributes of the miner's status to be maintained by each node about every nodes in the network

S. no.	Parameter	Size	Role
1	Node_ID	4 bytes	To maintain store the participants node's identifier
2	CCF	1 byte	To maintain the **Computation Capacity Factor** of an individual node i.e. available CPU, Memory, Network bandwidth
3	UF	1 byte	To maintain the current resource **Utilization Factor** of an individual nodes in the network
4	TF	2 bytes	**Trust Factor** i.e. overall trustworthiness of the individual node in the network

$$TF = CCF + UF + TWF \tag{4}$$

The trust factor of a node is used for selection of consensus agents for mining the block.

This trust factor is broadcast to all the nodes / miners in the system. This initial setup is done when any node / miner joins the p2p swarm. Each node maintains a list indexed on following attributes:

i. Load of BSM sorted on the load. Nodes above a certain threshold are designated as RHBM else RLBM.
ii. Further the same list is sorted based on the value of TF
iii. List of private miners is sorted on the TF score. TF of PM's above a certain threshold are designated as highly reliable else trusted/suspicious miners.

In the proposed system, the miners are categorized into four different groups based on their trust factor as shown in Fig. 6. The categorized five groups are:

– G1: Highly reliable RHBM,
– G2: Highly reliable RLBM,
– G3: Highly reliable Private (Authorized) Miners RAM,
– G4: Moderately reliable RLBMs & RAMs,
– G5: Un-trusted miners or other miners

G1, G2 and G3 are the groups of miners that achieve trust factor above 10 whereas in group G4, the miners with trust factor between 5 to 10 are included. The miners that have trust factor below 5 are classified under the G5 group as shown in Fig. 5. These miners will never get chance for being selected as consensus agents as discussed in Sect. 3.4.2.2. So this proposed method reduces the overhead of broadcasting a new block reduces by more than 50%. This again saves computation time and network bandwidth.

3.4.2.1 Role of leader in consensus mechanism The consensus mechanism discussed above uses multicast instead of the broadcast thus ensuring the scalability of the proposed system. The selection of the miner's for verification of the newly created block is responsibility of the leader miner based on the TF. Each miner in the network maintains a miner node status table. The leader selects randomly 25% miners from G1 group, 25% miners from G2 group, and 50% miners from G3 and 25% of G4 groups are selected. These selected nodes are called consensus agents. These consensus agents verify the new block and broadcast their votes to all the peers on newly created block.

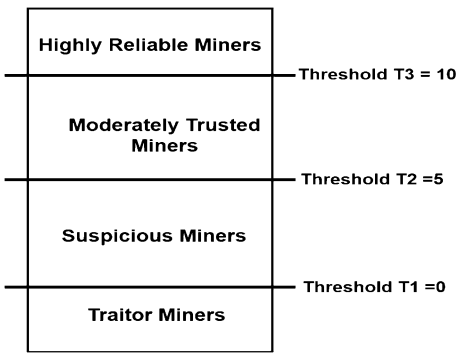

Fig. 6 Thresholds for classification of trust value of miners

3.4.2.2 Role of consensus agents The consensus agents receive the newly created block from the leader. The consensus agent verifies all the transactions stored into the block and the digital signature of the leader. After the verification process, consensus agent broadcast its consensus on newly created block to the all peers in the network.

3.4.2.3 Role of the other miners The miners including consensus agents receive the newly created block from the leader and store it to the temporary buffer. Now all the miners wait for the consensus votes of the consensus agents. Each miner maintains miner node status table; hence, each miner waiting for consensus, can identify the consensus agents. The miners updates the trust factor of the consensus agents based on the votes and trust management policy. This table records the list of those agents that are in favor of adding the block meaning thereby that the block is valid (all transactions listed in block are verified and authentic) and list of the agents those who are not in favor of the block meaning that the block is invalid as shown in Table 2. All the Miner stores the votes of the agents into this table.

On receipt of votes from all the agents, each miner computes the final consensus on newly created block based by the counting of votes. It is proposed that minimum 10% of the votes among nodes of G1, 41% of G2, 51% of G3 and 25% nodes from G4 are required in order to achieve final consensus as shown in Fig. 7.

