An Architecture for Blockchain-based Cloud Banking

Thuat Do

Hong Kong University of Science and Technology, Dept. Math.
Clear Water Bay, NT, HK,
thuat86@gmail.com

Abstract. Blockchain has been practiced in crypto-currencies and cross-border banking settlement. However, no clear evidence that a distributed ledger network (or Blockchain) is built within domestic payment systems, although many experts believe that Blockchain has wide applicability in various industries and disciplines. As the author's best knowledge, no one has published a clear architecture and a feasible framework for a Blockchain-based banking network. Thus, "*how Blockchain can be implemented in domestic banking systems*" is a big challenge. The most important contribution of this work is to give a feasible and viable framework resolving that problem. The author investigates a Blockchain-based payment framework, more explicitly, a decentralized banking architecture running on the top of existing banking cores. The Blockchain network has two tiers: master nodes (block generators) and normal nodes (validators). The consensus mechanism is introduced as a composition of Proof of Stake, Proof of Reputation and/or practical Byzantine Fault Tolerance. In addition, nomination and approval mechanisms are added to the governance to enhance legal compliance and compatibility with real Fintech space. Some qualitative analysis is provided to show that the proposed Blockchain banking framework offers better security, scalability and decentralization, while easily adapt with different national regulation environments, among other Blockchains. In the application aspects, the framework is implementable and deployable for decentralized payment network and smartcontract infrastructure for domestic markets, then enable a complete and unified digitized space for cloud banking and financial services.

Keywords: Blockchain, Byzantine Fault Tolerance, cloud banking, decentralization, distributed ledger, distributed ledger technology, proof of stake, proof of reputation

1 An introduction

1.1 A literature review on Blockchain and its applications

Distributed Ledger Technologies (DLTs) are based on two fundamentals: cryptography (public keys, hash functions) and consensus mechanism. Its goal is to create a unified and trusted ledger which is secure, always available, shared among the involved parties and impossible to control by any single party. In terms of information technology, a distributed ledger is simply a replicated database of transaction data and some other information (e.g. coin reward, messages).

Based on architecture, all the implemented DLTs can be classified into three types: Blockchain, Tangle and Hashgraph. While the two laters are complex systems based on the Directed Acyclic Graph structure, the former is easily understood as its name, *a chain of blocks*. IOTA is the most famous project deployed Tangle [17] since 2017. Hedera [7] is a typical project applied Hashgraph since 2019. However, Blockchain is the most popular, intensively studied and developed DLT which is original from Bitcoin and proven via many notable projects, for instances, Ethereum, Ripple, Corda-R3, Azure (Microsoft), Quorum (acquired by Consensys from JP Morgan Chase).

Blockchain has become a new HOT industry worldwide not only in cryptocurrency communities but also among scientists, technologists, developers and regulators. Chinese government has promoted Blockchain as a breakthrough technology and gave huge support for research and development, targeting the leading position of the nation in the new space. According to CBINSIGHTS's report [8], Blockchain and DLTs can revolutionize the global financial sector worth around 134 trillion dollars, ranging in the following zones.

Payment. By establishing a distributed ledger, Blockchain provides faster payment with lower cost in comparison to current banking systems. Cross-border payment is usually complicated, time-consuming and costing $5-20\%$ remitted amount, while Blockchain is believed to cut down the fee to $2-3\%$.

BitPesa is a B2B payment Blockchain-based company operating in Kenya, Nigeria and Uganda, gained over 25,000 customers after 5 years, processed more than 1 million transactions worth of 340 million dollars. BitPay is another Blockchain-based payment company in the US, funded 72 million USD, accepting bitcoin payment.

Clearing and settlement. Ripple, a Blockchain startup specializing in bank settlement, estimates that it could cut 33% fee compared to SWIFT. Ripple has more than 100 customers. Stella collaborates with IBM to develop a Blockchain-based international payment for 44 banks in over 72 countries with 47 currencies. It only takes a few seconds to complete a transaction on its Blockchain. Corda-R3, a distributed ledger platform for bank settlement, aims to become a new *operating system* for the financial market. It has raised 107 million dollars from Bank of America, Meryll Lynch and HSBC in 2017.

Identity verification. This crucial process normally requires many steps and takes long time, multiple duplicated among financial institutions and companies. Blockchain helps create a decentralized, easily accessible, fast verifiable and secure database of digital identities with privacy. Cambridge Blockchain and Tradle are fintech startups which utilize Blockchain to enhance various procedures in banks with the help of a customer verification system.

Security token offering and digital asset exchange. In 2015, Nasdaq planned to use Blockchain for their private market platform, with the introduction of Colored Coin concept, to distinguish coins used in transactions with other types. Nasdaq joined Citigroup to invest in Chain, a Blockchain company which provides a reliable decentralized database that records all stock and ownership transactions in real time. Putting stock on Blockchain could save 17 to 24 billion dollars annually for global processing fee.

Credit and syndicated loan. By eliminating the *gatekeeper* in lending and credit, Blockchain can reduce risk. In 2016, Credit Suisse, Symbiont, R3 and Ipreo completed the first stage of a project using Blockchain in syndicated loan market. In April 2018, international banks, BNP Paribas, BNY Mellon, HSBC, ING, Natixis and State Street, jointly supported Fusion LenderComm by Finastra, a Blockchain platform for syndicated loan. BBVA, Mitsubishi UFJ and BNP Paribas gave a 150 million dollars of syndicated loan to Red Electrica, a Spanish electronic company. The event was recorded on Ethereum.

Trade finance. By simplifying procedures, Blockchain can strengthen transparency, security and trust among partners on the globe. TradeLens (Maersk and IBM joint venture) and eTradeConnect (formed by Hong Kong banks) are notable distributed platforms for trade finance. Voltron (under R3 and CryptoBLK) operates Blockchain-based platform for letter of credit application.

Crowdfunding. Initial Coin Offering (ICO) is a new way for tech startups to approach funding. In the first half of 2018, ICOs raised 13.7 billions dollars, doubled from 7 billion in 2017, according to Businessinsider [9].

Accounting and Audit. Distributed technology can help remove lots of paperwork involved in this field. Blockchain can become as a decentralized notary. Furthermore, smart contracts are useful for automatic invoicing. PricewaterhouseCoopers has developed Blockchain-based accounting service for enterprises.

