Video Computing Across Trust Domains Based on Blockchain

Yangyang Gao†
Innovation Center
China Academy of Electronics and Information Technology
Beijing, China
ygao@innovations.center

Yangyang Li
Innovation Center
China Academy of Electronics and Information Technology
Beijing, China
yli@csdslab.net

Yue Jia
Innovation Center
China Academy of Electronics and Information Technology
Beijing, China
yjia@innovations.center

ABSTRACT

Smart city construction brings great development opportunities for the video surveillance industry, but it also brings significant challenges. With the development of Internet of things and artificial intelligence technology, video computing across different trust domains has become important and necessary for ensuring public safety and promoting smart city construction. With the continuous increasing of video front-end equipment and massive video data, trust and security problems across different domains, network bandwidth and computing resources are gradually becoming bottlenecks of video computing. We propose a solution based on integration of blockchain and Internet of things which brings together and distributes video data and computing resources to enhance the edge video computing capability. Blockchain provides a distributed solution for trust video computing across different trust domains. We evaluate the performance of blockchain-based video computing solution across different trust domains and the results show that this solution could provide trust video computing across trust domains feasibly and efficiently. This solution implies a new trigger of trust distributed applications and innovative trust economic ecosystem.

CCS CONCEPTS

• Insert CCS text here • Insert CCS text here • Insert CCS text here

KEYWORDS

Blockchain, Edge cloud, Trust, Security, Privacy, Video computing, Internet of things

ACM Reference format:

*Article Title Footnote needs to be captured as Title Note
†Author Footnote to be captured as Author Note

ACM *TURC-AIS'19, 17-19 May 2019, Chengdu, China*
 978-1-4503-7158-2/19/05…$15.00
https://doi.org/10.1145/3321408.3326693

Yangyang Gao, Yangyang Li and Yue Jia. 2019. Video Computing Across Trust Domains Based on Blockchain. In *TURC-AIS 2019: ACM TURC Conference on Artificial Intelligence and Security, May 17–19, 2019, Chengdu, China. ACM, New York, NY ACM, New York, NY, USA, 9 pages.* https://doi.org/10.1145/3321408.3326693

1 Introduction

In recent years, with the development of smart city construction and Internet of things, the video surveillance industry has developed greatly. There are many video front-end devices have grown explosively, therefore the video data and relative resources have increased exponentially. The video front-end devices belong to different organizations and they formulate various trust domains. For the sake of trust, security and privacy consideration, there are barriers for sharing resources and video data to create more value for public safety and smart city construction.

Video computing across trust domains has become a demanding technology which can be deployed based on the independent video surveillance systems to achieve broad range integrated computing capability and analyze more valuable targets. Video computing is one typical type of the Internet of things (IoT) applications. Different video surveillance systems belong to different trust domains. Different trust domains could not share the video data and computing resources with other trust domains securely and reliably. The video computing across trust domains could not be implemented with the shortage of trust among various trust domains. To overcome the barriers, the blockchain technology has been involved into the solution.

Many projects relate to blockchain integrated into Internet of things have been developed include but not limited to IOTA [1] providing a revolutionary new transaction settlement and data transfer layer for the IoT, Atonomi bringing Trust and Security to IoT [2] and Secure and Safe Internet of Things (SerIOT) [3]. According to those search results of the blockchain applications in IoT, there are two types of applications which are token-based and token-free. The blockchain could revolutionize the development of IoT ecosystem [4-7]. The agent server in an IoT system supports the function of blockchain nodes. The full and lightweight blockchain function could be deployed on different physical nodes [8-10]. Besides, the InterPlanetary File System (IPFS) could be deployed as the big file storage of the blockchain [11-14].

The Merkle tree and other encryption mechanisms integrated with distributed consensus algorithms could help maintain the security and privacy for IoT systems [15-18]. Normally, IoT in itself is a distributed communication system. Blockchain works as a distributed ledger solution. Integrating these two techniques could be both a trigger to revolutionary application and an innovative economic ecosystem [19-22]. The blockchain works as a potential solution considering feasibility, efficiency and other metrics of performances.

The storage solution of IPFS helps to solve the problem which blockchain cannot store big files and documents. Integration of IPFS and blockchain could provide a solution, in which the blockchain can search new documents stored in IPFS. IPFS is a content addressing scheme which could provide content index. The indexed content identifier could be stored in Blockchain, which cannot be modified and deleted. The mapping between IPFS file and blockchain could be used for trust file searching and retrieving. The mapping could be an efficient solution for distributed file sharing and trust web searching mechanism. The content addressing integrated blockchain could be improved through the identity trust and content self-verification. On the basis of content addressing, the integration of blockchain and IoT could be employed in many realistic application scenarios.

2 Problems

With the development of smart city, there are more and more video surveillance systems. Most of them are separated by the organizations and the video content could not be shared and interchanged to bring more value. Internet of videos is one type of IoT, which is a distributed communication system as well. Blockchain can work as a distributed ledger solution. Integrating these two techniques could bring a possible solution for trust video computing among different trust domains. Without blockchain, it is difficult to achieve the goal of trust video computing across different trust domains. Although, blockchain provides a possible way for trust video computing across trust domains, there are still many problems to be solved.