This ensures the following:

i. Majority vote among BM is achieved although only few reliable nodes participate,
ii. This multicasting also reduces network load &
iii. Even if all the RAMs collude, these nodes can't hijack the consensus mechanism.

Each miner including leader and consensus agents vote for the final consensus. This final consensus decides whether the block should be added to blockchain or not. The leader notifies the block status to the bank server that generates the e-cheque clearance transaction.

Table 2 Agent vote during consensus process

Hash of new block	Favorable agents			Not favorable agents		
	CN ID	Response time	Group	CN ID	Response time	Group
HashValue	RHBM1, RHBM2, RHBM3, ...	T1, T2, T3, ...	G1	RHBM5, RHBM8, RHBM9, ...	T1, T2, T3, ...	G1
	RLBM1, RLBM2, ...	T4,T5, ...	G2	RLBM7, RLBM 6,	T4, T5,	G2
	RAM1, RAM2, RAM3, ...	T7, T8, T9.....	G3	RAM4, RAM4, RAM8, ...	T7, T8, T9.....	G3
	MRAM1, MRAM2, ...	T10, T11, ...	G4	MRAM7, MRAM9, ...	T10, T11, ...	G4

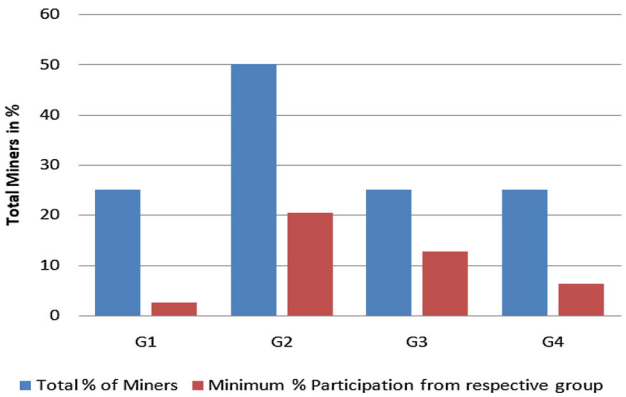

Fig. 7 Vote share for final consensus

3.4.2.4 Analysis of proposed trust based consensus mechanism Analysis of the proposed TCA is carried out in order to establish its validity and robustness. Further, the results obtained are compared with the widely used PoW [20] algorithm based on the following parameters:

i. Number of messages exchanged,
ii. Time required to achieve consensus &
iii. Analysis of CPU, memory & network utilization of consensus node (CN).

During the experiment, all these parameters are recorded and analyzed when a new block is being created and broadcast to all miners for verification of transactions stored in it.

Number of messages exchanged The performance of the proposed TCA consensus approach is measured in terms of number of messages required as shown in Table 3 to achieve the consensus. In traditional approach, all 'N' miners participate in consensus process and broadcast their consensus to all 'N − 1' nodes. This causes the overhead in network as total N(N − 1) messages are exchanged. In the proposed approach, fewer numbers of nodes are selected on the basis of respective trust value only and these selected nodes participate in the consensus mechanism. During different simulations, results are recorded with increasing number of miner nodes (N) and its impact on the total number of messages exchanged in order to achieve consensus. Let, the total number of miners are N,

Among these N, let, total number of G1 miners be $g1$, total number of G2 miners be $g2$, total number of G3 miners be $g3$ and Total number of G4 miners be $g4$.

Hence $g1 + g2 + g3 + g4 = N$,

Let the total consensus agents selected from G1 group be defined by $a1$ as $(25 * g1)/100$, $a2$ as $(50 * g2)/100$, $a3$ as $(25 * g3)/100$ and $a4$ as $(25 * g4)/100$. Hence total number of message exchange (TME) require in consensus process are:

$$TME = (a1 + a2 + a3 + a4)(N - 1)$$

Minimum number of consensus message (MFC) required in achieving Final_Consensus is:

$$MFC = \{(a1/10) + 1 + (2 * a2/5) + 1 + (a3/2) + 1\} * (N - 1)$$

Total message exchange required in proposed approach are also compared with the traditional approaches as shown in Table 3.

