Democratic Centralism: a hybrid Blockchain architecture and its applications in Energy Internet

Li Jun Wu[1], Kun Meng[1,2], Shuo Xu[1], Shu Qin Li[1,2],Meng Ding[1,2],Yan Feng Suo[3,4]
1.School of Computer, Beijing Information Science and Technology University,Beijing,China
2.Joint Lab of Sensing and Computational Intelligence, Beijing Information Science and Technology University, Beijing,China
3.School of Computer and Communication Engineering,University of Science and Technology Beijing,Beijing,100083
4.National Research Center for Information Technology Security, Beijing, 100084
1.wlj615965477@163.com, 2.mengkurt@bistu.edu.cn

***Abstract*—Blockchain is attracting more and more attentions from many kinds of fields, such as finance, industry, and theory researchers. Rather than viewing blockchain as a novel technology, we should think it as an innovation for managing digital society, which provides fundamental principles to support democratically distributed applications. Based on the design and application of the Energy Internet, this paper analyzes the core architecture of the initial blockchain technology, and combines the security of the public chain with the efficiency of the private chain,solving the poor efficiency problem of the initial blockchain by using the high efficiency of private chain.At the same time, it inherits the security and non-tampering of initial blockchain.This paper designs a new hybrid blockchain storaging mode that is Block Static Storage(BSS,internal structure is N+X hybrid blockchain,following can be referred to as N+X HBC),for purpose that improving the overall efficiency of the Internet running, achieving decentralized supervision, and provoding a credible, safe and efficient performance of the Energy Internet in the storage of its massive data, as well as a huge business system.**

Keywords—energy internet; hybrid blockchain; decentralized data storage

I. INTRODUCTION

The goal of Energy Internet is to provide a strong backbone transmission network, improve the level of intelligence. Energy Internet is transferring a centralized, one-way, producer controlled energy system into a large number of distributed, two-way energy supply model, and meeting the interact between producers and consumers in the Energy Network[1].The massive users, data of power consumption and massive electrical equipment is the biggest characteristic of energy, so the biggest challenge the Internet facing today is to reform the architecture of the Energy Internet, to achieve the on-demand and two-way transmission and real-time dynamic balance, to maximize the proportion of clean energy accessing[2].

The TransActive Grid project in New York, USA, is jointly developed by LO3,a developer of micro grid and ConsenSys,blockchain technology developers.The project is connecting the solar power generation family to the electricity purchase family through the blockchain network, can manage the record transaction without the participation of the personnel, and can represent the future community to manage the energy system[3].In this paper, we design a new hybrid blockchain storage system based on the Energy Internet,which can meet the requirements,which are security and efficient storage.

Bitcoin is considered as the first complete decentralized electronic cash and blockchain is one of its most critical support techniques. The provision of blockchain guaranteed that all data wrote in blocks could not be changed practically. In fact, the data in blocks has been encrypted and approved by distributed anonymity participators through Internet.The ledeger of blockchain is allowed to be downloaded and stored by all nodes whatever they download and store.

In[4], authors consider the backdrop of complete decentralized blockchain based cryptocurrencies, such as Bitcoin, and present a hierarchy cryptocurrencies framework that decouples the generation of the monetary supply from the maintenance of the transaction ledger.

N+X hybrid blockchain storage strcture in this paper is composed of manager block(private nodes) and storage block(public nodes). Essentially,manager block is a public network agency with high credibility, responsible for massive business processing and achieving mutual supervision mechanism.Being similar to the responsibility of each block in the original block chain,manager block broadcast the data information for each transaction, and will verify the accuracy of each data before broadcasting.After the first verification, it is the time for other random, distributed storage block to verify the integrity of the stored data, whether data is “double spending” invalid data.The second verification is done, all storage blocks update new trading data synchronously.Being similar to the management of initial blockchain, all of storage blocks records of the same ledeger.Through applying the hybrid blockchain in the Energy Internet,it achieves the intelligent, efficient and safe operation and management mechanism of Energy Internet.This paper first discusses the general core technology of initial block, and puts forward the characteristics and requirements which must be included in storage system, then according to requirements of the storage system,this paper introduces the various parts of the structure design of N+X hybrid blockchain storage architecture,based on the background of applications in Energy Internet.