The prerequisite for different video surveillance sharing and cooperation is the trust establishment among various trust domains. Firstly, there is a problem rooted in the content storage on the blockchain. The root is the content which could not be verified before they are posted on the blockchain. The alliance of video computing could be established to help solve this problem. In order to guarantee the correctness and security of the content, the alliance nodes should function as verification nodes to check the posted content. Then the verification nodes push the checked content to the whole blockchain if they comply with the regulations of the alliance. After all these have been done, users could trust the content on the blockchain. The alliance should be agreed on and polled to be established. If attackers destroy any alliance node, there would be harmful for the security of the blockchain. Therefore, there should be a feasible mechanism to establish the alliance and the validated regulations. The alliance and the regulations should be tested in sandboxes before the mechanisms are validated on the blockchain. Above all, the pre-verification of video content and security check process should not be checked only on the blockchain technology. The distributed security problems could be solved through establishment and deployment of the alliance security mechanism.

Secondly, the video producers and posters identity trust would be a precondition for trust video computing. The video producers and posters identity should also be verified and protected from the attackers, the public address could be one-time usable, which is dynamic and removed after the first usage. By doing so, the identity of the blockchain could not be traced and mapped by the attackers. Identity security and content security could be guaranteed through the mechanism of alliance and the regulations. With the enhancing of alliance security, the security of blockchain could be improved greatly [23-26]. The establishment of alliance and guarantee of regulations help to solve the trust and security problems in the video computing across different trust domains.

In addition, the video front-end equipment has grown exponentially, and as a result the video data has been greatly increasing. The video computing across different trust domains brings challenges for computing and network resources request and distribution. To solve these problems, the edge cloud would be employed to handle the distribution of resources to improve the video computing performance.

3 Blockchain

Based on blockchain, IPFS and secure alliance, there could be a possible solution for some IoT application scenarios. Imagining that the IoT endpoints function as a blockchain nodes, they could be collaborated and work more efficiently and reliably. The IoT nodes could be verified and arranged to a trust identity in the IoT system, which could be valid across different trust domains. The IoT nodes with verified identity could function and deploy the automatic chaincodes to execute smart contracts. A chaincode in the blockchain could be triggered by the condition which related to the real service scenario and the physical environment. The real services could trigger one or a series of smart contracts, which is processed by deploying relative chaincodes to finish different actions. These actions could be automatically executed by the IoT system nodes. With the smart contracts, the IoT system could be designed to execute various tasks automatically.

In different IoT systems, services and demands are customized. The smart contracts are designed to adapt to the physical environment and the real services. When the trigger conditions are fulfilled, the smart contracts in the blockchain could be executed on the IoT endpoints. In the internet of videos, the trigger condition could also be applied as an alert condition. If there is any harmful content within the camera video, the trigger could be fulfilled and posted to the alert center automatically. In the internet of vehicles, cars could be triggered to arrange to most appropriate charge points to recharge themselves and automatically find the nearest parking lot when the route destination is not far away.

3.1 Compatibility

With the smart contracts, there are many other scenarios that could be developed in IoT systems such as the internet of videos. The automatic tasks could be mapped to the smart contracts to facilitate the society. A good design of smart contract mapping to the real service could save the cost greatly. Given a deep analysis of the IoT scenarios, there are many other applications could be developed and designed to help the real services. Considering the edge computing demands, the IoT integrated with the backend of the IoT system could also be feasible. The edge computing nodes collaborate with the endpoints and the cloud platform. With the smart contracts, the edge computing usage and cost could be computed easily. The endpoints and the edge computing resources distributions could be designed more efficiently. The edge computing could be deployed more efficiently on the smart contracts. The request nodes could apply for computing, network bandwidth and storage resources while the cost could be computed reasonably and the resources distribution could get consensus among all nodes. With the smart contracts mapping to the edge computing, the resource distribution and cost computation could be deployed more easily and efficiently. Therefore, the blockchain integrated with IoT system could solve a lot of inherent problems and bring many advantages. Integrating the IoT and blockchain technology is a good choice in the distributed scenarios and applications.

3.2 Integration

Each IoT application scenario could be mapped to a distributed application (DApp) based on blockchain. The application-related resources should be managed by the management modules which are controlled by the smart contracts. The distributed applications could be implemented on the blockchain. Each IoT system application scenario could be related to a DApp, with the development of various DApps based on blockchain, they could gradually become a large scope of blockchain with permissioned authentication. Real time DApps could not be created directly on the blockchain technology. To support real time DApps, the blockchain technology should be integrated with other technologies, such as smart contracts and consensus algorithms, which could function as a key part of the integration architecture.

In the video computing across different trust domains, different IoT nodes communicate with nearest edge computing nodes to apply for resources. Then the edge computing layer responds to the endpoints and distribute the resources to the endpoints and push the results to the next hop according to the pre-set process. The blockchain could be instantiated by the related chaincodes to automatically execute the smart contracts about the cooperation between endpoints and edge computing nodes.