According to Gartner [6], Blockchain is one of the most promising technology trends and can generate more than 176 billion USD by 2025, and 3.1 trillion USD by 2030. The technology is not yet mature, but it is temporary. Blockchain has been studying and developing extensively with significant progress.

1.2 The paper's structural contents

The article consists of seven sections. The first one gives a brief introduction about Blockchain (more generally, distributed ledger technologies) and its applications in real world. The second one presents the status and challenges of implementing the technologies in banking sector, the inspiration to build a feasible framework of Blockchain cloud banking. Section 3 describes the framework in details, for instances, network architecture, workflow, core protocols. The next section shows a deep discussion on governance of the Blockchain-based banking network, then it introduces node management mechanism and reputation system over the network. Section 5 presents block production and consensus process. The consensus is a modification of Delegated Proof of Reputation (DPoR) introduced in [18], and can be viewed as a hybrid of Proof of Stake and a reputation ranking system. Section 6 differentiates the proposed framework with existing Blockchain networks (both public and private/enterprise), then analyzes its advantages. The final section gives application perspectives, assessment and conclusion. The most important contribution of the paper is a Blockchain framework for cloud banking with network architecture, governance and consensus mechanisms clearly described.

2 Blockchain in domestic banking: challenges and inspiration

When studying applications of Blockchain in banking and finance, people immediately think about global crypto currencies (e.g. bitcoin, ether, Libra, etc), international settlement or money transfer (e.g. Ripple, Corda-R3, Quorum which aim to replace Swift Code protocol), international trade-finance (Tradelens, eTradeConnect). Obviously, there are big barriers in cross-border value transfer that Blockchain can erase. Nonetheless, *"how Blockchain can disrupt national banking systems? Can it renovate a national payment gateway, i.e. interbank payment?"* are big questions without any example or proposal out there. Relating Central Bank Digital Currency (CBDC), big organizations has published investigations and reports combining both regulation and technology consideration. World Economic Forum (WEF) indicated 10 use cases that central banks can apply DLT [1]. After that WEF provides a study and assessment toolkit for CBDC policy maker [3], which mentions stablecoins as an alternative and example for CBDC. Bank for International Settlements (BIS) appreciates DLT to offer a resilient digital currency system [2]. Brookings [12] presents design choices for CBDC together with deep investigations on centralized and decentralized ledgers, digital identification, digital wallet, account and UTXO models. China has developing its digital Yuan (already in piloting stage) but no backed peer-to-peer network or Blockchain design behind the digital currency is disclosed or open apparently (read more in [19]). Overall, developers cannot find any implementable framework in the mentioned studies to build a Blockchain (or DLT) network for domestic banking applications.

Alipay, Wechatpay, M-Pesa have been successful to provide a frictionless and seamless payment, even more extensive banking and financial services (e.g. saving, investment) to end-users everywhere simply via mobile, without coming to bank offices. Based on connections with bundles of banks (via APIs), they provide many banking services, but they are not truly banking institutions with full regulatory compliance (which is unfair for banks). In addition, they are centralized escrows possibly causing concerns on monopoly, financial security (single failure), transparency and privacy. No one can find a *ready-to-run* open API platform for banking services (i.e. Inter-Banking Cloud Infrastructure as a Service), which allow many fintech firms to provide inclusive banking and finance applications to end-users seamlessly with low implementation cost and without friction.

Smartcontract is successfully applied in crypto space but not in the conventional industries, although its wonderful potential of applications in various disciplines and landscapes is described extensively. For example, smartcontract can function as the second-layer of a CBDC system and boost innovation from commercial banks and fintech developers (Section 7, [2]).

Although many researches on application of Blockchain and DLTs in banking sector have been conducted, there is no feasible framework for implementation. Therefore, the author is going to design a Blockchain network architecture for banking and financial industries, attaching with core protocols, governance and consensus mechanisms. In the next sections, the terms of the Blockchain, the network, the cloud, the banking cloud, the Blockchain banking cloud all refer to our proposed framework (i.e. the Blockchain-based banking cloud, unless otherwise specified. Analogously, the terms of account, wallet, address are used alternatively, unless otherwise specified. Readers can understand that *banking cloud* refers to a decentralized IT infrastructure while *cloud banking* means banking services running on the cloud. However, in this paper, those two terms can be used alternatively.

3 A framework for Blockchain-based banking cloud

3.1 Sketching a network architecture

The author envisions a Blockchain-based banking network, in other word, a decentralized infrastructure for various banking and financial applications, e.g. money transfer, payment, saving, investment, etc. The network can function a decentralized cloud banking infrastructure as a service, running on the top of existing core-banking systems. Then all banking and financial services can be implemented as decentralized applications, running on the top of the cloud (i.e. the Blockchain), which utilize all advantages of Blockchain and smartcontract, while preserving the essential legal compliance and security of the banking systems.

3.2 Two-tier network and workflow

The proposed network is not pure peer-to-peer like Bitcoin, Ethereum and other public Blockchains. It consists of two classes (or tiers): master nodes and normal nodes (see Fig. 1) with different right and role. The necessary and sufficient conditions to become such a node will be presented in Section 4.

- **Master nodes** are block generators who hold the ultimate power, be able to function all core protocols and the consensus mechanism, and store full block-data. Only legitimate banks can become master nodes. The block generators verify submitted transactions, then gather in a block and finalize it according to the consensus mechanism (presented in Section 5).
- **Normal nodes** are transaction validators. Banks, financial institutions, payment service providers, big merchants, can join the network as normal nodes. The validators receive transaction proposals from clients (i.e. from end-users), validate them and then forward to master nodes for confirmation and finalization.

In general, clients may submit their transaction proposals directly to master nodes. However, master nodes give priority to the validated transaction pool. Normal nodes help validate transactions before sending to master nodes, thus reduce the block generators' workload. The workflow is provided in Fig. 2. In addition, the network allows nodes attaching their private chains (or private payment channels) on the main chain, thus improving the overall scalability and performance.

3.3 Block-data and distribution

Since the network is classified into two distinguished tiers, its block data should be designed in a different way to assure appropriate compliance and privacy. Block data is divided into three parts: Header, State and Body (see Fig. 3. A short description for block data attributes is given below.