The analysis of results listed in Tables 3 and 4 revels that the proposed approach requires on an average only 32.2% of message exchange per consensus process as

Table 3 TME and MFC analysis in varying number of nodes in network

S. no.	N	g1	a1	g2	a2	g3	a3	g4	a4	TME	MFC
1	100	30	8	30	15	20	5	20	5	3267	1386
2	200	50	13	50	25	50	13	50	13	12,736	4378
3	300	70	18	70	35	100	25	60	15	27,807	9867
4	400	100	25	120	60	100	25	80	20	51,870	18,753
5	500	120	30	150	75	130	33	100	25	81,337	28,942
6	600	140	35	180	90	160	40	120	30	116,805	36,539

Table 4 TME and MFC comparison of traditional and proposed approach

S. no.	N	PoW		Proposed approach		Message reduction proposed approach (%)	
		TME	MFC	TME	MFC	TME	MFC
1	100	9900	4951	3267	1386	33	27.9
2	200	39,800	19,901	12,736	4378	32	21.9
3	300	89,700	44,851	27,807	9867	31	21.9
4	400	15,960	79,801	51,870	18,753	32.5	23.4
5	500	249,500	124,751	81,337	28,942	32	23.2
6	600	359,400	179,701	116,805	36,539	32.5	20.3

compared to traditional PoW approach. The proposed trust based consensus mechanism requires minimum 23.66% MFC from trusted miners to achieve the consensus.

3.4.2.5 Byzantine failure property *Agreement condition* On receipt of votes from all the agents, each miner computes the final consensus on newly created block based on the vote count received. It is proposed that minimum 10% of the votes among nodes of G1, 41% of G2, 51% of G3 and 25% nodes from G4 are required in order to achieve final consensus. Failure of few agents shall not prevent achieving final consensus.

Validity Each miner computes the final consensus on new block based on agreement condition. This algorithm decides the validity of the new block based on the proposed consensus policy. Another role of the each miner is to update the trust value of the consensus agents. The trust value of each agent is updated based on the trust management policy as elaborated in Sect. 3.4.2.1. Any miner is moved to unreliable miner list as soon as its trust value decreases below certain threshold. The proposed value of the TF threshold is different for each group of miners. This is important since BSMs shall always carry computational systems that are no match with the resources of AM. Hence, if differential TF is not used, then during selection of nodes for mining, PMs shall always be part of the dominating set of nodes. This shall risk the consensus hazard as these entities can collude. Termination Based on the agreement condition and validity, final consensus is computed based on the agreement of the trustable nodes from each group.

Agreement result

Case 1: In case of No failure

Agreement attainable;

Case 2: Crash failure

Total number of miners are N and among these N, let, total number of G1 miners be g1, total number of G2 miners be g2, total number of G3 miners be g3 and Total number of G4 miners be g4. Agreement is attainable even if (a1+a2+a3+a4) nodes among total N nodes are working.

Case 3: Byzantine failure

Condition for byzantine failure $f <= |(N-1)/3|$ Here, f denotes number of failure-prone processes and N is the total number of processes. In the proposed system, agreement is attainable because it requires agreement of 33% of nodes for achieving the final consensus. Hence even if 33% nodes fail, there still exist enough number of agents.

Comparasion with practical byzantine fault tolerance (pBFT): In pBFT [4] model, an algorithm works effectively when the total number of malicious nodes doesn't exceed by 1/3 of the total nodes. This means that the algorithm is reliable if at most $(N-1/3)$ nodes are reliable. In proposed trust based consensus mechanism, at most 1/3 of the trusted nodes from group G1, G2, G3 and G4 are required for agreement. Hence, this condition shall never arise and the approach is reliable even if more than 33% of overall nodes are malicious.

