X.Blockchain

Yongseok Kwon

2017-05-23 Rev 1.

Abstract

The emergence of Bitcoin and the rapid growth of the transactions predicated on it proved the fact that the blockchain technology is safe enough to be trusted for implementation of the transaction ledger.
The reason why the blockchain technology draws the attention is because it eliminated the trusted third-party (TTP) institutions in the assurance of credibility apart from the existing methods and because it made the arbitrary manipulation of the transaction details substantially impossible by having all transaction details stored in a distributed way at the systems of all participants of the network.
The most critical core concepts with the blockchain technology are the concepts of 'Decentralization' and 'Distributed Ledger.' Based on the existing methods, all transactions were recorded at a single centralized server at the center and the credibility of the transactions was certified by the central server (trusted third-party institution). However, the transactions recognized within the blockchains are 'verified' and 'agreed' after being transmitted to all participants of the network and linked in a sequential (linear) pattern after being consolidated by the unit of blocks.

The size of blockchains in which the details of all transactions are recorded is bound to grow gradually as the cumulative number of transactions grows, i.e., as the time elapses, and this means there will be the point in time some day when it is substantially impossible for all participants in the network to store and manage the whole blockchains. That is, the systems (nodes) with the capacity capable of the storage and administration of the whole blockchains will progressively diminish in their number with a high possibility to form a relatively small group of nodes over time. And this will bring about the centralization in another form. Under the circumstances whereby the whole blockchains are managed by a relatively small group of nodes, the credibility of transactions can't help but rely on the small group of nodes. That is, this means that the 'decentralization' as the fundamental concept of the blockchains can be compromised significantly.

Particularly with respect to the application of blockchain technology for protection of electronic documents, this document aims to seek the remedy for the size problem of the whole blockchains and the centralization problem of nodes thereof by proposing the X.Blockchain as a transformation to the multidimensional structure from the existing linear structure in terms of the linkage structure of the blockchains.

Problems

The size of blockchains is bound to grow continuously in proportion to the cumulative number of transactions as time passes. When we faithfully stick to the fundament concept of the blockchains in which the ledger is stored and administrated in a decentralized pattern by all nodes participating in the network of blockchains and, based on this, the credibility of transactions can be assured without the trusted third-party institutions, the problem of the continuously growing size of the blockchains will inevitably cause the limitations eventually with respect to the participation of nodes. That is, in order to participate as a full node[1] to store and administrate the huge blockchains, a certain minimum level of capacity is required such as the storage spaces. This level of required capacity will keep increasing in proportion to the size of the blockchains thereby leading to the decrease in the number of nodes eligible for participation and this will again cause the 'centralization' problem in another form[2]. As of May 2017, the size of the whole blockchain containing the transaction data of Bitcoins has already exceeded 115 G[3] and the blockchain of Ethereum has recently exceeded the size of 20G too.