- The **Header**
  1. Hash of previous block (i.e. hashing value of the previous block data).
  2. Time stamp presents the time point of block generation.
  3. Root hash of the Merkle tree.
- The **State**
  1. New registered identification hashes (e.g. hashing values of [*name, identity number, birthday*]).
  2. New registered account addresses (e.g. hashing[*bank code*] +hashing[*public key*]).
  3. Balance and state updates show new state changes on the entire network, (e.g. [*identity-account mapping, account addresses, available balance, other new states*]).
  4. Coinbase presents rewards (paid via a native token like bitcoin, ether). Feebase describes stable-coin-based transaction fee. Rewards and fees are accompanied with an appropriate distribution over the nodes.
- The **Body**
  1. Clearing updates show clearing statistics among participant banks (commonly master nodes only) so they can proceed to settlement, e.g. via an outside clearing house.

2. Transaction records show detail information of all transactions and their hash values, e.g. [*sender's addresses, receiver's addresses, number of transferred tokens*].

The proposed block data and its distribution differ with existing public Blockchains in the following major points (also read more in Section 3.4).

– **Account** and **identity**: Identification hash is mapped with a real identity stored off chain. An identification hash may be attached with (at least) one or many account addresses. Every account must be mapped with at least one identity.
– **Coinbase** and **feebase** presents a dual-token model. The coinbase utilizes a native token (like bitcoin, ether) to incentivize participating nodes for contribution to the network operation. The feebase uses stable coins (i.e. digitized fiat currencies based on bank pledge) as transaction fee utilities, except native coin transactions.
– **Clearing update** gives clearing statistics among participant banks so they can proceed to settlement, especially in real time without a centralized clearing house, provided a builtin central bank digital currency.

Master nodes play the critical role of full block data storage and full operation on the network. When a block is produced and endorsed, the generator will broadcast it fully to other master nodes, the header and the state to normal nodes. The normal nodes can use the header and the body for Simplified Payment Verification (SPV) and transaction validation without asking master nodes. SPV nodes on Bitcoin Network must ask full nodes to verify certain transactions. Thus, normal nodes in our network are neither precisely equivalent to Simplified Payment Verification nodes nor full nodes on Bitcoin or Ethereum. In addition, block data (specified relevant transaction info) is partially updated to the associated users. This task is normally done by normal nodes and client servers.

3.4 Core protocols

We are going to describe the core protocols of the proposed Blockchain-based banking cloud, which are identification protocol, incentive protocol, stable coin protocol and clearing protocol (the three laters are for master nodes only).

Identification protocol utilizes hash (checksum) techniques to help identity verification better and faster. The Blockchain network does not store customer identity information but its hashed value for cross verification. Member banks and other network participants keep their own customer identity information in their own private database. The only thing the members do is registering (i.e. submitting) identity hash values on the network. Note that each identity hash is identical with one and only one body (e.g. an individual, a company or an organization).

The procedure is as followed.

1. An user request opening an account on the cloud banking network. The node storing his identity info will hash the data, then broadcast the hashed value associated with (at least) one or many new public addresses to the network. The registration is complete once the identity hash and its associated address(es) are included in a confirmed block. Then the user can make transactions.
2. If no identity information exists, then the user is required to complete Know Your Customer (KYC) process. After KYC, it returns Step 1.

The identification hash helps the network's participants verify the existence of an identity while keeping the original identity information confidentially outside the Blockchain. This protects privacy and confidentiality while facilitating cross verification, certification and information exchange. Note that all public Blockchains (e.g. Bitcoin, Ethereum) store anonymous addresses without any mapping to real identities. Our proposed Blockchain is anonymous on chain but every account is associated with a verified KYC info stored off-chain (at least in some node's private database).

Incentive protocol is implemented at the bottom of the Blockchain, and only master nodes (as block generators) have the right to function and maintain it. The protocol issues a unique native token (or native coin) utilized for staking (in the consensus mechanism) and rewarding on the entire Blockchain network. The native coin represents the intrinsic value of the Blockchain cloud banking network analogously to crypto assets (e.g. BTC of Bitcoin, ETH of Ethereum), which may varies over time. Therefore, no stable coin (e.g. digitized fiat types) can satisfy that special nature. The protocol will pre-mine a certain amount of native coins at the genesis block (i.e. block 0) to use for initial staking of the foundation nodes. After that the new coins are generated as reward per newly produced block and distributed appropriately to all nodes, and possibly to the development foundation. This is clearly indicated in the coinbase of the block state (see Section 3.3). For example, the parameters of the incentive protocol can be set as followed (also read Section 4).

- The block reward rate is max 2% of the current supply per year, evenly divided per block. One can set a maximal supply (e.g. 1 billion native coins), i.e. the protocol will not generate new coins any more after reaching that number.
- In each block, coinbase protocol computes and distributes new generated coins and transaction fees (applied for native coin transactions and specified executions only) as the following. Assuming there is N nodes on the Blockchain network.
  - 10% or $1/N$ (for which smaller) to the block generator.
  - 5% or $1/2N$ (for which smaller) to the block endorsers who co-sign to finalize the block (if any), other than the generator.
  - 10% or $1/N$ (for which smaller) to the transaction validators (evenly divided by the number of native coin transactions included in the block),

- 3% or $1/3N$ (for which smaller) to the development foundation.
- The rest 72% will be distributed evenly as 44% to all master nodes and 28% to all normal nodes.

Stable coin protocol (more explicitly the fiat digitization protocol) is implemented at the bottom of the Blockchain, i.e. only master nodes have the right to operate and maintain it. The protocol allows issuing digital tokens 1-to-1 corresponding to equivalent cash pledged in bank and burning the tokens corresponding to cash withdrawal amount. This means no new currency is issued. The token is simply an accounting representative of cash reserve in bank. The protocol also provides digitized fiat balance update of all accounts on the network. Zero Knowledge Proof algorithms can be implemented to blind user balance updates (in the state of block data) sending to normal nodes. An implementation of shielded transactions and addresses can be found on Tron using zk-SNARK [4]. The purpose is protecting privacy on the entire network while allowing easy verification and fully tracking on the master nodes and the account holders respectively.