3.4.2.6 Time required to achieve consensus In this experiment, time to achieve the consensus on same block is recorded for the proposed approach and proof-of-work approach. In each iteration, the number of miners is increased by 100 with consensus nodes (CN) being constant. From Figs. 8 and 9, it can be observed that the proposed trust based consensus mechad 9nism requires

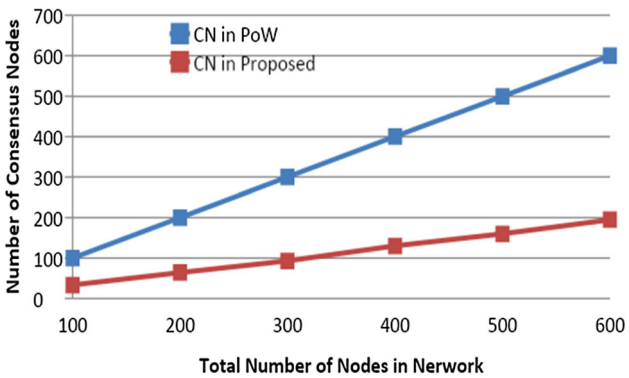

Fig. 8 Comparative number of participation of nodes during consensus in PoW [20] and proposed approach

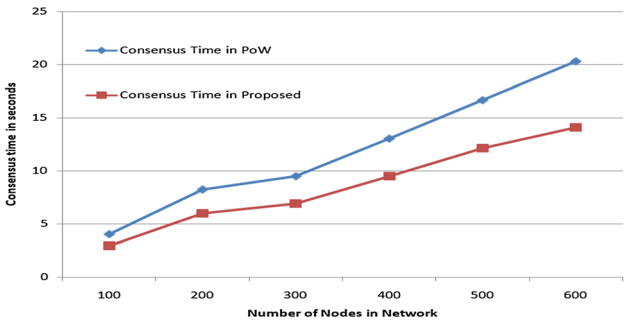

Fig. 9 Comparative time for achieving consensus in PoW [20] and proposed approach

fewer consensus nodes nodes as compared to PoW for achieving consensus. Coupled with this benefit is atleast 25% lesser time requirement for adding any new block.

3.5 Proposed multithreaded parallel transaction search algorithm (MPTSA)

In any blockchain application, among other factors, the time for consensus on any new block also depends on the number of transaction placed in new block. This is because each miner has to traverse the blockchain in order to verify these new transactions. Hence, the deeper the blockchain traversal required, higher the time required to verify the transactions. To reduce the verification time, this paper proposes a multithreaded parallel transaction search algorithm. This algorithm traverses the blocks in parallel by using kernel level threads. Searching a transaction in blockchain involves traversing blockchain sequentially and comparing each transaction details with the attribute of transaction being verified. To reach any predecessor block, the hash value of that block that is stored in its successor block is used. The retrieved block contains list of transactions and hash value of its previous block. In the proposed approach, certain number of kernel level threads is used to achieve the parallelism in tasks such as retrieving a block and comparing the transactions. One of the threads gets placed at previous block while all other threads perform read and comparison operation as shown in Fig. 10. This causes parallel processing of transaction comparison

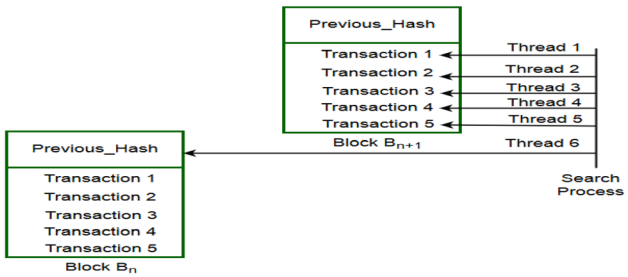

Fig. 10 Proposed parallel transaction search

task along with advance block retrieval. For example, if a block contains 5 transactions in any blockchain, then the proposed approach searches for the transaction with 6 threads such that one thread always works for retrieving the contents of previous block and remaining five threads perform transaction comparison operation for five transaction per block. This will enhance the overall performance of the searching time with multi-core processing capability. Figure 10 shows the illustration of parallel search execution of task.

3.6 Analysis of proposed multithreaded parallel transaction search algorithm (MPTSA)

To verify the performance of proposed MPTS algorithm, experimental setup carried out in java on machine having CPU configuration as Intel i7-4790 @ 3.60 GHz, RAM 8GB DDR3 (1600 MHz), Networking: 10/100 Ethernet, 2.4GHz 802.11n wireless, Storage: 100GB. In this experiment, random query is fired and search time of the proposed approach with different number of parallel thread is obtained. The overall experiment is performed in two scenarios.