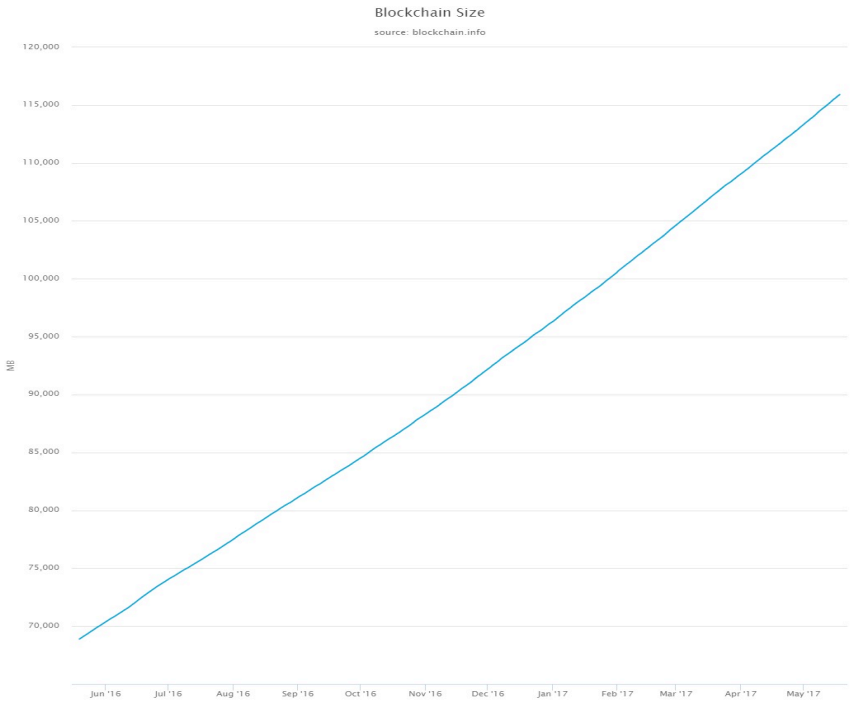

Figure 1. Bitcoin's full blockchain size

[1] The full node means the node to mine the new blocks after storing the whole blockchain.

[2] As a solution to this problem, the Bitcoin side proposes SPV. This is a method to minimize the resources required by conducting the authentication of transactions only with the information at the block headers excluding the transaction data and is indispensable in the application of blockchains for electronic documents. If it is the transaction details that compose the transactions as it relates to the cryptocurrency, the electronic document data comprises the major part of transactions in the electronic document applications. At this time, the size of document is large enough to render the comparison with the transaction details of the cryptocurrency meaningless and therefore the blockchains do not contain the document data itself.
Unless otherwise noted in this document specifically, the 'size of blockchain' refers to the 'size of the blockchain header.'

[3] Size of the whole blockchain including all of the transaction data describing the transactions and the block header information.

In addition, with respect to Bitcoin, the current number of full nodes existing across the whole world is estimated at around 5,000 ~ 7,000.
On the other hand, the numerous user clients (including the mobile devices) failing to meet a certain threshold level in their capacity will be restricted in their participation as a full node. For this reason, the user clients are unable to carry out the confirmation of the credibility of transactions on their own (without the trusted third-party institutions) but have to raise the request to the relatively smaller group of nodes and are expected to accept the result presented unilaterally. Here, the small group of full nodes acts like the 'trusted third-party institutions.'

This problem of the 'centralization of full nodes' is caused by the high capacity of computing power required at the time of the storage of the whole blockchain which became quite huge as mentioned previously and the creation (mining) of blocks. And the reason why the storage of the whole blockchain is required here is because it is meaningless to selectively pick up only the blocks needed indeed since the blockchain is implemented in the linear linkage structure. The group of blocks with the linkage information lost between each pair of the sequential blocks here and there cannot be used for confirmation of credibility by any means and, above all, it does not have any value in itself.

In a sense, this problem is unavoidable as it comes to the 'transactions' involving the cryptocurrency. Any type of restrictions or categorization cannot be allowed in the recording of the transfer of a certain amount of currency from a certain account to another. It is impossible to categorize the transactions on the basis of the 'amount' of currency or the 'account' used for transfer of the currency. Since every transaction has the same implications and it is impossible to categorize the transactions of the same implications no matter what kind of criteria may be applied, it seems unattainable in a practical sense to deviate from the linear structure in dealing with the records of this nature.

However, on the other hand, in the case of the 'electronic documents,' a diversity of records related to the document are taken care of with the focus laid on the document itself apart from the case with the cryptocurrency. The creation, modification, transmission, reference, disposal and all other records relate to the corresponding document.
This means that the document itself and the records related to it can be categorized on the basis of the 'document', which further means that the chains in a blockchain can be organized into a multitude of chains rather than a single linear structure.

N-Dimensional Blockchain – X.Blockchain

In reflection of the characteristics of the electronic documents as mentioned previously, X.Blockchain categorizes all of the records (transactions) related to a document based on the document itself or the other 'criteria' equivalent to it rather than connecting them with each other in a single linear structure. And by organizing multiple chains in accordance with the same criteria, it proposes the blockchain of the multidimensional type.
For instance, when the 'document' is used as the criteria, the 'first creation' of each document is recorded in the same blockchain (main-chain) of the linear structure as the existing blockchains. However, the additional records (transactions) such as those for the modifications and others made in relation to the specific documents which were already recorded in the main-chain are recorded in a sub-chain as another chain created on the basis of the block within the main-chain as the genesis block[4] rather than the main-chain.

