2019 IEEE International Conference on Blockchain (Blockchain)

ArtChain: Blockchain-enabled Platform for Art Marketplace

Ziyuan Wang, Lin Yang, Qin Wang, Donghai Liu, Zhiyu Xu, Shigang Liu
Blockchain Innovation Centre
Swinburne University of Technology

***Abstract*—Blockchain is an emerging technology that has the potential to revolutionize the global industry and create a trusted relationship in a multi-party business network. There are a number of practical use cases where blockchain has been applied. One specific area is the Art industry, where it is a natural fit in the way that art forensics and transactions are conducted, tracked and recorded. This motivates us to develop the ArtChain platform to assist the Art Industry. In this paper, we present ArtChain, which is an integrated trading system based on blockchain. It includes the front end, the back end, the services, the smart contract, the chain connection and the deployment scripts from the bottom to the top. To the best of our knowledge, this is the first deployed blockchain-enabled art trading platform in Australia. It provides a transparent yet privacy-preserving, and tamper-proof transaction history for registration, provenance, and traceability of art assets. Our objective analysis and evaluation show that the ArtChain platform is applicable and practical. For the interest of other researchers, our system implementation related resources are open-sourced on Github[1].**

I. Introduction

Blockchain, also known as distributed ledger technology (DLT) [1], is designed to support verification-driven transaction services within a generally un-trusted ecosystem. The design of blockchain technology ensures that no one business entity can modify, delete, or even append any record to the ledger without consensus from other network participants, ensuring the immutability of data stored on the ledger. Blockchain is now being used in several industry applications such as blockchain-enabled traceability and provenance for food safety [2] documentation and cross-organization workflow management in trading and logistics [3].

With $200 billion of annual trading, the art market is one of the largest unregulated markets in the world, accounting for one-third of the amount of crime just behind drugs and guns [4]. Tens of millions of dollars are transferred with little or no documentation and transparency. Current challenges and issues in the art market are: (1) lack of transparency on prices and ownership history (provenance) and inadequate control of transaction data due to the information asymmetry; (2) the authenticity and appraisal of high-value works of art is difficult; (3) lack of the value of artworks at the primary art market and transparency trading at the secondary auction market (both online and offline); (4) lack of recognition, public attention and care for a large number of artists; (5) it is difficult for the artists to get royalty payment from the secondary market.

Blockchain technology possesses a natural fit to improve the transparency, keep records and reduce illicit activities in the art market, due to its inherent properties [5] [6]. In this paper, we present our project work, called *ArtChain*, a blockchain-based art trading system, which has been piloted and operated as a working product in practice. It is expected to provide a complete solution towards these challenges by creating a new ecosystem for the art keeping, trading and transferring. *ArtChain* fundamentally builds up the underlying architecture of blockchain to support a commercial-level trading platform centered around art assets. The core value proposition of the platform lies in:

- *Privacy Protection* Shared ledger along with permissioned control ensures the transparency of each transaction which guarantees the privacy protection in art trading and provenance.
- *Traceability* Real-time tracking of individual artworks combined with the blockchain ledger assists in the fight against counterfeit artworks.
- *Irreversibility* The on-chain registration of collectors offline assets provides an immutable digital record of the artwork, which guarantees the true ownership, the provenance and the value of the artwork.
- *Transparency* Publicly displaying artworks to a wider range of professional investors, leveraging the openness of art ecosystem.

II. Blockchain Solution towards Art Trading

In this section, we start with the rationale behind the use of blockchain for an art marketplace, and then discuss the benefits of this blockchain-enabled platform.

A. Rationale behind Using Blockchain

The major entities or participants in our solution are described in the following.

- *Artist* Established artists along with new generation artists all have equal opportunities for professional evaluation and to publish their artworks. Published items will be available for trade.
- *Art gallery* After artwork is registered on the blockchain system, it can be tracked and located in real-time giving an additional level of security to galleries.

[1] https://github.com/ArtChainGlobal

978-1-7281-4693-5/19/$31.00 ©2019 IEEE
DOI 10.1109/Blockchain.2019.00068

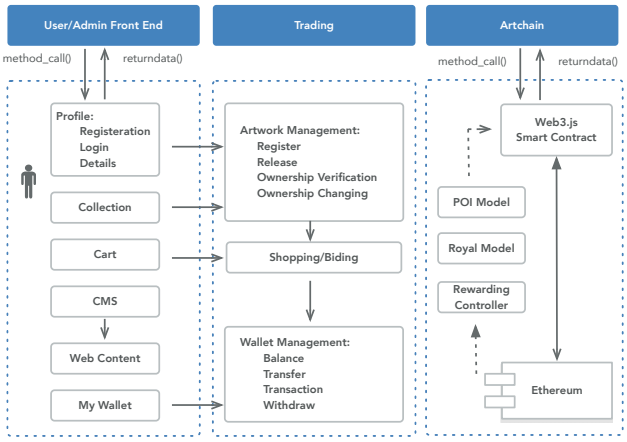

Figure 1. System architecture

- *Auction house* Data stored on blockchain can be synchronized with auction houses, opening up new channels for a greater global audience participation. More traffic equals more opportunities for all involved.
- *Collector* Online synchronization of collectors offline art assets. This proves ownership and sets the provenance of the pieces for future generations ensuring the value is preserved. Access to a global database with extensive filtering capabilities.