978-1-5090-5759-7/17 $31.00 © 2017 IEEE
DOI 10.1109/ICEI.2017.38

II. CRITICAL COMPONENTS OF BLOCKCHAIN

A. *Independent participators*

The nodes involved in the blockchain are random and non counting.Initial blockchain assumes that any participator may create and verify transactions and blocks, any legal blocks have to been successfully verified by majority of participators, and any minor modification for existed block must be agreed with by all participators who store blockchain copy, but no one completely knows who has copies[5]. Hence, for practice, it is almost impossible to modify any existed blocks.

B. *Dependence of blocks*

Blockchain is based on block as a basic unit, which is formed into a chain by means of a directed relation, and has no boundary.Bitcoin as an example,which is shown in Figure 1,block is constantly based on the latest block,calculating the random values consistently until the hash meet requirements, becoming a valid block.By steps of blockchain formation,new transaction requirements broadcast to all nodes,each node collects the new transaction in a block,each node began to generate random strings, random answers,when a node find the answer matching the random number(provided by lattest block) , then broadcast the generated block to all nodes;all nodes verify the transaction, when the information contained in the new block is valid, all nodes accept theis new block.

As for the transactions in the blockchain,blockchain ensure the security and accurity of transactions. Blockchain provides an unchangeable distributed database with strong security measures. However, the efficiency of initial blockchain technology is the most critical challenge, for Bitcoin every block(contains mainly exchange transactions which has several bits) equally is verified successfully in ten minutes, which hinders it to be used broadly in many systems.The speed of private chain transaction can be faster than any other block chain, this is because a small amount of nodes still has a high degree of trust, does not require each node to validate a transaction[6].

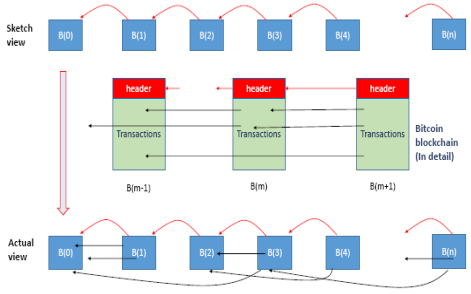


Figure 1. Bitcoin Blockchain

- Security

Once the data is realeased,there will be incountable loss for users.The Energy Internet is composed of amount of electric devices and electric inistitution.Releasing information is the catastrophic disaster.The data storaging system serving for power grid must make sure the security of information including users' home adress and privacy information.

- Intelligence

At the same time when more and more technologies supporting intelligence appear,the Energy Internet should take advantages of these advanced techniques including blockchain.Beacause of the decentralization data storage,the masses tend gradually to trust decentralized supervising.The decentralized storage reduces fussy procedure for Energy Internet.The method of public supervising make sure the trading running validly and efficiently without artificial participate.

C. *Examples*

- Sia

Sia is the product of Nebulous Incorporated.Sia is a platform for decentral cloud storage,realizing the renting between all of the participants in the Sia[8].If transactions occur, must be accompanied by the formation of cryptographic protocols, Sia is responsible for storaging protocol of every single transaction, Sia platform itself does not to be used for storaging, these protocols are stored in the blockchain and can be public auditeyed. Protocals include that clients inform of what data to be storaged, reward methods reached between the two sides in the form, the host needs regularly prove to customers to inform files are stored safely, and there is punishment mechanism corresponding for any missing file.

- P2P File System-IPFS

Juan Benet designed the IPFS, InterPlanetary File System (IPFS) is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files[9].IPFS is based on distributed version control system Git, using the same content addressing mode, can switch service version according to the different service demands. At the same time,IPFS coordinates and maintains the metadata with different forms of distributed hash table.IPFS takes advantages of BitTorrent to exchange file data, rewarding for the users who sharing source,and those who do not share resources will receive the appropriate punishment.

- BigchainDB

McConaghy proposed an extensible blockchain database–BigchainDB[10].It points to performance of 1 million writes per second throughput, storing petabytes of data,and sub-second latency.The design of BigchainDB starts with a distributed database(DB), and through a set of innovations adds blockchain characteristics,for example,decentralized control, immutability, and creation & movement of digital assets.

Obviously, replacing centralized storage with new architectures is mean method.This paper posed a hybrid blockchain for improving the efficiency of trading and data-storaging and ensuring the security at the same time.

III. N+X HYBRID BLOCKCHAIN

This paper present a hybrid blockchain mechanism composed of private blockchain and public blockchain.The private blockchain is designed for verifying the accuracy of the transactions related to the grid,while the public blockchain

serves for identifying the integrity of data.The reason why this mechanism is called N+X is there exist N private nodes and X public nodes generated by PCs from anwhere and anytime.The application of private blockchain makes the attribute for improving the efficiency of storaging data.This section will introduce the design of N+X,the incentive ways for attracting more participants.The structure of N+X hybrid blockchain is shown in Figure 2.