[4] The first block in the blockchain

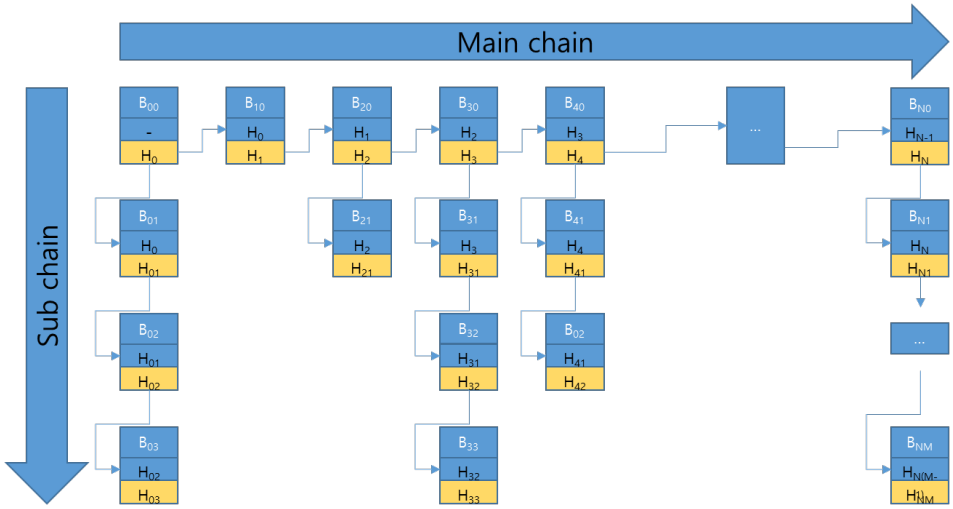

Figure 2. X.Blockchain

The above figure depicts the X.Blockchain of 2-dimensional structure. Assuming the main-chain is based on the 'document' as mentioned previously, each of the blocks (B_{00} ~ B_{n0}) comprising the main-chain includes the records about the creation of new documents and at the same time each of them can serve as the genesis block for the sub-chains. For instance, if there occurred the first modification to the electronic document E_{20} of which the creation was recorded in B_{20}, it will be recorded in B_{21} in the sub-chain which was created based on B_{20} as the genesis block rather than B_{30} which is the next block in the main-chain.

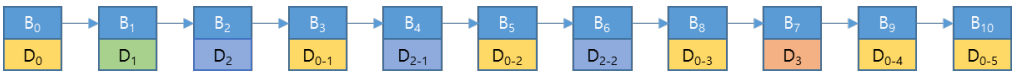

Figure 3. Blockchain of the Linear Type

Within the blockchain structure of the linear type, the additional records for modification and others of a document require the additional blocks though they may be related to the same document.
The above figure is an example where the addition of documents D_0 ~ D_3 to the blockchain was implemented in a linear pattern. In this example, document D_n signifies the creation and D_{n-m} signifies the additional records which were generated in relation to document D_n such as the modification, transmission and others. In the case of document D_0, a total of 6 records (~ D_{0-5}) was generated including the creation and for document D_2 a total of 3 records (~ D_{2-2}) was generated.
In a linear blockchain as above, each client should acquire and store all of the whole blocks in order to verify the credibility of the specific documents on its own. That is, even for a client who only needs the document D_2, a total of 11 blocks is necessary including the blocks D_0, D_1 and D_3 which are not necessary in reality and the blocks D_{0-1} ~ D_{0-5} including the additional records related to D_0.

However, this same scenario can be implemented by using X.Blockchain as follows.

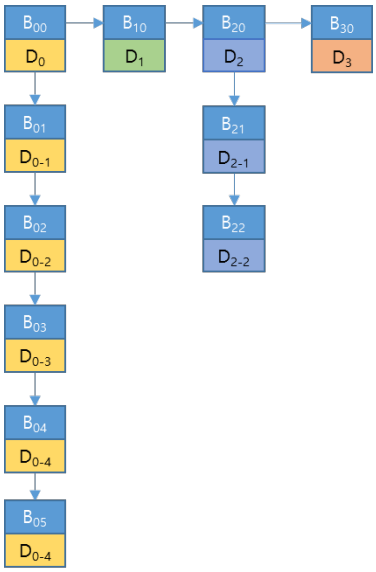

Figure 4. X.Blockchain

In the above figure, B_{00} ~ B_{30} comprise the main-chain and the sub-chains are included which use B_{00} and B_{20} as their genesis block, respectively. In this type of blockchains of the multidimensional structure, all clients don't need to contain the whole blockchain. In case the document D_2 is necessary only as in the above example, the credibility or otherwise of document D_2 can be confirmed on one's own if the sub-chain using D_2 as its genesis block and the main-chain at the next higher level are in possession without the need of the whole blockchain. That is, it does suffice to possess the information about total 6 blocks including the blocks B_{00} ~ B_{30} from the main-chain and the blocks B_{21} ~ B_{22} from the sub-chain.