Based on the blockchain, the IoT system could be improved in many aspects including efficiency, security, reliability and trust and so on. The smart contracts also support smart IoT systems. The IoT systems can automatically finish real services according to the environment and system conditions. This advantage could also better support the smart operations of large scale IoT systems. The blockchain could be a good solution for different trust domain endpoints cooperating with other nodes. The blockchain could be employed to establish trust among different trust domains which could be identified and verified. The endpoints identity and the data gathered could be verified through different mechanisms. If other trust domains need to use the data, they could cooperate with each other through the blockchain technology, the data sharing and data privacy could be guaranteed by the blockchain technology. The IPFS could also be used to store large data files and indexed hash putted on the blockchain. Data users could gain the data usage authorization and pay for the data using cost. The blockchain could compute the cost and distribute the authority to the data users, the payment could be forwarded to the data source trust domain. This could build a relatively complete ecosystem of the integration of blockchain and IoT systems. The interplanetary linked data (IPLD) of the IPFS could bring a new data structure for the addressable content in IoT system, while the Merkle tree could be used to verify the content integrity.

3.3 Challenges and Contributions

There are many problems in IoT system which could be solved based on the integration of blockchain technology. The cooperation of cloud platform, IoT edge computing nodes and IoT end points could be trusted among different trust domains. Different trust domains dominate their own IoT endpoints and belong to different edge computing nodes and cloud platform. In order to facilitate the cooperation and collaboration of different functional nodes, the blockchain could be deployed to support the solution.

A significant problem should be considered is that how to bring the IoT data to the blockchain, which is a difficult problem that must be confronted by the system whose data would be put onto the blockchain. Each application scenario has different needs for the data put onto the blockchain. In some cases, the data needs to be posted on blockchain may even not be electronic format, which is the preliminary requirement for data put onto blockchain. Therefore, the application of blockchain could be hard to evolve fast without electronic data process and then put onto blockchain following the specific application data regulations. Digitalizing the files and documents that would be put onto blockchain is the basis of the blockchain-related services. Digitalizing is the precondition for blockchain-related implementation. The files and documents should be electronic and digitalized to support the blockchain-related services. Based on the blockchain technology, the problem could be solved and the new ecosystem could grow fast and positively. In the internet of videos, the video data verification and storage should be considered before the data posted onto the blockchain.

There is a shortage of integration architecture of blockchain and Internet of videos. The solution of video computing across trust domains would also handle the distributed large video data and the required computing resources. In order to solve the problems of trust video computing across different trust domains, the contributions are as follows.

We propose an integration architecture of blockchain and IoT systems, which provides the framework of integrating blockchain and Internet of videos. The IoT system is distributed, the

blockchain architecture complies with the existing architecture and there is no big revolution in the existing architecture of IoT systems.

In addition, in order to distribute the video computing resources, we propose edge cloud chain, which could manage and distribute the computing resources to the video computing tasks. The blockchain layered between the edge computing layer and the endpoints layer, besides the blockchain nodes could be deployed between the cloud platform and edge computing layer. The cloud platform could use blockchain nodes to manage the edge computing resources, which establishes the trust between the cloud platform and edge computing nodes. The edge computing nodes could cooperate with each other to provide resources for the IoT nodes.

In the deployment, the blockchain nodes could be a new addition to the existing architecture, or they could also be deployed on the existing nodes to function as blockchain nodes. The distributed blockchain nodes could bring reliable system and there could be hardly one-single-node failure problem.

We evaluate the solution through different video computing tasks across different trust domains, the results indicate the feasibility and efficiency of the solution.

4 Solution and Evaluation

We propose a solution for video computing across trust domains based on blockchain. The solution is composed of the integration architecture, the edge cloud chain and trust video computing applications and the deployment. Based on video computing tasks across various trust domains, we evaluate the feasibility and efficiency of the solution performance.

4.1 Integration of Blockchain and IoT systems

In the integration of blockchain and IoT systems, we consider the IoT system requirement and the blockchain functions. Considering the various IoT systems, there are two steps to put IoT system data onto blockchain. One is that data and files should be transferred to electronic format, the other is that the application regulation for data and files that need to be used for data process when putting them onto blockchain. There could be some common regulations and some application-specific regulations. It may take a period of time to transfer data and files while designing and implementing feasible regulations. The integration-based DApps design and development could also be considered in this stage, which could bring advantages to the whole system design and development. By doing so, the blockchain and application implementation could be combined tightly and the application could be more efficient and feasible.

The application scenario could be classified and extracted to build the main framework for the same classification. This could be a reference for the similar application scenarios, which could be a basis of further development of the DApps in IoT scenario and the whole ecosystem. The ecosystem could be expanded greatly based on the blockchain technology. The blockchain integrated with IoT systems could evolve to a new stage.