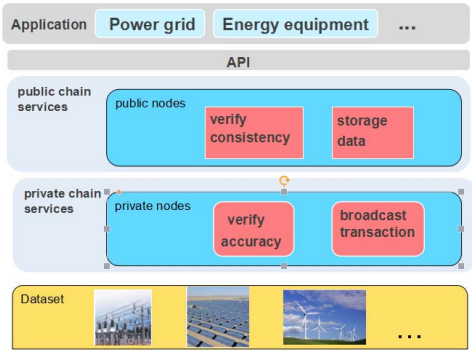


Figure 2. Structure of N+X Hybrid Blockchain

A. The design of Block Static Storage(BSS)

Private nodes (in essence,they are grid engicies with high authority) can view the data prototype,while,random public nodes are only used to verify the integrity of data and ensure transaction integrity, and can only see the encrypted hash value of data,rather than the data.

The data stored in the Block Static Storage (BSS,internal structure is N+X hybrid blockchain) can no longer be deleted and modified, which can only be added and updated.In the overall structure of the N+X hybrid blockchain, all block were divided into manager block and storage block,manager block is responsible for verifing the accuracy of the data in the business and storaging the index for querying data.The construct in this paper is designed at the background of Energy Internet, manager blocks are consist of grid institutions with high trust in the nationwide.The differences between manager blocks and blocks of initial blockchain include that mining is not involved in N+X, manager blocks are only responsible for externally broadcasting the new data(only to all public nodes), verifing the legitimacy,and storaging the indexes of data for later querying.Storage block and manager block are independent of each other, and storage blocks are a distributed cluster to verify the consistency of the data.Users query data record in the manager block according to the feedback data (data hash), with the hash computed in the storage block to find the data.But for the protection of user privacy information,for registered users (public blocks),users can not see the original data in the display interface, the original data has been added a layer of protection, the original data is hidden in the memory, can only be read by the BSS system, public nodes can only see the data encrypted hash value.It is also very good protection to all electricity users data privacy.

Because this article is based on the design in grid system of Energy Internet,so storage blocks is generated by a large number of distributed PCs' registerring.Each computer registered in the BSS system is a recognized and orderly pubic nodes (forks may be appear),so public nodes is random, large amount and public.In the operating mechanism of BSS,data integrity verification is completed only by random public nodes, but public nodes does not focus on the accuracy of the data to be stored,and all public nodes take participate in the synchronous recording.

- manager block

Manager blocks is essentially national grid institutions with high credibility, namely the N in the N+X hybrid blockchain, numbers of known peer manager blocks monitor and supervise each other to ensure the Energy Internet open, transparent and notarization.Manager blocks firstly broadcast new transaction data to other manager blocks,all manager blocks receives a new transaction data to verify the accuracy of the this new data in Energy Internet transactions according to the principle of grid transaction, after these manager blocks confirm the result,the manager block that broadcasted data receives the feedback results, if all agreed,BSS storage system will randomly select over 2/3 public nodes in all distributed public nodes, these selected public nodes will be in charge of verifing the consistency (data integrity) of data.The process of transactions in BSS is shown in Figure 3. In order to improve the intelligent services of Energy Internet , specifically for each of the data index oriented, convenient for users to query their trading data at any time.The storage structure of manager block includes,the previous manager block ID (at this time the manager blocks constitute the ring chain),current manager block ID,the Merkle HASH1 of all transaction data in BSS(to ensure the data can not be tampered, for the integrity of the public nods checksum, will be sent to the public block together with the original data,so it has been dynamically updated),Index record (in essence, the Hash value of each new data, the user will receive the data after storing the index, convenient for data-querring corresponding public nodes). As shown in Figure 4(a) .