The stable coin is issued based on user request, and the cashin and cashout procedures are as followed.

- **Cashin** allows users (with registered account on the network) deposit to the Blockchain network based on their cash balance in bank. For example, an user requests a deposit of $1000, his home bank verifies and confirms if his cash balance is enough. Then the bank (also a master node) issues $1000 stable coins to the user's Blockchain account.
- **Cashout** allows users withdraw cash from his own balance on the Blockchain. For example, an user requests a withdrawal of $1000, any member can verifies his balance and confirms cash providing. Then $1000 stable coins are deducted from the user account and sent to the burning address (containing exactly non-reusable redeemed stable coins).
- Cashin must be executed by associated banks while cashout can be provided by any member of the network.
- Fee for Cashin and Cashout is cash basis and depends on the service providers.

In addition, the stable coin protocol allows nodes to setup their desire fee for transaction validation and confirmation, except native coin transactions. The protocol also returns feebase to be included in the state of block data (Fig. 3). In addition, the protocol allows multiple stable coin issuance. Each type of stable coins can be easily converted to others via atomic swap techniques which has many practiced implementations in crypto-currency space.

Clearing protocol is implemented at the bottom of the Blockchain, and only master nodes have the right to operate it. Per block, the protocol reads

```
#per participant bank, run
   Cash_flow = Cashin - Cashout
#then for the entire network, return
   Clear(positive Cash_flow group, negative Cash_flow group)
```

The *Clear* function returns the outside clearing house a statistics for further settlement and state update within the corresponding banks. Note that the following equation is always hold per block

$$\sum cashin = \sum cashout + \sum fees + \sum stable\_coins. \tag{1}$$

Note that in Equation (1), the fees (if applied) are paid in stable coins for all transactions, except native coin transactions, and the stable coins are usable (i.e. not redeemed).

Unlikely pairwise clearing method used in central clearing houses, our Blockchain banking cloud enables group clearing among multiple parties. For example, assuming that there are five banks $\{B_1, B_2, B_3, B_4, B_5\}$ in the clearing process.

The central counterparty always does all pair-wise clearing and settlement (10 computations and 10 updates) per transaction update

```
clear(B_1,B_2)  clear(B_2,B_3)  clear(B_3,B_4)  clear(B_4,B_5).
clear(B_1,B_3)  clear(B_2,B_4)  clear(B_3,B_5)
clear(B_1,B_4)  clear(B_2,B_5)
clear(B_1,B_5)
```

On the other side, our clearing protocol only does clearing and settlement between the positive and negative groups, hence simplifies and speeds up the process. Moreover, it offers a capability of real time settlement provided a builtin CBDC. For example, without loss of generality, assuming that the banks has the corresponding balances, $\{+x_1, +x_2, +x_3, -x_4, -x_5\}$, where $x_i > 0, i = 1, ..., 5$. Then the protocol does 5 computations and 5 updates per block

```
Y = x_1 + x_2 + x_3
Z = x_4 + x_5
Deduct (x_1/Y)*Z from B_1
Deduct (x_2/Y)*Z from B_2
Deduct (x_3/Y)*Z from B_3
Settle x_4 for B_4
Settle x_5 for B_5.
```

4 Governance on the network

Our proposed Blockchain is neither permissionless nor permissioned. In fact, no central authority exists on the network. Then a nomination mechanism is introduced to ensure that only qualified candidates have opportunity to join the group of network operators while preventing corruption caused by one centralized authority and potential malicious guys.

4.1 The conditions to become a node

The necessary condition. To become an operating node, a candidate must stake a required minimum amount of native coins to activate (or register) the pair of public-private keys with the network. A higher minimum stake is required for master node role.

The sufficient condition. A body wishing to become a network operator (i.e. a master or normal node) must complete registration first, and then nomination. Explicitly, a candidate for normal node is required at least two nominations from normal nodes or one nomination from master nodes. A candidate for master node is required at least two master node nominators. One may ask an additional condition that the two nominators must possess (in summation) a minimum percentage (e.g. 10% or $2/N$ for which smaller) of the total reputation scores of all nodes, where N is the number of nodes. See reputation score in Section 2. Of course, at the genesis block, no nomination happens, and the foundation nodes are all promoted up by the developer legitimately. Note that, if the developer is not a legal licensed bank, it may not be a master node, because other foundation banks do not allow to build up such a network.

Node deactivation. An active node can decide itself to leave the network, simply inform its leaving with other nodes. Another way, operating nodes can vote to kick out some node if it is not honest with proven damage evidences for the network, or it is not qualified longer under the assessment of the majority. Votes are weighted by reputation scores (see Section 2) and at least 68% of weighted majority from the network is needed to deactivate a node. This mechanism helps removing proven malicious nodes from the network and promoting high quality nomination, honest commitment and frequent activities.

4.2 Reputation score system

Reputation is very important in social reality. It bases on two major factors: wealth and performance (or achievement). Thuat Do et. al. investigated reputation in Blockchain space and introduced a novel framework for consensus, namely Delegated Proof of Reputation, see [18]. Therein, ranking (inspired by Google's PageRanking) is an essential component contributing to reputation, applied not only for nodes but also all accounts on the network. It exploits the idea that a node's ranking is built up over time based on its cooperation (connection) and work achievement. Basically, more valuable transactions, more connection will get higher ranking. This paper doesn't study the ranking algorithms. The author only takes the idea that ranking is helpful to reduce the number of faulty nodes and malicious actions on the network while promoting integrity and quality contribution, hence improve overall security and reliability on the network.

Removing resource power suggested by EOS [5] and [18], the reputation engine in this paper computes staking and ranking factors to return normalized reputation scores. It is assumed that all qualified nodes have abundant resources to solve the tasks on Blockchain. The reputation scores are used for voting and choosing block generators, and formulated

$$Rep = \mu S + (1 - \mu)R, \tag{2}$$

where Rep is reputation score, S is normalized staking index and R is normalized ranking score. Readers refer to [18] for more detail on the reputation and ranking framework, computation and advantage analysis. The parameter μ in Equation (2) is the control multiplier balancing staking and ranking components. In the early stage of the Blockchain, the numbers of connections and transactions are small (i.e. insignificant), thus μ should be large and then gradually decrease. One can set $\mu = \max\{2^{-h/K}, \theta\}$, where $0 < \theta \leq 0.5$ is constant, K is a positive integer and h is block height. That means $\mu = 1$ at the genesis block, then monotonously decreasing to 0.5 at block $K-$th, and $\mu = \theta$ whenever $2^{-h/K} \leq \theta$.