In first scenario, length of the blockchain is kept 1500 blocks and size of block is 40 KB. In second scenario, the length of blockchain is kept 2000 blocks and size of each block is fixed to 400KB. In both scenarios, the search time of the approach is recorded for 1, 4, 8 and 16 threads as shown in Fig. 11. For six different simulations, the average time reduction for searching any cheque transaction details is more than 60% on an average. Hence the proposed MPTSA shall lead to faster clearance of the pending cheque transactions.

3.7 Vulnerability analysis of the proposed approach

The digital documents are always vulnerable to alteration, threat of being counterfeit etc. Apart from this, customer may create multiple copies of digital document; hence vulnerability of the issued e-cheque for alteration and double spending problem needs to be analyzed. This section discusses the inherent capability of proposed system to handle such security threats.

3.7.1 Handling the threat of alteration of e-cheque

In the proposed system, the e-cheque issued by any drawer is always recorded in the blockchain in the form of a transaction. The blockchain is stored on nodes that are residing in different sites and connected through decentralized p2p network. Proposed system is able to detect altered e-cheques at the time of deposit of e-cheque

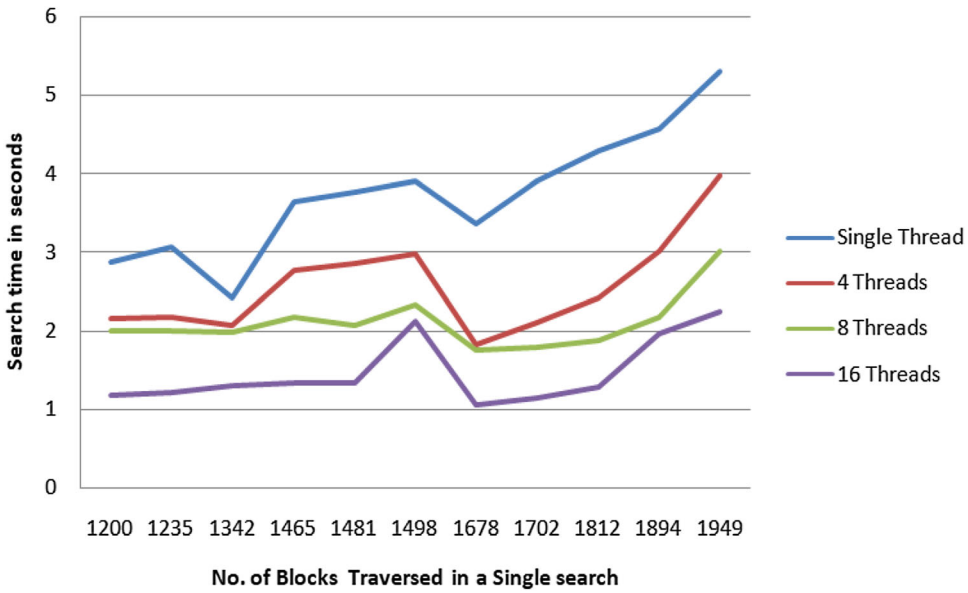

Fig. 11 Comparative search time for searching a transaction from blockchain with different level of parallelism