Figure 3. Transactions in BSS

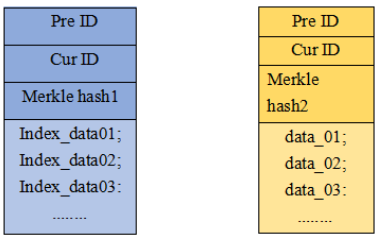
- storage block

Storage block focus on checking whether the data is tamperied (data consistency) and data storage, it is generated by a registration of users in BSS.Once one user registers suuccessfully,this PC becomes a recognized public nodes accepted by national BSS,namely the X in N+X hybrid blockchain.For example, in a city, the grid operation system of this city is based on BSS storage architecture, if a family

registered with the BSS,becoming the legal public node of entire national BSS, and enjoying the rights that supervision the consistency of data.Incentives of N+X hybrid blockchain(later introduced) will attract more PCs, so the shorty of data storage room is easily solved.Because storage blocks is directly involved in the storage of data and ensuring that the data is not tampered.When a public node is selected randomly to verify the consistency of the data, firsly public node receives the data logging request,then it will calculate the Merkle Hash1 of data sent by private nodes(manager block), then calculate the Merkle Hash2 of data stored in public nodes plussing new data.Both of HASH are compared, if the two hash values are equal,it implies the data has not been tampered.Storage block cludes,the previous block (storage block) ID,current manager block ID,the Merkle hash2(it is synchronized with all transaction data of BSS, is also dynamically updated, and the accuracy is verified by comparing it with Merkle hASH1 in Figure 4(a)),the raw data stored in the storage domain(when the user queries the data to calculate the hash, according to the Index_data in Figure 4(a) to search data). As shown in Figure 4(b) .

B. Incentive mechanisms

In order to expand the BSS storage system, attract more and more grid users to participate in the distributed storage structure, and improve the storage capacity and reliability of BSS,storage block will be rewarded.As many of the distributed storage system, the economic feedback attracts users to participate in distributed storage system.For example, Sia[2] adopts interest driven reward mechanism,bilateral clients(storage provider and storage applicant) reach an agreement before the trade is built,including economic transactions in the process of trade, in the supervision of network consensus, storage providers and storage applicant to follow the original agreement.N+X hybrid blockchain storage only draws lessons from the economic feedback mode of Sia.If a PC becomes a member of BSS, verifying and recording will receive a special economic or material feedback as BSS's membership.At the same time, according to the user's performance in the system,BSS will cumulate or revoke credit score to boycott the dishonest users in the energy Internet.Under such economic incentives, BSS will attract more and more PC machines involved in the N+X hybrid storage blockchain, while creating a credible, healthy Energy Internet environment.



(a) (b)

Figure 4. (a)Structure of Manager Block, (b)Structure of Storage Block

IV. APPLICATION SCENARIOS IN ENERGY INTERNET

When this kind of storage structure is applied in the Energy Internet,the efficient and the expence of transaction will be improved.Energy Internet is designed to provide users with a more intelligent, safe regulatory environment. The application of BSS storage system in Energy Internet is shown in Figure 5. In Figure 5,A,B,and C are power grid institutions which form a distributed and mutual supervision structure.Upper part of chart represents a distributed public nodes net which is responsible for verifying integrity and storaging data. Energy Internet will connect mass distributed devices(distributed generation equipment, energy storage equipment, smart appliances and electric vehicles, etc), large-scale users and the integration of various energy networks[1].So the Energy Internet has a very large scale of equipment operation data, business operation data and the most popular users' privacy data.

Blockchain technology (the core idea) applied to the Energy Internet,it makes the Energy Internet not only has the advantages of intelligence,but also for security,reliability added a protective barrier.Based on technical characteristics of public blockchain and private blockchain, the private blockchain and public blockchain are combined to improve the efficiency of the transaction.Because the private nodes is composed of known power mechanism with high credibility,which is familiar with business related grid,private nodes has the authority to verify the validity of the transaction.So when new data transactions need to be recorded in ledger, all manager blocks must firstly checked the accuracy of the transaction, according to the business principle of grid system,verify the validity and effectiveness of the business data.After the first verification is done,manager blocks inform the storage blocks selected randomly to verify whether the data has been tampered. Through checked two times, data can be updated to ledgers of all storage blocks in BSS system.

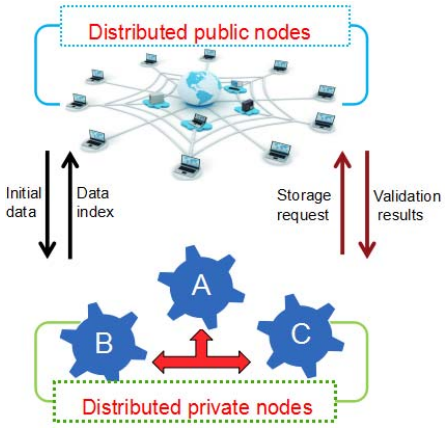


Figure 5. N+X Hybrid Blockchain Applicated in Energy Internet

V. EXPERIMENT AND ANALYSIS

In this paper, on the basis of existing research results, 4 servers were used to build the private chain, and an existing public chain joinning together to form an experimental environment.The generation of batch data is used to simulate grid's transactions in BSS storage system, then statistical analysis was performed according to the transaction efficiency.