In the integration, we consider the data protection and sharing in IoT systems. The blockchain layer provides a solution for balancing the need of data protection and data sharing. The distributed IoT system should be integrated and identified through integration of blockchain and IoT system, the device identity authorization, the data generator, data producer, data consumer, data propagation and data value throughout the whole IoT system should be considered deeply to guarantee the parties in the system could run fluently and efficiently. Without data sharing, the ecosystem development would be compromised. With fast expansion of IoT system, data sharing would be a great need in the future and a good sharing mechanism could promote the smart society evolution. While the data security is guaranteed, the data usage and transfer process could be tracked to be informed to the data owners. The data owners should authorize the data usage and transfer. The disclose level of data should also be managed by the system. The desensitization of data should also be executed to guarantee data protection.

The integration architecture is designed based on the above consideration of problems and targets. As shown in Figure 1, the architecture of IoT over Blockchain include four layers including the IoT system layer, the blockchain layer, the smart contracts layer and the application layer. This architecture is customized for the internet of videos. The IoT system layer includes the video surveillance systems; the blockchain layer includes video content verification and video computing resource management and distribution; the smart contract layer is responsible for different video computing negotiations including the video data and computing resource request and response; the video application layer includes different video computing application scenarios.

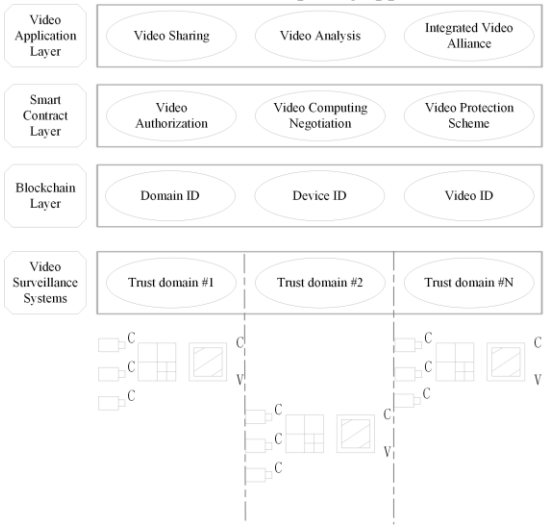

Figure 1: IoT over Blockchain Architecture

4.2 Edge Cloud Chain

In this architecture, the trust video computing across different trust domains has to solve the problem of computing resource management and distribution. The solution of video computing across trust domains is edge cloud chain, which requires edge cloud

architecture to handle the video computing resource distribution. Edge cloud computing would form permissioned chains to support various distributed applications. When applications evolve to a large scope, the edge cloud chain needs to become larger and some chains could become public to meet different demands of various application requirements. Edge cloud chain is built upon the endpoints and the edge servers, besides between the cloud server and edge server to meet the integration design and deployment of the edge cloud chain. The cloud servers provide backend support for the edge server, and the edge server supports for the endpoint service requirements. In the edge cloud chain, the edge cloud server resources management responds to the service resource requests and decides whether the application could be responded to support the video computing task, and the edge cloud chain provides different kinds of access mechanisms to different IoT endpoints, considering the hardware and software requirements for the endpoints.

Edge cloud chain is used to distribute resources and improve the whole system performance. Without support of blockchain nodes, the IoT devices should traverse a gateway to access to the edge chain, and the other devices supporting chain nodes could directly access to the edge cloud chain. Given the hardware resources such as RAM, storage, CPU and network interfaces, the devices could function as a full-chain node, or as a lightweight chain node to finish part of the chain node functions. The edge cloud chain could be integrated with smart contracts to realize different functions in the distributed application scenarios. The smart contracts API could be used to access the endpoints data, which could be processed or directly transported to the edge chain, the edge chain could execute different actions to meet the application demands.

The edge cloud chain brings many application scenarios for IoT systems. The non-currency resource-related services include resource management, cost computation and resource request and response. The edge cloud chain could evolve to support many service demands. The different applications could be supported by the integration of edge cloud chain and smart contracts. The IoT application demands could be mapped to edge chain and smart contracts. The IoT endpoints could be seen as a trigger to execute the smart contracts, the smart contracts process the endpoints data and execute the different operations in the edge chain, the edge chain could be used as the resource computation and cost computation to support the resource management. The edge chain stores the results of the request and response to manage the IoT system resources, the performance of the edge chain depends on the schemes used in the edge chain. Merkle DAGs could be used for content addressed and indexed, the search performance could be improved in the distributed scenarios. In the internet of videos, the edge chain could verify and distribute video data and computing resources. The video data index is stored in the edge chain, and the edge cloud resource information is also recorded in the edge chain.

4.3 The Distributed Systems and Applications

In the integration architecture, the smart contract layer supports the application layer. There are many schemes designed to adapt to different system preferences in various application scenarios. The IoT systems become more efficient with the deployment of the integration of edge chain and smart contracts. This solution integrates the smart contracts and the edge chain, the IoT endpoints could trigger the edge chain to support the application requests. The edge chain could request the backend servers to provide more efficient resource utilization.