B. Benefits of a Blockchain-enabled Art Marketplace

Firstly, the artwork authenticity and traceable data can be simply achieved. Provenance is crucial when it comes to collecting art. Not having a record of the ownership history for a masterpiece often raises suspicion that it could be stolen or fake, hence a distributed ledger can be used to trace the transfer of ownership over a period of time, and serve as a decentralized database securing provenance data and other important information related to artworks. This allows for quick and indisputable ownership transfer in trading.

Secondly, royalty payment from the secondary market for artists can be achieved. A 5% royalty will be payable to visual artists on certain commercial sales of their work. This entitlement is created by the Resale Royalty Right for Visual Artists Act 2009.However, due to the difficulty in tracking the resales in the current art market, often artists do not necessarily get the royalty [7].

Thirdly, Blockchain audit trail helps in detecting tax evasion and money laundering. Add-on analytics or AI services can predict the current value of an artwork based on shared transparent data. This helps primary market valuation, which is more difficult and more speculative than secondary market due to a lack of market history.

Furthermore, our solution is designed to become an open, expandable infrastructure orientated towards the art industry. This means that participants will have the opportunity to develop an extensive range of art-related applications for specific scenarios based on the foundation of ArtChain.

III. System Overview

In this section, we first present the foundational principles the architecture is based on, the high-level architecture and its main components. Then, we present basic data model design and the trading process of the platform. In addition, we discuss the trust and security issues.

A. High-level Architecture Design

We first evaluate several blockchain platforms to inform our decision on which platform to apply. Based on the business requirements and technical assessment we decide to use the Ethereum private blockchain and Proof of Authority (PoA) [8] as the consensus algorithm. Initially, we considered to use Hyperledger Fabric to implement our system due to its capability, popularity and maturity. However, it lacks support in native token, which is a key business requirement in our design as the art trading platform hopes to integrate the payment process and the ownership transfer process. We design and implement a utility token called ACGT to achieve the high performance requirement. Refer to Section IV-A Tokenization for more details.

Here, we adopt microservices architecture for the following benefits: (1) Allows quick parallel development of various components in the application landscape; (2) Reduces discussion time between various groups developing various components; (3) When done properly, provides clean reusable interfaces; (4) When done properly, reduces handshaking in interfaces; (5) Reduces the risk and time of integration/chain testing. The architecture design is shown in Figure 1.

There are three layers in the system: the user front end, the trading back end, and the ArtChain blockchain layer.

- *User Front End:* includes the following functions: managing Profile for user registration, login and user details; displaying art Collection; shopping Cart; user Wallet; and CMS (Content Management System) to create and manage web content.
- *Trading Back End:* consists of Artwork Management, Shopping/biding, and Wallet Management. Artwork Management includes artwork registration, ownership verification and ownership transfer. Artists or collectors conduct the registration of their artworks through the assessment system of professional institutions within ArtChain. Their works of art will then be eligible for trading and participating in the ecosystem.
- *ArtChain:* including the following components: (1) *Royalty model:* responsible for artists royalty payment in the resale of their artworks. (2) *POI model:* manage *Proof of Interaction* (POI) agreements, which are used as incentives to grow the ecosystem of applications.

Figure 2. Data model: *User* Class

More details are described in Section IV-A. (3)*Rewarding Controller:* based on POI model to manage the rewarding to participants. The details are business confidential information, which is out of the scope of this paper.

B. Design of Data Model

There are three major groups of data objects stored in the distributed ledger as illustrated as follow:

- *User:* contains all information related to a user's profile, login, wallet, and auction events attended. An artist is also a user, with additional information and verification. The detail is shown in Figure 2
- *Artwork:* consists of details, tag, history of ownership transfer, and order details. These class represents the workflow related to the masterpiece. The detail is shown in Figure 3.