Reputation penalty. If a node is kicked off from the network (see Section 4.1), then its nominators' reputation score will be considered as zero for 30 following days, although having positive values. Other punishments on reputation score can be voted and decided by the majority, then applied where appropriate.

5 Block production and consensus mechanism

A bundle of consensus protocols are proposed and implemented in various Blockchain networks. The most popular ones (by order) are Proof of Work (PoW), Proof of Stake (PoS) and Delegated Proof of Stake (DPoS). In this part, the author exploits Delegated Proof of Reputation (DPoR), introduced in [18], with a modification (i.e. removing resource power in overall reputation).

Accounts on the network are allowed to grant their reputation scores to operating nodes (this is similar to voting procedure in Tron [4] and EOS [5]). A node's reputation score (included granted quantities) is converted to the probability of the node to be selected as transaction validators, block generators, reputation score providers and random source generators. Higher reputation score implies greater probability and hence earning more rewards and fees. Assume that the groups of master nodes and normal nodes are $\{M_1, ..., M_p\}, \{N_1, ..., N_q\}$ associated with reputation scores $\{Rep_1^M, ..., Rep_p^M\}, \{Rep_1^N, ..., Rep_q^N\}$, respectively, where p, q are positive integers. Then the normalized probability outputs are

$$Prob_i^M = \frac{Rep_i^M}{\sum_1^p Rep_j^M}, \quad Prob_i^N = \frac{Rep_i^N}{\sum_1^q Rep_j^N}. \tag{3}$$

Block producing process is divided into *epoches* and *gaps*. Each epoch contains a fixed length of blocks. Between two consecutive epoches, there is a short gap for conclusion on reputation score update and re-generating random sources. Based on the computed probabilities, the random sources determine:

- a reputation score result provider for the next epoch (or next K epoches);
- a random source generator for the next epoch;
- an ordered group of transaction validators among normal nodes;
- an ordered group of block generators among master nodes.
- an ordered group of gap-block generators (among all nodes) for the next gap.

To finish a certain gap, a special block (*gap-block*) is generated to record the info. A compensation (paid in native coins by the other nodes or coinbase reward) is given to the providers and the gap-block generator. The gap block (containing new reputation scores and random sources only) is valid and confirmed if at least 51% of the total reputation scores (including the granted quantities) of all nodes signed "*agree*". In addition, the gap block refers to the previous one to make it a check-point for reference or recovery if necessary.

Basically, a block generator, in its turn, will choose transactions validated by legitimate validators to package into a block. After that, it broadcasts the block randomly to other master nodes for finalization via a practical Byzantine Fault Tolerance (BFT) algorithm. There are many practical BFT algorithms out there, see [10, 11]. An open source of BFT implementation is Tendermint Core [14] which has been deployed on Binance Chain [16]. Normally, BFT requires at least $f+1$ replicas, $2f+1$ nodes and $\mathcal{O}(n^2 f)$ communication complexity to ensure error-free process and fault tolerance system, given f faulty nodes. Thanking to nomination mechanism, it is expected to reduce f remarkably, then speed up communication and finalization process. BFT allows a secure and instant finality on blocks and transactions but its broadcasting process is complex and costs long time. If real-time finality is not a strict requirement, the author suggests replacing BFT broadcast by the longest chain rule (as Bitcoin, Ethereum, Tron applied). In fact, a transaction on Tron Network can be considered as final (or immutable) if there are 20 block confirmations (equivalently 60 seconds), not a long wait.

The Algorand [15] Blockchain uses a Byzantine Agreement protocol and verifiable random function in its so-called *pure PoS* consensus system. Such a random function is a usefully practical implementation to deploy on other PoS-based Blockchains, as random sources play a critical role in the selection of block generators and transaction validators fairly and honestly.

6 Differentiation and advantage offering

Our proposed Blockchain framework differs from all the existing public, private and consortium Blockchains in several beneficial ways.

Creative and flexible architecture with two tiers offers a high adaptivity and compatibility with various banking and IT systems, while allowing nodes to attach their private chains easily. Some public Blockchains (e.g. EOS, Tron) designate network participants into super nodes (block generators) and standby nodes (doing nothing). On our proposed Blockchain, every node has its own role and tasks.

Novel block data and heterogeneous distribution make the framework more friendly with privacy and confidentiality while fully ensuring necessary tracing and tracking. This improves the compliance and adoption among regulators and banking institutions.

Novel nomination mechanism guarantees stable network expansion with qualifying entrance, hence enhances reliability among nodes.

Reputation system offers better decentralization (via granting reputation score) rather than pure staking and voting mechanisms on Tron and EOS, while promotes nodes and application developers working honestly and actively to gain reputation (see more rationales in [18]). Note that PoW (resp. PoS) Blockchains have been facing centralization on giant mining pools (resp. staking concentration on capital whales).

The advantages of the Blockchain cloud banking can be easily pointed out, both on technology side and application perspectives.

Better security, scalability and decentralization. Nomination entrance reduces potential faulty nodes, hence improve overall security. Two-tiers architecture with the capability of connecting private chains allows network scaling greatly. Reputation system promotes decentralization of network and builds trust on the network.

Fairness for developers. Application developers are important value contributors of any Blockchain network. Unfortunately, they do not have any right in the existing Blockchains' governance, although their billion dollar business are running on their tops. Our Blockchain framework gives the developers a chance to join network operators based on their reputation.

Regulation and adoption friendliness. Banks are more pleasant to join the network because the master node design precisely presents their special role, right and responsibility in the banking and financial sector. KYC problem, privacy and confidentiality are all resolved by the identification protocol (see Section 3.4) and block data distribution (see Fig. 3). As a consequence, the framework has high compliance capability with regulatory environments in different nations, and can satisfy real business practices.