Moreover, the problems of the distributed systems and the trust distributed applications could also be supported by this solution. To implement the trust distributed applications in the IoT systems more efficiently, the smart contracts and the rule engine are designed more specifically to adapt to different application requirements. The smart contracts could be designed more efficiently by deploying different mechanisms. The applications could also be improved by the deployed edge chain, the edge servers could cooperate with the IoT endpoints to gain more specific resource management, small traffic load, low delay and more services capacity.

The smart contracts work as a point of entry for the resource management mechanism to actively make the cloud resources report in the edge computing platform. When the percentage of available resources has been at a low level, there could be some actions to process the incoming services requests and meet the requests more effectively and process the requests of the IoT services according to the IoT system state and make a fast decision to distribute resources to the requests of IoT services. This could be more efficient to influence the system resource distribution and achieve the performance improvement of the IoT systems.

The distributed metrics of blockchain technology could provide a basis for deploying the IoT applications. And it is efficient to employ different smart contracts executing different tasks and processing demands. The distributed blockchain with the distributed applications supports more efficient distributed application deploying and processing. The solution combines the application and the blockchain technology tightly and steadily, which could employ the advantages of the blockchain to boost the application development and solve the existing and potential problems which would be confronted in the development. Therefore, the video computing across trust domains could be implemented based on the blockchain and IoT infrastructure. The services require distributed cooperation among various trust domains. The performance of the distributed systems could be improved by the solution.

The distributed applications could be implemented based on the blockchain technology, which provides a trust basis for the applications and execute collaborative computing tasks. Trustless parties cooperate to negotiate and establish trust among themselves based on blockchain. The established trust could be employed to accomplish many trust-related applications. The edge chain could be a practical framework for the blockchain application. The video computing across different trust domains application is implemented based on the edge chain.

4.4 Deployment

The solution of edge chain could be implemented on the existing infrastructure or on the new devices which would add new nodes to

the network. To efficiently deploy the edge chain as shown in figure 2, the existing infrastructure could be integrated with the blockchain technology. The edge chain locates at the edge of the IoT system, the edge of the IoT system takes the responsibility of applications and edge computing between the end users and the cloud backend server. Edge chain could record the IoT system resources and transactions to provide resource distribution and management. Edge chain establishes the trust of the end users and edge resources, which distributes edge cloud resources to the end users without directly forwarding the tasks to the cloud backend servers. Edge chain would integrate the blockchain technology into the edge cloud and the distributed IoT applications.

The integration of edge chain and smart contracts could provide a new method of designing and deploying resource management schemes to improve the whole system performance. The smart contracts contain a series of actions which would be operated in the IoT system. With the design and deployment of smart contracts, the edge chain could be accessed by the IoT endpoints and the backend servers, which could make IoT trust distributed applications become more efficiently and feasibly.

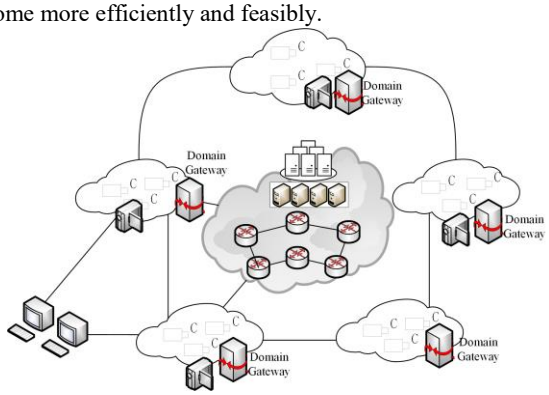

Figure 2: Edge Chain Deployment Illustration

The edge chain is responsible for computing resource request, response, cost computing and finishes the whole transaction of resources. The edge chain in the IoT system edge cloud supports resource sharing and distribution. The end users could get corresponding resources to execute the computing tasks and provide efficient resource distribution and management. The edge clouds could establish trust to collaborate with each other and improve the whole system performance from the bird-view point. The edge chain works as an infrastructure to implement the trust collaboration among different trustless edge clouds. The trust infrastructure is based on the blockchain technology, which supports the edge computing among different edge clouds. The edge chain provides the edge cloud with a collaboration to improve the resource utility efficiency. The edge chain is deployed to collaborate different edge clouds to improve the IoT system performance. The edge chain records the transaction and traces transaction untampered log, which could provide different nodes collaboration trust basis for distributed applications. As a result, the deployment of the edge chain could provide edge clouds with trust resources sharing and video edge computing across different trust domains.

The edge chain provides a scheme to distribute and compute the cost of the end users, which could use the free resources to create more value. The edge cloud resources could be integrated and collaborated to undertake the same task and achieve the rewards based on the done work. The work billing could be negotiated and deployed on the edge chain. The edge chain with the billing smart contracts could support the edge cloud collaboratively. The smart contracts could be integrated with the edge chain to execute specific operations to support various computing tasks. The edge chain could be enhanced by the smart contracts, which map to different application scenarios. The applications could be supported by the blockchain technology based on the smart contracts. The smart contracts function as the middleware between the edge chain and the applications. The edge chain integrated with smart contracts could be applicable for different application scenarios. The applications could be implemented based on the edge chain integrated with specific smart contracts. Different applications have their specific requirements, which map to different smart contracts. The smart contracts deployed on edge chain could be triggered by different conditions and execute different actions.