Here, the 'criteria of categorization' applied to the main-chain don't necessarily be the 'document.' Depending on the implementation of the service, the 'department' units can be used as the criteria or otherwise the group of documents related to each other can serve as the basis of the categorization.
In addition, the sub-chains can also be so implemented as to serve as the main-chain of the other sub-chains. In the case of a cadaster, if the 'region' of a broad coverage is used as the criteria for the main-chain, the units smaller than it such as the city, county or ward are used as the criteria for the first sub-chain and the specific land lots are used as the criteria for the second sub-chain, the blockchain can be implemented in a 3-dimensional structure as in the figure below rather than the 2-dimensional structure shown in the above figure.

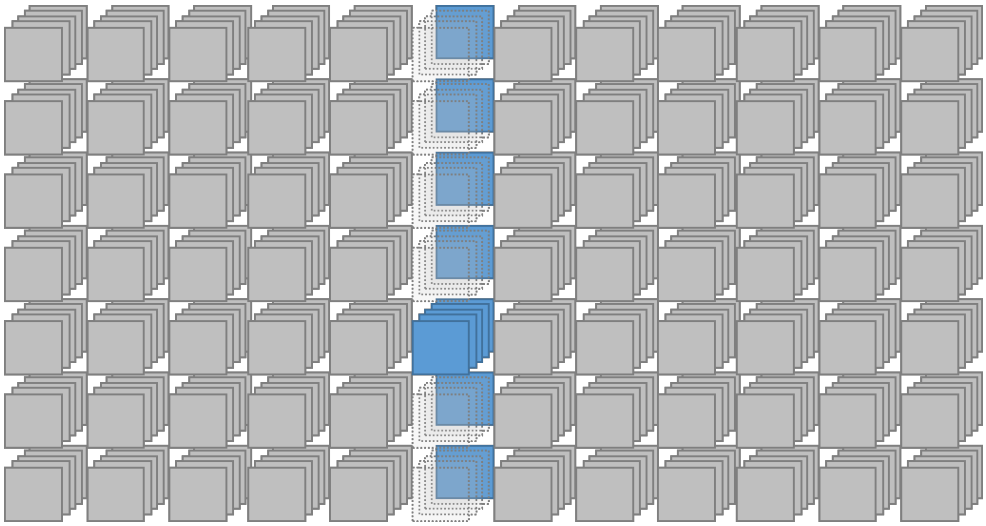

Figure 5. X.Blockchain of 3-dimensional Structure

In the X.Blockchain, the full nodes assuming the responsibility for mining of new blocks should still have the information about all blocks. However, as it comes to the confirmation of the credibility of documents rather than mining, the clients (user devices) don't need to have the information about all blocks. Each user can verify the credibility of the document of interest sufficiently by possessing the sub-chain containing the document which require the verification and the main-chain at its immediate higher level without the trusted third-party institutions. At this time, the full nodes assume only the role for mining but not as the trusted third-party institutions to confirm the credibility or otherwise.

Parallel Transaction Processing

With the blockchains of the linear structure, all of the transactions (Transaction) generated while the creation of a block is under way are placed in the waiting condition until the mining of blocks commences the next time. Moreover, in view of the condition that the size[5] of individual blocks is not allowed to grow indefinitely, it is sufficiently conceivable that the transactions in the waiting condition may have to wait till the mining of blocks after the next time but not till the next time. The waiting time until the transaction disseminated across the blockchain network is confirmed after being included in a block reduces the 'number of transactions processed per second (TPS[6])' leading to the delay in the processing of transactions accordingly.
However, with X.Blockchain, the concurrent progress of the mining of blocks is possible for each sub-chain. For instance, the mining of B_{n0} in the main-chain and the mining of B_{2m} in the sub-chain can be progressed simultaneously. That's because B_{n0} and B_{2m} do not have mutual linkage relationship since they belong to different blockchains independent from each other.