As shown in Figure 6, it describes the implementation process of a transaction in the N+X hybrid blockchain architecture. First of all, according to the requirements of the N+X hybrid blockchain,the specific consensus mechanism is modified in the project. Then, through the deployment of the files nodes(ledgers) and other content in the 4 server, the private chain connected in P2P network (public chain) is built. Finally,when data is requested to storaged, four private nodes verify the accuracy of transaction synchronously.After the transaction is verified by private nodes and public nodes successful, the data was successfully stored in the public chain, and the following information is returned, such as the hash of data,the time when transaction occured, confirmation number and so on.According to the above description,the transaction related to the grid is simulated by simple data storage.

Figure 6. Implementation Process of Transactions

At the same time, the production of records is observated and analysed according to the time dimension. As shown in Figure 7, the abscissa represents the production of a block in a public chain (the new transaction data is legally recorded), and the ordinate represents the processing time of the transaction. In the N+X hybrid blockchain architecture, although the numerical fluctuation is influenced by factors such as network delay, the block generation rate maintained only at more than ten seconds,and efficiency have been greatly improved compared with the Ethereum project, so the efficiency of the Energy Internet can be effectively improved by N+X hybrid blockchain storage mechanism.

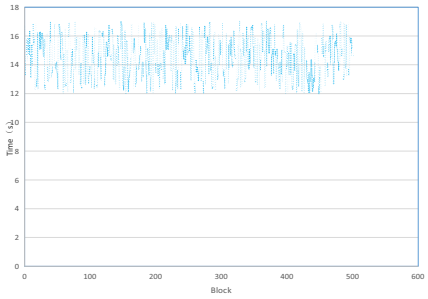


Figure 7. Speed of Transaction Generation

VI. CONCLUSION

Through the hybrid blockchain composed of privade blocks and public blocks applied in the Energy Internet,the high efficiency of private blockchain is applied in Energy Internet,and the security of public blockchain is also applied in Energy Internet.Through the observation and analysis of the above simulation experiment, the improvement of storage efficiency is obvious in the N+X hybrid blockchain storage mechanism.This kind of blockchain storage mechanism improvs the high efficiency,intelligence and resource optimization of Energy Internet.In the next research work, we can continue to improve the incentive mechanism to improve the storage structure of the hybrid block chain, and constantly expand the internal structure of hybrid block chain, improve transaction processing scalability and storage capacity.

VII. ACKNOWLEDGEMENT

This work was supported by National Natural Science Foundation of China (Nos.61502039), Joint Lab of Sensing and Computational Intelligence.At the same time, I would like to thank my teacher, Kun Meng ,Mr Meng gives me numerous constructive comments and helps.I will thanks my partner, Shuo Xu,he gives me great support in this work.In addition, there esists other teachers' help and encouragement.I would like to express my sincere gratitude to them.

REFERENCES

[1] Wang Jiye, Meng Kun, Cao Junwei, et al. Information Technology for Energy Internet： A Survey [J]. Journal of Computer Research and Development, 2015, 52(3):1-18 (In Chinese).

[2] Dong Zhaoyang, Zhao Junhua, Wen Fushuan, etc. From smart grid to energy internet: basic concepts and research framework[J]. Automation Of Rectric Power Systems, 2014, 38 (15) : 1-11.(In Chinese).

[3] TransActive Grid, LO3 energy and consenSys[EB/OL].[2016-06-12].http://www.transactivegrid.net.

[4] G. Danezis, S. Meiklejohn. Centrally banked cryptocurrencies. NDSS'16.

[5] S. Nakamoto. Bitcoin: a peer to peer electronic cash system. 2008, bitcoin.org/bitcoin.pdf.

[6] http://www.8btc.com/bitcoin-ng-2.

[7] UK Government Chief Scientific Adviser, "Distributed Ledger Technology: Beyond Block Chain, " Government Office for Science,2016,https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

[8] Sia: Simple Decentralized Storage.David Vorick,Luke Champine.Nebulous Inc.November 29, 2014.

[9] IPFS - Content Addressed, Versioned, P2P File System(DRAFT 3) .Juan Benet.juan@benet.ai.

[10] BigchainDB:A Scalable Blockchain Database(DRAFT) .