The solution employs the IPFS as the storage layer of big files, the blockchain as the access layer of content, the content in the system has its own identity. The addressed content index could be putted on the blockchain, which could be accessed through the content hash value. When the content changes, the hash value changes accordingly and the history of the values could record the history of the content changes. The record of the changed values could work as a proof for traceability.

The applications are deployed with the edge chain through the design and deployment of smart contracts. The edge chain could make the edge cloud resource utility efficiently, which provides a framework for solving the edge cloud and computing collaboration. The framework could also be used for other applications such as the edge cloud resource distribution and the end user management policy, the edge cloud trust applications such as computation of cost and reward. The edge chain integrates the blockchain technology with the IoT systems, which provides more efficient edge cloud services for end users. The edge chain provides a solution for trust distributed application scenarios, which could be a good way to guarantee trust and security of the distributed IoT systems.

4.5 Evaluation

The computing across different trust domains could be solved by integrating IoT systems with edge chain, which supports trust distributed applications efficiently. The edge chain would be more applicable with the smart contracts design and implementation. The applications could also be supported by the integration of edge chain and smart contracts. The edge chain is a good demo for other chains to be implemented in IoT systems. The solution of the edge chain includes the blockchain modules, the device identity and the resource management and distribution.

The evolution of edge computing is based on the distributed trust basis. In the edge chain modules, the blockchain provides the trust domain for video data and resource distribution. The edge chain integrated with smart contracts could be deployed to bring new types of applications in the IoT system. The edge chain provides the trust infrastructure for edge computing. The IoT system integrated with blockchain could bring trust distributed applications. The applications could be implemented more efficiently. The blockchain could also be improved by the ecosystem development. And the IoT system could be enhanced and triggered by the blockchain technology. Therefore, distributed edge chain cooperates to implement the trust basis for the distributed applications.

In the internet of videos, the integration solution of blockchain technology could be applied. The blockchain deployed in the trust domains supports trust video computing across different trust domains. The edge chain could bring trust and resource utility improvement in the system. To evaluate the video computing edge chain across different trust domains, we provide several trust domains with video files shared to create more value. The evaluation includes two tiers, one of which are video files verification and sharing, and the other is the resource request and distribution using smart contracts to request resources in the edge cloud. The evaluation components are shown in figure 3.

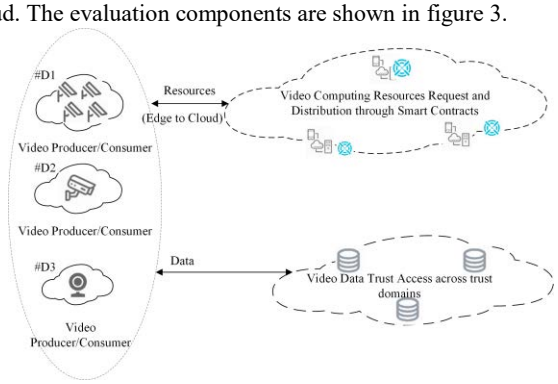

Figure 3: Evaluation Setting of the Solution

In the evaluation, we employ different amount of video trust domains, the video computing tasks has different resource requests. Without the solution, the video computing across trust domains could not be implemented without negotiation of domain organizations. With the solution, we could automatically verify the video files and check whether the needed computing resources could be satisfied or not. The evaluation shows that the time consuming for video request and response per task will not increase with the trust domains and tasks number varies, as shown in figure 4. The resource request could be automatically done through the smart contracts, the consumed time of different task amount in different trust domain is shown in figure 5, and the consumed time per task of resource request will not be varied with the increasing of task amount, as shown in figure 6. The time consuming for video computing per task will not increase with the trust domains and tasks number varies, as shown in figure 7.

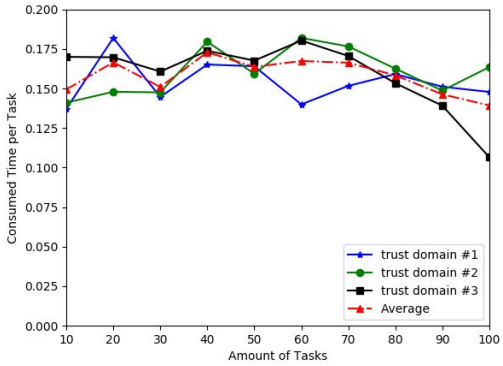

Figure 4: Consumed Time per task of Video Request and Response in Different Task Groups