Creative banking infrastructure design. This paper introduces the first framework for a Blockchain cloud banking which is universal and has many advantages compared to the conventional models. Moreover, by offering open APIs, the cloud will gather many fintech firms involved in the innovation of the financial industry. The Blockchain not only provides a secure and scalable cloud infrastructure for digital payment and banking services but also offers a feasible solution for financial inclusion expansion and coverage, especially to unbanked people via eKYC and digital banking model (see Fig. 5).

7 Applications, assessment and conclusion

Worldwide experts have recognized that Blockchain has many application potentials in all areas of the banking and financial sector. Regarding the applications of the introduced Blockchain banking cloud, it is applicable in an wide range of financial disciplines: accounting audit, asset tokenization, auto-invoicing, autogovernance, clearing settlement, credit info sharing, electronic payment, microfinance, micropayment, peer-to-peer money transfer, global money remittance, letter of credit, smartcontract-based transaction, syndicated lending. These perspectives are clearly indicated in many studies [2, 3, 6, 8, 12].

In November 11, 2020, all major media channels in crypto-currency space reported the Ethereum split issue happened at block 11234873. It observed a different chain held by a minority of the network miners whose the old Geth version (an Ethereum Blockchain client software) contained a dormant bug which was detected and reported two years ago. The issue affected deposit and withdrawal activities on Binance and many other crypto-currency exchanges. Although the bug was fixed and the whole network updated the main chain held by the majority, the event raised a big concern on centralized giant client servers. Moreover, the issue revealed that large network Blockchains possibly face the same failure due to latency and obsolescence among various groups of block keepers. Together with mining power concentration, people question decentralization and safety of Ethereum blockchain (see safety definition on [13]). Despite limited decentralization, Tron and our Blockchain frameworks offer many advantages on efficiency, stability and optimality while being robust and persistent to various attack and collusion schemes. In particular, they provide an easy recovery possibility which is very hard on Bitcoin and Ethereum (see a completed split and rollback on Ethereum Blockchain after the DAO attack).

Let acronym our proposed Blockchain Banking Cloud as BBC. According to the systematic framework (PREStO) introduced by S. Leonardos et. al. [13], we have a brief summary (see Table 1), assessment and comparison among Ethereum, Tron and BBC in Table 2.

More rationales to the assessment Table 2, our Blockchain model utilizes reputation system, hence offers higher decentralization of network resource distribution and fairness to application developers (also value contributors on the Blockchain). In addition, by the nomination and voting mechanism, our Blockchain has sustainable governance and network expansion.

For conclusion, the paper has introduced a novel framework for Blockchain banking cloud as a fundamental infrastructure for an open API platform in banking sector, then promoting innovation in payment and financial applications. The proposed Blockchain is implementable with clearly described architecture, governance, consensus, necessary techniques and protocols. We present assessment and potential applications corresponding with published studied frameworks. Although our tentative design leads to a domestic peer-to-peer banking system, the Blockchain model can be used for international bank settlement, cross-border escrow (money remittance) network wherein a secure, sharing, reliable, synchronous ledger and transaction processing system among participants is necessary and useful.

In the further work, the author shall provide more quantitative analysis on the Blockchain banking cloud, especially on the reputation system with some experimental results from existing public Blockchain transaction data.

PREStO Framework		**Design of Blockchain**
Persistance	Weak/strong persistence	51% attack defender, large network
	Majority attacks	Blockchain-Trilemma
	Recovery mechanisms	Design of sustainability
	Governance & sustainability	Decision of governance schemes
Robustness	Fault Tolerance	Protection against collusion
	Out-of-Protocol Incentives	Well elaboration with adversaries
	Resilience to attacks	
Efficiency	Positive scale effects	Scalable design
	Throughput rate	Energy saving
	Economy of resources	Compare to conventional solutions
	Benchmarking to centralized models	
Stability	Incentive compatibility: Participation, Operations, Applications	Incentive mechanisms
	Decentralization: entry barriers, distribution of resources	Protection against adversaries
	Fairness: reward allocation, voting-decision making	Decentralization motivation, fair distribution of resources
Optimality	Liveness	Architecture & Sybil protection
	Safety	Safety vs liveness trade-off
	Scope	Smartcontract execution
	Privacy features: public/private, permissioned/-less	

Table 1: Challenges & research opportunities in the design of Blockchain Protocols [13]

References

1. Central Banks and Distributed Ledger Technology: How are Central Banks Exploring Blockchain Today? Insight report, World Economic Forum (March 2019). bit.ly/3aGt23U
2. Central bank digital currencies: foundational principles and core features. Bank for International Settlements (October 2020). https://www.bis.org/publ/othp33.htm
3. Central Bank Digital Currency: Policy-Maker Toolkit. Insight report, World Economic Forum (January 2020). bit.ly/3mHDg69
4. DPoS consensus mechanism. bit.ly/3aGtb7s
5. EOS Consensus Protocol. bit.ly/37M3tws
6. Forecast: Blockchain Business Value, Worldwide, 2017-2030, Gatner's research. gtnr.it/3pyccZd
7. Hedera Hashgraph. https://docs.hedera.com/guides/
8. How Blockchain Could Disrupt Banking (2018). bit.ly/3aFq13y
9. ICO fundraising. bit.ly/2KVcWrX
10. Miguel Castro and Barbara Liskov. Practical Byzantine Fault Tolerance. OSDI'99: Proceedings of the third symposium on Operating systems design and implementation, pp. 173–186 (1999).
11. Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance and proactive recovery. ACM Transactions on Computer Systems (2002). bit.ly/3aFijqk