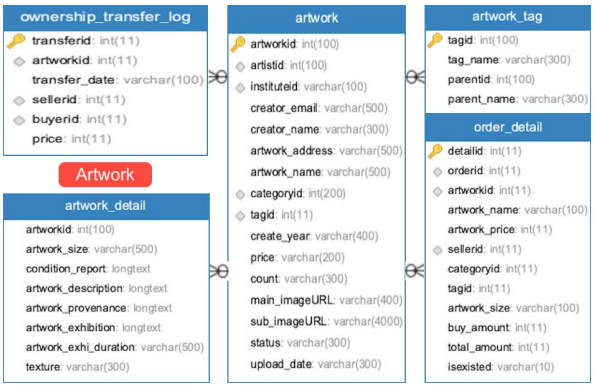

Figure 3. Data model: *Artwork* Class

Figure 4. Data model: *Trading* Class

- *Trading:* combines an order with the artwork and the buyer's basic information and the shipping address. The detail is shown in Figure 4.

The trading process is shown in Figure 5. When the user's trading request is received, Profile Services and Trading Services are triggered to retrieve the customer info and trade info. After checking the trading conditions, Payment Services are responsible for handling payment. Then Reward Services are called to request and receive the reward information. In the end, Shipping Services handle the shipping information.

C. Trust Establishment

ArtChain co-operates with specialized or high-profile partners in the primary or secondary markets of the art industry, including museums, art galleries, and auction houses, to establish the **original** ledger nodes and provide core functions such as validating, ordering and generating blocks of transactions. These ledger nodes and other agent or routing nodes work together to protect the blockchain network.

We use Proof-of-Authority (PoA) as the trust model of ArtChain network. PoA is well-suited to regulated industries where entities are responsible for maintaining the network (known as authorities), rather than remain anonymous as in mining-based chains.

For our practical purpose, well-known museums and art galleries are acting as authorities in ArtChain network to conduct authenticity and price assessment for an artwork. They are called SuperNode. Supernodes perform validating, block generation and publishing.

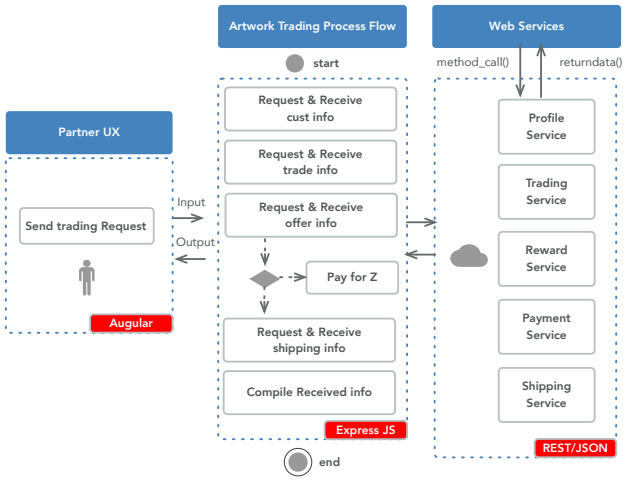

Figure 5. Trading Process

Any node attempting to engage in malicious conducts or falling under attack will be immediately detected by other nodes in the network once it shows unusual behaviour (e.g., sending illegal transactions, traffic attacks, and data tampering). The network will immediately isolate the particular node and send out warnings. ArtChain deploys ledger nodes throughout the primary and secondary art markets, including internet companies, cloud service providers and a large number of collectors of works of art and artists, which, from a probability point of view, can eliminate the possibilities where the majority of nodes fall under attack or collude to engage in malicious conducts.

Initially, we set up 100 nodes to provide sufficient redundancy and fight against 51% attack. Currently, they are deployed at AWS and Ali cloud and not activate all at the same time. We monitor the nodes behaviour and dynamically replace the crashed nodes. We plan to extend the deployment to be more decentralized on other clouds. In this regard, an important issue to consider is the trade-off between decentralization and performance.

IV. Scalable Blockchain Implementation

In this section, we present the implementation of ArtChain network. We first introduce tokenization and how it works in our system. Then we describe the design and implementation of the upgradable smart contract for the purpose of improving function and fixing bugs. Finally, we discuss how to preserve privacy and confidentiality as required by regulations and business needs.

A. Tokenizaiton

Tokenization refers to converting an asset into a digital token on the blockchain system, so that ownership of the asset can be transferred via smart contracts. Smart contracts have functions for automatic transactions, formulas for calculating asset prices and other specific features [9], [10]. Tokenization is not simply the creation of a token. Instead, it is about the design of the whole system, including understanding the various rights and issues.

There are two types of token in ArtChain: the security token ACG[2] and the utility token ACGT.

ACG token comes with the essential technical features of digital currencies, including a steady issue curve, free trading, immunity to double-spending attacks, and traceable transaction history. These features are secured through the ledger architecture and smart contracts. We develop relevant E-wallets for corporate or institutional users, which incorporate all essential functions for interactions with the applications on ArtChain.