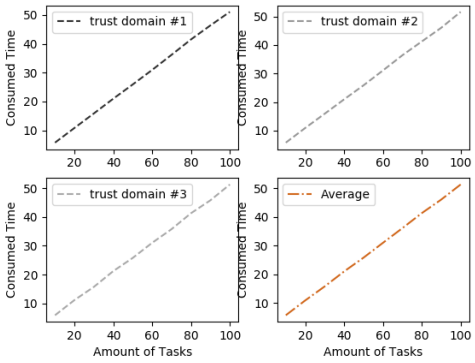

Figure 5: Consumed Time of Resource Request Tasks in Different Trust Domains

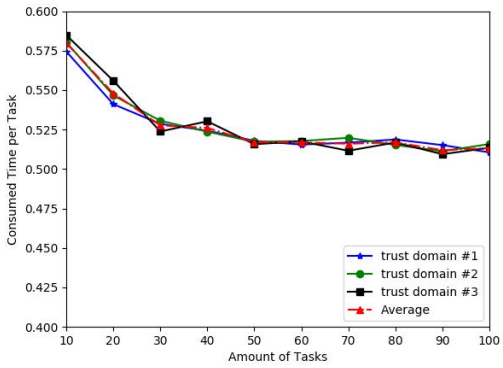

Figure 6: Consumed Time per Task of Resource Request in Different Trust Domains

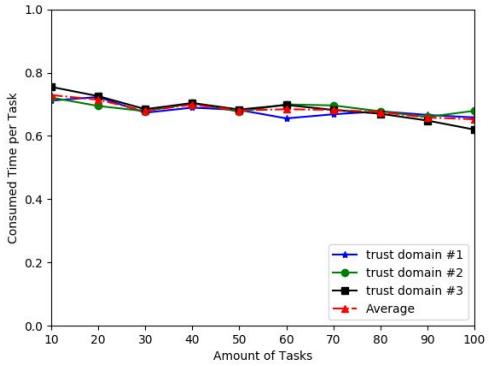

Figure 7: Consumed Time per Task in Different Trust Domains

The results indicate that the video computing based on the blockchain solution could guarantee the feasibility and efficiency with the increasing task amount. In the video computing across different trust domain, the video data could be verified and fetched efficiently and securely, and the video computing resources request could be processed through smart contracts automatically and efficiently.

5 Conclusion

The integration of blockchain technology and the IoT systems provides the architecture and solution for the distributed and trust application scenarios. The hierarchical architecture of the integration of IoT systems and the blockchain is a part of the edge chain. The IoT systems include endpoints, edge cloud and cloud servers. The integration is composed of edge chain, cloud servers and endpoints. The IoT system resources are distributed among the endpoints based on the blockchain and smart contracts. The smart contracts could apply the blockchain to the IoT system applications. The smart contracts could be designed according to the application scenarios. The smart contracts and the blockchain technology can build the integration of IoT systems and the blockchain technology. The smart contract is related to the specific application scenario. The IoT systems and the blockchain technology could be integrated according to the application scenarios. The integration could meet the application requirements based on the smart contracts. The smart contracts could be applied to the application scenarios. The endpoints, edge chain and cloud servers provide the basis for the integration deployment. The integration of the blockchain technology and IoT systems could support distributed and trust applications. The blockchain technology could be used for the distributed trust applications.

In the video computing across trust domains, the blockchain integrated with IoT systems could improve the performance of resource distribution and utility efficiency. Based on the blockchain technology, the smart contracts could bring more efficient resource request and distribution. The blockchain and edge chain could be deployed in the IoT systems. The integration of the blockchain and the IoT system could bring more application scenarios and evolve to a larger ecosystem. The cloud server and edge chain could bring new triggers for the distributed trust applications. The architecture could be modified to integrate IoT systems with blockchain technology.

The solution of integrating the blockchain technology with the IoT systems could be a good exploration for the trust IoT system applications. The IoT system application scenarios could be expanded to a new level with the metrics of trust and distributed with the integration of blockchain technology. The integration of the blockchain technology and IoT systems is fundamental for the trust applications. The distributed trust systems could be evolved based on the blockchain technology and IoT systems.

In addition, the distributed trust ecosystem could evolve to other areas. The integration of blockchain and IoT systems has the following metrics.

- A Trust overlay on a trustless network
- Video content addressed in the distributed system
- Difficulty target for the video computing across trust domains
- Blockchain storage and authentication
- The video data could be stored in IPFS
- The authentication information could be stored in the blockchain
- The security of the video search is guaranteed by the blockchain
- The video computing resources negotiation are based on smart contracts

The integration of blockchain and IoT systems provides another way for evolving and deploying the distributed trust applications. The IoT systems could become trust-enhanced based on the blockchain technology. The contents are stored in IPFS, the blockchain could be integrated with the content address and index. The blockchain technology could be applied into the IoT systems. The integration could be improved in many aspects. The trust, security and the distributed consensus could be implemented in the practical scenarios. The integration could trigger the application development, which could provide a reference for the potential application scenarios. An integration of the blockchain technology, smart contracts and IoT systems could provide the basis for trust distributed application ecosystem. The large scale of distributed systems could be implemented based on the blockchain technology and the edge chain. The large scale of distributed network could be implemented based on the enhanced security and trust brought by the blockchain technology integrated with the IoT systems.