<table>
<tr><th><b>PREStO</b> framework</th><th>Ethereum</th><th>Tron</th><th>BBC</th></tr>
<tr><td><b>P</b>ersistance</td><td>High</td><td colspan="2">High</td></tr>
<tr><td>- Weak/strong</td><td>Strong</td><td colspan="2">Medium</td></tr>
<tr><td>- Recovery mechanisms</td><td>Hard</td><td colspan="2">Easy</td></tr>
<tr><td>- Governance & sustainability</td><td>Majority follow</td><td colspan="2">Majority voting</td></tr>
<tr><td><b>R</b>obustness</td><td>High</td><td>High</td><td>High</td></tr>
<tr><td><b>E</b>fficiency</td><td>Low</td><td>High</td><td>High</td></tr>
<tr><td>- Scalability</td><td>Extremely bad</td><td>Good</td><td>Good</td></tr>
<tr><td>- Throughput</td><td>Very low</td><td>High</td><td>High</td></tr>
<tr><td>- Energy</td><td>Consuming</td><td colspan="2">Saving</td></tr>
<tr><td>- Benchmarking</td><td>Extremely low</td><td colspan="2">Medium</td></tr>
<tr><td><b>S</b>tability</td><td>Medium</td><td>Medium</td><td>High</td></tr>
<tr><td>- Incentive</td><td>Fairly</td><td>Fairly</td><td>Good</td></tr>
<tr><td>- Decentralization</td><td>Highest</td><td>Medium</td><td>High</td></tr>
<tr><td>- Fairness</td><td>Medium</td><td>Medium</td><td>High</td></tr>
<tr><td><b>O</b>ptimality</td><td>Medium</td><td>High</td><td>High</td></tr>
<tr><td>- Liveness</td><td>High</td><td>High</td><td>High</td></tr>
<tr><td>- Safety</td><td>Medium</td><td>High</td><td>High</td></tr>
<tr><td>- Contract execution</td><td>Slow, complex</td><td colspan="2">Fast &amp; less complex</td></tr>
<tr><td>- Privacy</td><td>Public & permissionless</td><td colspan="2">Public & semi-permissionless</td></tr>
</table>

Table 2: Assessment among Ethereum, Tron and BBC based on PREStO.

12. Sarah Allen, Srdjan Capkun, Ittay Eyal, et. al. Design choices for Central Bank Digital Currency: Policy and technical considerations. Global Economy & Development at BROOKINGS (July 2020). is.gd/DO9Oq7
13. S. Leonardos, D. Reijsbergen and G. Piliouras. PREStO: A Systematic Framework for Blockchain Consensus Protocols. IEEE Transactions on Engineering Management, pp. 1028-1044, vol. 67, no. 4 (Nov. 2020). doi: 10.1109/TEM.2020.2981286.
14. Tendermint Core. https://github.com/tendermint/tendermint
15. The Algorand Consensus Protocol. bit.ly/3nZGuDP
16. The Binance Chain Blockchain. https://docs.binance.org/blockchain.html
17. The Tangle. t.ly/sT6T
18. Thuat Do, Thao Nguyen and Hung Pham. Delegated Proof of Reputation: a Novel Blockchain Consensus. IECC'19 Proceedings of the 2019 International Electronics Communication Conference, pp. 90-98, Japan. bit.ly/2KQ72IM
19. P. Boring and M. Kaufman. Blockchain: The breakthrough technology of the decade and how China is leading the way – an industry white paper. Chamber of Digital Commerce and Marc Kaufman, Partner, Rimon Law (Feb. 2020). bit.ly/3rsgPFJ

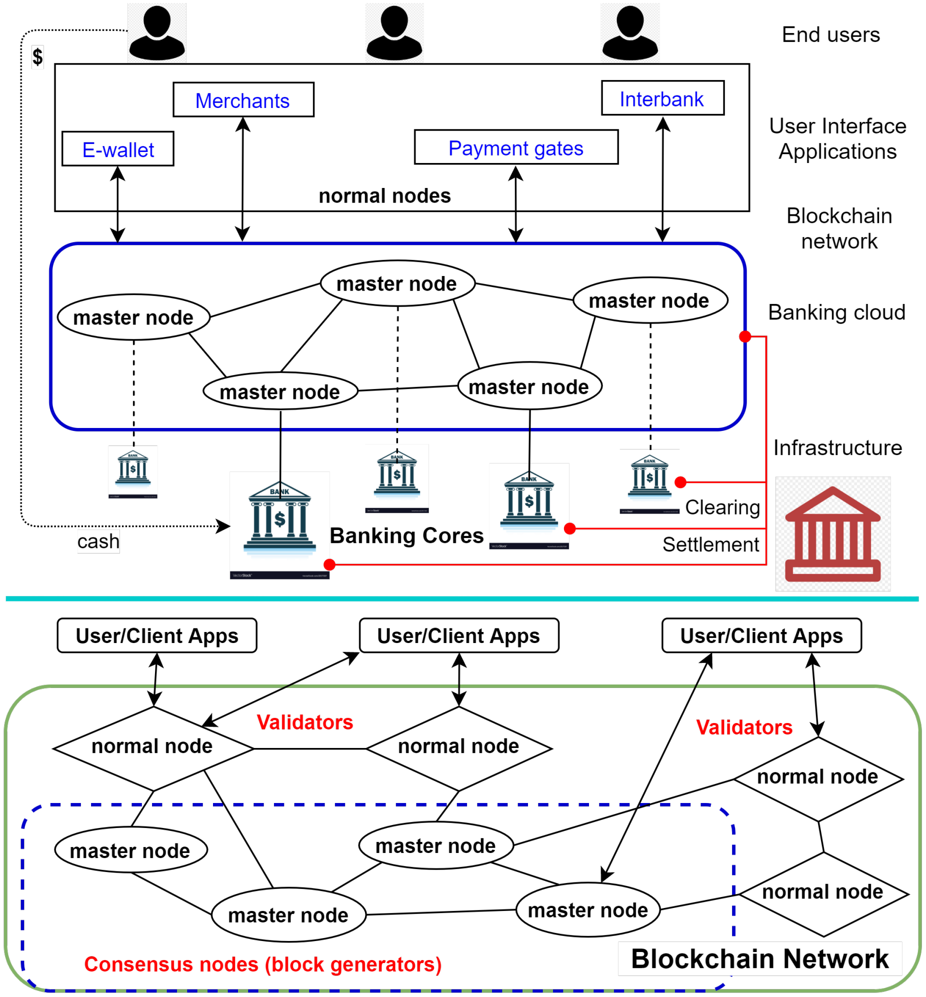

Fig. 1: Sketching the Blockchain banking cloud: block generators and transaction validators.