[5] The size of a block is limited to 1MB with Bitcoin. The limitation on the size of blocks causes the number of transactions which can be included in a block to be restricted leading to the decrease in the number of transactions (Transaction per Second – TPS) which can be processed per unit of time. At present, the discussions for expansion of the block size of Bitcoin are under way and the block size of 2MB is used in some implementations like the Bitcoin Classic but this is not widely accepted by the miners.

[6] At present, Bitcoin records around 7 TPS.

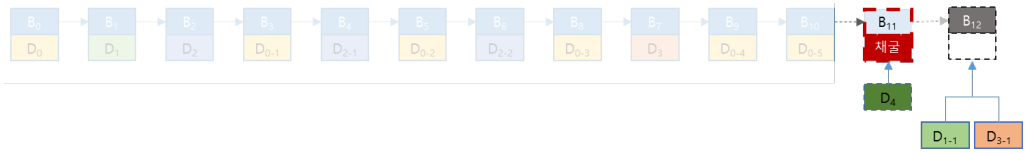

Figure 6. Transaction Processing – Blockchain of Linear Structure

The above figure assumes that the modifications were made to documents D_1 and D_3 after D_4 was newly created based on the same scenario presented previously. With the blockchain of the linear type, the records of the modifications to D_1 and D_3 are held in the waiting condition while the mining is under progress for the new creation of D_4. After completion of mining for creation of D_4 in block B_{11}, when the mining is started for the next block B_{12}, the records of the modifications to D_1 and D_3 are included in B_{12} and recorded to the blockchain at last when B_{12} is finally connected to the blockchain after completion of mining.

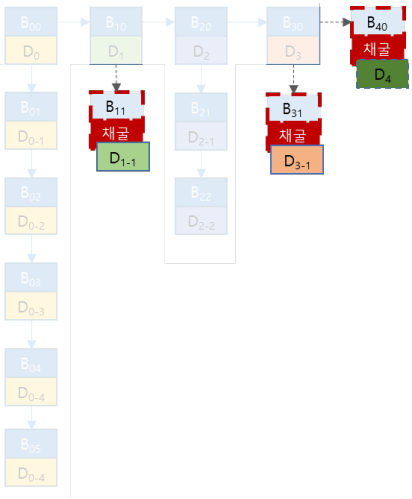

Figure 7. Transaction Processing – X.Blockchain

However, with X.Blockchain of the multidimensional structure, as can be seen in the above figure, the mining of the blocks B_{11} and B_{13} in regard of the modification details to documents D_1 and D_3 doesn't need to be kept waiting until the mining is completed for block B_{40} for creation of document D_4. In the example presented, the mining for all new blocks B_{40}, B_{11} and B_{31} can be progressed at the same time independently from each other.

Effectiveness

The situation is assumed where the certificate of individual resident registration is converted into the electronic document and administrated by using the blockchain technology in order to explain the differences between the application of X.Blockchain and the application of the existing blockchain.

It is further assumed that there exists one certificate of individual resident registration for each person of the population, which comprises 1 block, and that the certificate of individual resident registration is

renewed for each of the persons who migrate to a different location to change their address each year with the information about the renewal recorded in a separate block.

[Unit: Thousand Persons, %, Thousand Cases], Source: Korean Statistical Information Service 「Domestic Population Migration Statistics」

		2016
Total Migration	**Number of Migrating Persons**	7,378
	Ratio of Migration (%)	14.4
	Number of Immigration Cases Reported	4,636
	Gender Ratio of Migrating Persons (Female=100)	103.9
Net Migrating Persons in Each Region	**Capital Region**	-1
	Central Region	41
	Honam Region	-16
	Yeongnam Region	-40

According to the National Statistics Portal (http://kosis.kr), the total population in the Republic of Korea was 51,525,338 persons as of the end of 2015. As it is assumed that there is a copy of the certificate of individual resident registration for each person of the population and the certificate is renewed whenever the migration occurs, it can be estimated that there would have been total 7,378,000 cases[7] of renewal to the certificate of individual resident registration during the whole year of 2016 according to the data in the above table.

If this is implemented by the blockchain of the linear type, the initial blockchain will be composed of the same number of blocks as the total population and the same number of blocks should be added each year as the number of persons who migrated. If the blockchain was applied from 2016, the number of blocks within the blockchain would be as follows as at the end of 2016.