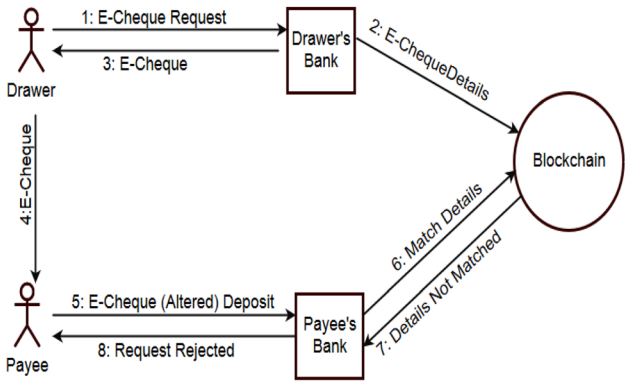

Fig. 12 Detection of e-cheque alteration

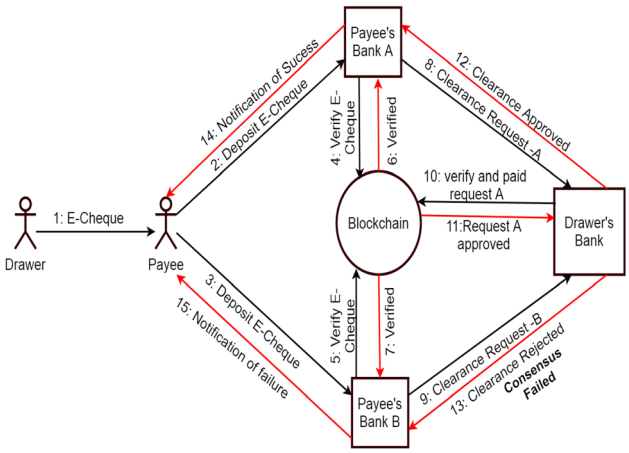

Fig. 13 Handling threat of double spending of e-cheques

because each deposit operation requires consensus of miners as discussed in Sect. 3.4. Figure 12 explains the detection and rejection process of any altered e-cheque by the proposed system.

3.7.2 Handling threat of double spending of e-cheque

The e-cheque issued to any payee may be deposited in multiple banks by the payee. As discussed in Sect. 3.3 that elaborates "Proposed Blockchain based e-cheque Payout Process", when a payout is achieved at one bank, then during subsequent payout process, the miner during the consensus process shall detect the attribute "request_type" as being set to "e-cheque payout" in "block_type" field to "e-cheque payout" as illustrated in Fig. 13. Hence, the proposed system shall not achieve consensus for this second payout of e-cheque. Hence the proposed framework prevents double spending problem.

Once a request of e-cheque is committed in blockchain, another request for the same cheque will be rejected. The second e-cheque deposit request is rejected during clearance process at drawer's bank level. Hence, the proposed system is able to detect double spending of e-cheque.

4 Conclusion

This paper proposes a novel approach for transacting with e-cheque in banking to improve the clearance time and to reduce the manpower requirement in processing of cheque requests. The approach is based on blockchain technology and can be adopted by the current banking system with minimum integration effort. In order to achieve this, an efficient leader election and trust based consensus mechanism is proposed. On an average only 32.2% of nodes

participate in the proposed trust based consensus mechanism and therefore message exchange per consensus process is much lesser as compared to traditional PoW approach thus making the system scalable. This reduces the communication overheads by using multicast instead of broadcast during consensus message exchange of messages. The time required to achieve the consensus for any new block is 25% lesser as compared to existing approaches such as PoW. The average time reduction for searching any cheque transaction details is more than 60% on an average aiding in faster clearance of the pending cheque transactions. Hence, the proposed e-cheque transaction framework is suitable to be deployed in real time banking and an increase in the number of transactions shall not degrade the performance of this system, making it scalable.