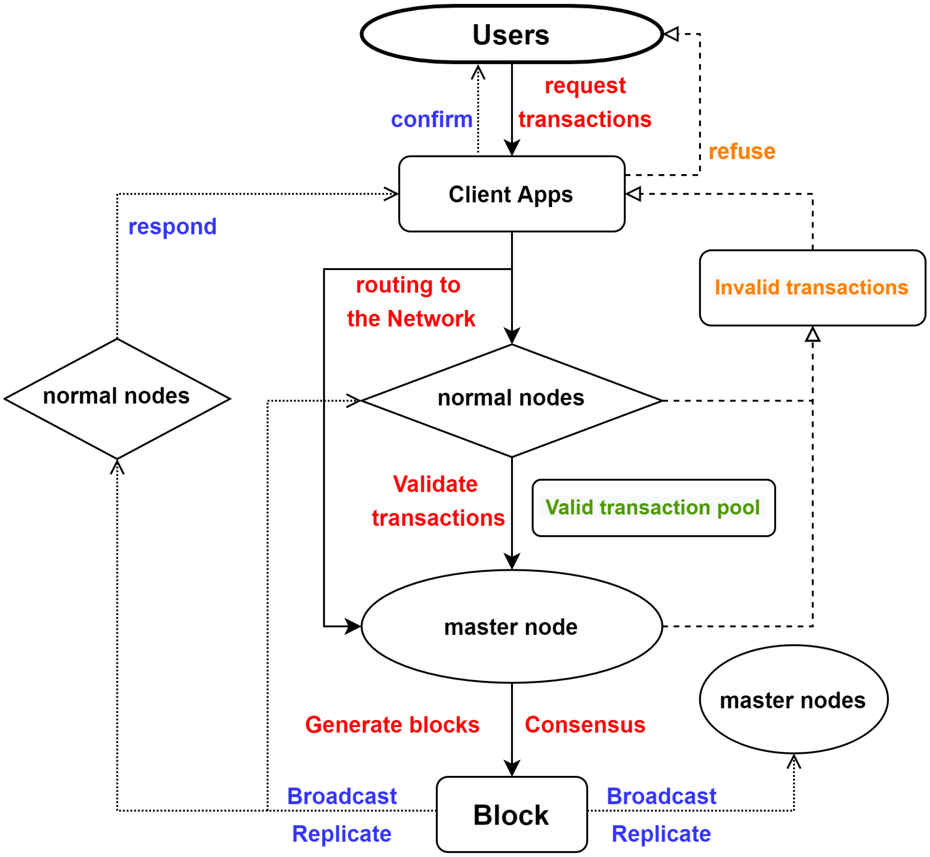

Fig. 2: A basic workflow.

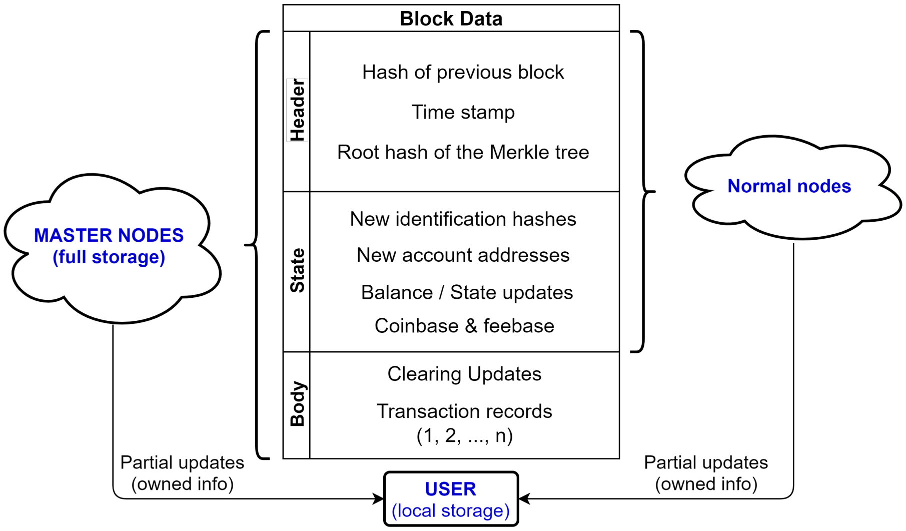

Fig. 3: Block data is distributed differently among participants.

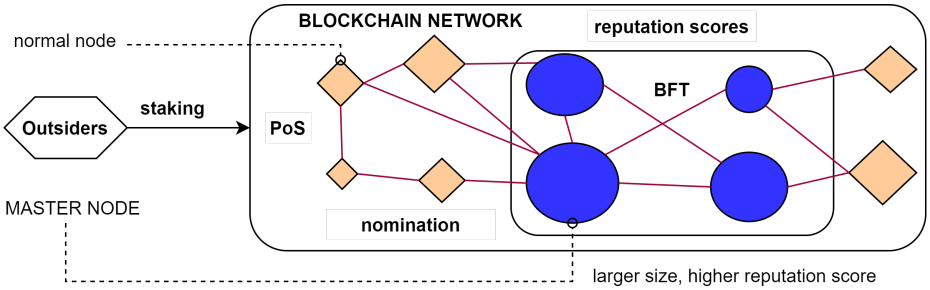

Fig. 4: Governance and consensus.

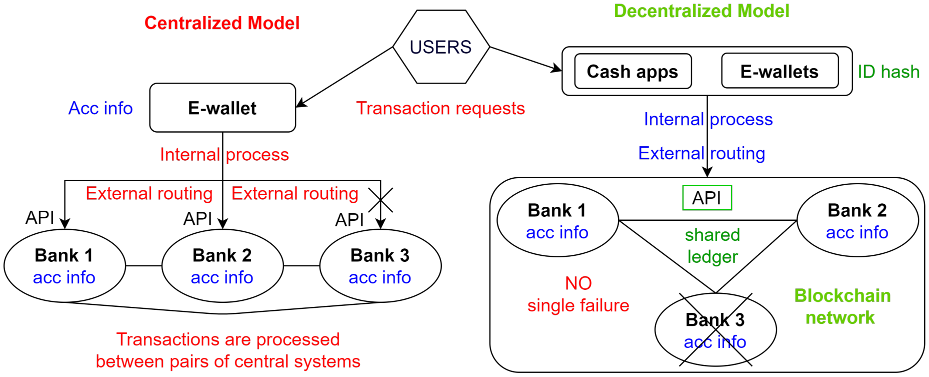

Fig. 5: Centralized vs decentralized payment applications.