51,525,338 (Number of Initial Blocks) + 7,378,000 (Number of Blocks Changed in 2016) = 58,903,338

And if we assume that 7,000,000 persons migrate on average each year, 7 million blocks will be added each year. If we further assume that the size of each block is 80 bytes[8], the size of the whole blockchain after the records accumulated for 10 years can be calculated as follows.

[7] According to the data published through the National Statistics Portal, the accurate number of persons who migrated in 2016 is 7,378,383.
[8] The size of Bitcoin block headers is 81 bytes.

$$Size\ of\ Blockchain = (51{,}525{,}338 + 7{,}000{,}000 * 10) * 80 / 1024^3 = 9.1\ G$$

That is, in the case of blockchains of the linear structure, the size of blockchain with the records accumulated for 10 years is 9.1G and this will grow by 0.52G each year in a linear pattern for the modifications made each year for migration.

If X.Blockchain is applied to the same scenario, though the number and size of total blocks are the same, the blocks added each year for modification will be organized into the sub-chains but not linked to the main-chain in a linear pattern. That is, the 70,000,000 blocks for the modifications for 10 years will be dispersed and organized into the sub-chains underneath the main-chain which is composed of 51,525,338 blocks. If the level of dispersion of the modification blocks to the sub-chains under the main-chain is evaluated based on simple arithmetic average, there will be 1 sub-chain for each block contained in the main-chain and each sub-chain will have 1.35[9] blocks. Based on this, the size of blockchain per person of population can be calculated as follows.

$$Average\ size\ of\ a\ sub\text{-}chain = (7{,}000{,}000 * 10 / 51{,}525{,}338) * 80 = 108.68\ B$$

$$Size\ of\ main\text{-}chain = 51{,}525{,}338 * 80 / 1024^3 = 3.83\ G$$

Apart from the blockchain of the linear structure, X.Blockchain makes it possible to selectively administrate the necessary data. This means that the service is possible for specific 1 million persons of population for administration of the certificate of individual resident registration and others for whatever reasons. In this case, the total storage space necessary for verification of the modification history to the certificates of individual resident registration for 10 years for 1 million persons can be calculated as follows.

$$3.83 + 108.68 * 1{,}000{,}000 / 1024^3 = 3.93\ G$$

In the future, the size of blockchain will be increased only as much as the size of the annual average modification blocks for 1 million persons each year.
The scenario in this chapter did not take into account the increase of the main-chain caused by new birth and the increase of the sub-chains[10] caused by death, marriage and divorce in its assumption. For this reason, a larger size will be required for all the blocks in reality. Moreover, the criteria of categorization will not necessarily be 1 person of population for the main-chain and 1 block may not necessarily include only one document (Transaction). For these reasons, the values calculated above are meaningful only for the relative comparison between the blockchain of the linear structure and the X.Blockchain of the multidimensional structure rather than for the real world interpretation.

However, whereas the above example included only 1 type of document, the certificate of individual resident registration, the same scenario may be applicable to a diversity of public documents at the same time in reality. As more of different types of documents are added, the relative advantage of the

[9] This corresponds to the average number of migration for 1 person of population for 10 years.
[10] As the increase portion to the sub-chains becomes larger, the efficiency of the X.Blockchain of the multidimensional structure will be the higher.

multidimensional blockchains in terms of efficiency will grow rapidly over the linear blockchains. In the example above, if another certification document from the other public institution is added with the assumption that the transactions like the modification history and others are generated at a rate similar to that of the certificate of individual resident registration, about 2 times of the blocks are needed in addition when 1 type of new document is added in the case of the linear blockchain. And if another type of document is added, the number of blocks will be increased in the same way.
However, in the case of X.Blockchain, the size of main-chain does not change and the blocks added due to the addition of a new document type will be added only to the sub-chains to give rise to even greater advantage in favor of the multidimensional X.Blockchain in terms of efficiency.

Conclusion

As mentioned, the size of the whole blockchains does not make any difference. The major distinction of the multi-dimensional X.Blockchain is that it enables the selective administration of the data (blocks) based on specific criteria. And it serves the useful purpose to allow the confirmation of the credibility of documents on one's own without the intervention of the trusted third-party institutions within the relevant scope as the user clients can selectively store and administrate the blockchains in their systems within the necessary scope.