In the future work, we could try to record the video transactions hop by hop and trace the network port metrics with the blockchain technology, the port metrics could be recorded in the blockchain. The edge chain could be used for distributing resources among different trust domains. The forwarding route could be recorded to analyze the traffic flow history. In this way, the trust of the network path could be established as well.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their careful reading of our manuscript and their many insightful comments and suggestions. The authors would like to acknowledge the financial support from the Beijing Science and Technology Plan(Grant No. Z181100009818020).

REFERENCES

[1] B. Siever, M. P. Rogers, "An IoTa of IoT (Abstract Only)." in Proc. SIGCSE, 2017, pp. 742.
[2] Atonomi, https://atonomi.io/.
[3] E. Gelenbe, J. Domanska, T. Czachórski, A. Drosou, D. Tzovaras, "Security for Internet of Things: The SerIoT Project." in Proc. ISNCC, 2018, pp. 1-5.
[4] I. Makhdoom, M. Abolhasan, H. Abbas, W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward." J. Network and Computer Applications, vol. 125, pp. 251-279, 2019.
[5] P. Sharma, M. Chen, J. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT." IEEE Access, vol. 6, pp. 115-124, 2018.
[6] L. Fan, J. R. Gil-García, D. Werthmuller, G. B. Burke, X. Hong, "Investigating blockchain as a data management tool for IoT devices in smart city initiatives." DG.O, vol. 100, pp. 1-2, 2018.
[7] N. Teslya, I. Ryabchikov, "Blockchain Platforms Overview for Industrial IoT Purposes." FRUCT, pp. 250-256, 2018.
[8] R. Agrawal, P. Verma, R. Sonanis, U. Goel, A. De, S. Anirudh-Kondaveeti, S. Shekhar, "Continuous Security in IoT Using Blockchain." ICASSP, pp. 6423-6427, 2018.
[9] P. Danzi, A. Kalør, C. Stefanovic, P. Popovski, "Analysis of the Communication Traffic for Blockchain Synchronization of IoT Devices." ICC, pp. 1-7, 2018.
[10] E. Regnath, S. Steinhorst, "LeapChain: efficient blockchain verification for embedded IoT." ICCAD, vol. 74, pp. 1-8, 2018.
[11] J. Benet, "Ipfs-content addressed, versioned, p2p file system." arXiv preprint arXiv:1407.3561, 2014.
[12] D. Dias, J. Benet, "Distributed Web Applications with IPFS, Tutorial." in Proc. ICWE, 2016, pp. 616-619.
[13] M. Sicilia, S. S. Alonso, E. G. Barriocanal, "Sharing Linked Open Data over Peer-to-Peer Distributed File Systems: The Case of IPFS." in Proc. MTSR, 2016, pp. 3-14.
[14] S. Muralidharan, H. Ko, "An InterPlanetary File System (IPFS) based IoT framework." in Proc. ICCE, 2019, pp. 1-2.
[15] B. Yu, J. Wright, S. Nepal, L. Zhu, J. K. Liu, R. Ranjan, "IoTChain: Establishing Trust in the Internet of Things Ecosystem Using Blockchain." IEEE Cloud Computing, vol. 5, no. 4, pp. 12-23, 2018.
[16] M. Hammi, B. Hammi, P. Bellot, A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT." Computers & Security, vol. 78, pp. 126-142, 2018.
[17] Z. Hao, R. Ji, Q. Li, "FastPay: A Secure Fast Payment Method for Edge-IoT Platforms using Blockchain." SEC, pp. 410-415, 2018.
[18] M. Khan, K. Salah, "IoT security: Review, blockchain solutions, and open challenges." Future Generation Comp. Syst., vol. 82, pp. 395-411, 2018.
[19] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities." Future Generation Comp. Syst., vol. 88, pp. 173-190, 2018.
[20] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT." IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184-1195, 2018.
[21] C. Qu, M. Tao, J. Zhang, X. Hong, R. Yuan, "Blockchain Based Credibility Verification Method for IoT Entities." Security and Communication Networks, vol. 7817614, pp. 1-11, 2018.
[22] A. Panarello, N. Tapas, G. Merlino, F. Longo, A. Puliafito, "Blockchain and IoT Integration: A Systematic Survey." Sensors, vol. 18, no. 8, pp. 2575, 2018.
[23] L. Zhou, L. Wang, T. Ai, Y. Sun, "BeeKeeper 2.0: Confidential Blockchain-Enabled IoT System with Fully Homomorphic Computation." Sensors, vol. 18, no. 11, pp. 3785, 2018.
[24] J. Chen, "Hybrid blockchain and pseudonymous authentication for secure and trusted IoT networks." SIGBED Review, vol. 15, no. 5, pp. 22-28, 2018.
[25] Y. Zhang, D. He, K. Choo, "BaDS: Blockchain-Based Architecture for Data Sharing with ABS and CP-ABE in IoT." Wireless Communications and Mobile Computing, vol. 2783658, pp. 1-9, 2018.
[26] T. D. T. Nguyen, H. Pham, M. T. Thai, "Leveraging Blockchain to Enhance Data Privacy in IoT-Based Applications." CSoNet, pp. 211-221, 2018.