References

1. Anderson, M.: The electronic check architecture. Financial Services Technology Consortium **123** (1998)
2. Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., Danezis, G.: Consensus in the age of blockchains (2017). arXiv:1711.03936
3. Barclays, I.: Barclays says conducts first blockchain-based trade-finance deal. https://reut.rs/2AQEG9w. Accessed 10 Jan 2019
4. Castro, M., Liskov, B., et al.: Practical byzantine fault tolerance. In: OSDI, vol. 99, pp. 173–186 (1999)
5. Chang, C.C., Chang, S.C., Lee, J.S.: An on-line electronic check system with mutual authentication. Comput. Electr. Eng. **35**(5), 757–763 (2009)
6. Cocco, L., Pinna, A., Marchesi, M.: Banking on blockchain: costs savings thanks to the blockchain technology. Future Internet **9**(3), 25 (2017)
7. Eyal, I.: Blockchain technology: transforming libertarian cryptocurrency dreams to finance and banking realities. Computer **50**(9), 38–49 (2017)
8. Gjomemo, R., Malik, H., Sumb, N., Venkatakrishnan, V., Ansari, R.: Digital check forgery attacks on client check truncation systems. In: International conference on financial cryptography and data security, pp. 3–20. Springer, Berlin (2014)
9. Guo, Y., Liang, C.: Blockchain application and outlook in the banking industry. Financ. Innov. **2**(1), 24 (2016)
10. Insurchain: Insurchain: a decentralized insurance blockchain ecosystem. https://github.com/InsurChain/whitepaper/blob/master/en/whitepaper-en.md. Accessed 10 Jan 2019
11. Jayadevan, R., Kolhe, S.R., Patil, P.M., Pal, U.: Automatic processing of handwritten bank cheque images: a survey. IJDAR **15**(4), 267–296 (2012)
12. Khalid, U., Asim, M., Baker, T., Hung, P.C., Tariq, M.A., Rafferty, L.: A decentralized lightweight blockchain-based authentication mechanism for IOT systems. Clust. Comput. **15**, 1–21 (2020). https://doi.org/10.1007/s10586-020-03058-6
13. King, S., Nadal, S.: Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. Self-published paper (2012)
14. Li, D., Cai, Z., Deng, L., Yao, X., Wang, H.H.: Information security model of block chain based on intrusion sensing in the IOT environment. Clust. Comput. **22**(1), 451–468 (2019)
15. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)
16. Nguyen, Q.K.: Blockchain-a financial technology for future sustainable development. In: *International conference on green technology and sustainable development (GTSD)*, pp. 51–54. IEEE (2016)
17. Niranjanamurthy, M., Nithya, B., Jagannatha, S.: Analysis of blockchain technology: pros, cons and swot. Clust. Comput. **22**(6), 14743–14757 (2019)
18. Rajender, M., Pal, R.: Detection of manipulated cheque images in cheque truncation system using mismatch in pixels. In: *2014 2nd International Conference on Business and Information Management (ICBIM)*, pp. 30–35. IEEE (2014)
19. Santander: Santander launches the first real-time trades in Spain using we.trade, a blockchain platform that helps companies go international. https://bit.ly/2Fw2pj7. Accessed 10 Jan 2019
20. Schwartz, D., Youngs, N., Britto, A., et al.: The ripple protocol consensus algorithm. Ripple Labs Inc White Paper **5** (2014)
21. Singh, K., Singh, N., Kushwaha, D.S.: An interoperable and secure e-wallet architecture based on digital ledger technology using blockchain. In: 2018 International Conference on Computing, Power and Communication Technologies (GUCON), pp. 165–169. IEEE (2018)
22. Singh, N., Vardhan, M.: Distributed ledger technology based property transaction system with support for IOT devices. Intl. J. Cloud Appl. Comput. **9**(2), 60–78 (2019)
23. starbase: Support innovative projects with star. https://starbase.co/star?lang = en. Accessed 10 Jan 2019
24. Tschorsch, F., Scheuermann, B.: Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutor. **18**(3), 2084–2123 (2016)
25. Tseng, L., Yao, X., Otoum, S., Aloqaily, M., Jararweh, Y.: Blockchain-based database in an IOT environment: challenges, opportunities, and analysis. Cluster Computing, pp. 1–15 (2020)

Nikita Singh received her Bachelor's degree in Computer Science & Engineering from Abdul Kalam Technical University, Lucknow, India in 2015 and M.Tech. in Computer Science and Engineering from Banasthali University Rajasthan, India in 2018. She is currently pursuing PhD degree in Computer Science and Engineering at National Institute of Technology Raipur, Raipur, India. Her research interests include image processing, computer vision and blockchain technology. She has published over 05 SCI and Scopus indexed research articles in International conferences and Journals.

Tarun Kumar is currently working in GL Bajaj Institute of Technology and Management, India as Associate professor. He received PhD degree in Computer Science and Engineering at Motilal Nehru National Institute of Technology Allahabad, Allahabad, India. His research interests include image processing, distributed computing and blockchain technology. He has published more than 14 research articles in various SCI and Scopus indexed journals and conferences.

Manu Vardhan received his PhD degree from Motilal Nehru National Institute of Technology Allahabad, Allahabad, India in 2013. Present he is working as Assistant professor in National Institute of Technology Raipur. He has published more than 50 research articles in various SCI and Scopus indexed journals and conferences. His research interest includes distributed computing, service oriented architecture (SOA), blockchain technology.