ACG token provides incentives for maintaining the ArtChain network and the ecosystem of ArtChain applications.

- *Network Maintenance:* the consistency of ArtChain network is jointly assured by ledger nodes. Ledger nodes will have the opportunity to be awarded with ACG as block rewards and transaction fees, to encourage them to contribute to the security and stability of the ArtChain network.
- *Ecosystem of Applications:* ArtChain will award users with newly added ACG in positive correlation within a certain cycle based on a number of indicators such as their frequency of interaction with the ArtChain ecosystem, levels of contribution, influence and the number of ACG coins they hold. All indicators of ecosystem incentives are quantifiable and verifiable, which are collected and calculated by ledger nodes. Incentives will be allocated under *Proof of Interaction* (POI) agreements.

The ratio of the incentives for ArtChain network maintenance and the incentives for the ecosystem of ArtChain applications will be dynamically adjusted by using a negative feedback mechanism to maintain the balance and stability of the ArtChain network and the ecosystem of applications. The specific indicators and algorithms will be published before any main relevant applications go online, and will be implemented and operated through open rules of contracts. Relevant institutional users of the ecosystem (art galleries, museums, auction houses and artists) will be consulted.

The utility token ACGT is only used internally to facilitate payment in art trading. It is a kind of stable coins, which are designed to have a stable price or value over a period of time, therefore, less volatile. These coins aim to mimic the relative price stability of fiat currencies on one hand, but keep the core values of cryptocurrencies such as decentralization and security, on the other hand. Each ACGT token is collateralized by an equal amount of fiat currency (1 AUD) held by

[2]https://etherscan.io/token/0x984c134a8809571993fd1573fb99f06dc61e216f

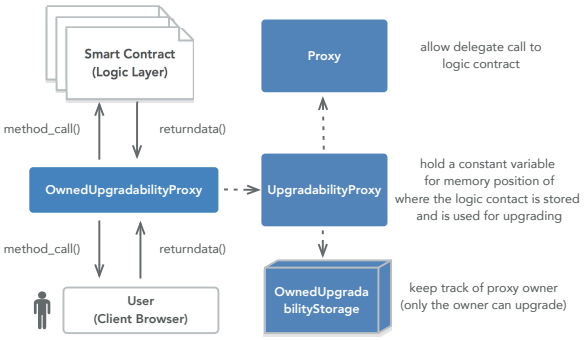

Figure 6. Zepplin proxy architecture pattern

a central custodian. Holders are guaranteed to redeem their token at any point for the stable value denominated in fiat.

B. Upgradable Smart Contracts

Smart contract, once deployed into the blockchain, is immutable literally. In consideration of bug fix and function improvement, lots of work has been done to propose an upgradeable design pattern of the smart contract [11].

The typical methods include:

- Separate logic and data
- Partially upgradable smart contracts system
- Separate logic and data in key-value pairs.
- Eternal storage with proxy contract

Among these methods, the proxy mechanism is most flexible and guarantees a 100% upgradable mechanism i.e., the logic could be completely modified while remaining the existing data state. In our system, we refer to Zeppelin's proxy patterns [12] and implement the so-called Unstructured Storage Pattern. The contract structure is shown in Fig 6.

By using this pattern, the system achieves following features:

- General user is unaware about upgrade of the contract.
- Implementation of logic contract is 100% upgradable.
- Data is stored in proxy contract. New data fields could be added by the upgraded logic contract, without touching existing data structure.

This design has also been chosen for the ZeppelinOS smart contract system, and gone through a full security audit.

C. Initializing Issue

In our implementation, we also address the initializing issue. This is a long-standing problem of upgradability solutions for Ethereum. Our aim is to create an upgradable logic contract, and we practically deploy a proxy contract which delegates to a pre-existing deployment of logic contract on the blockchain. Therefore the proxy contract has no chance to establish the initializing steps in the constructor of logic contract, and thus we need to do something special in order to correctly initialize the proxy contract.

Our workaround for it is to use an initializer function instead of the constructor, and make sure it is only executed once for a necessary initializing process. Other proposals could be found as Initializer Contracts [13] [14].

D. Safety Control

Transaction security: ArtChain network assures the security of users' accounts and funds by using blockchain consensus, digital signatures and end-users encrypted wallets. The artwork trading platform provides security services that are likened to those offered by financial institutions. It integrates data, applications and transactions in blockchain clouds through the efficient integration of data storage, network and other resources, so as to create a secure transaction environment.

Financial Management: ArtChain maintains high standards of integrity and ethical business conduct and is in compliance with relevant laws and regulations, as well as self-regulatory principles of the industry. We also implement a component to conduct the regulatory duty of Know-You-Customer (KYC).

E. Privacy and Confidentiality

ArtChain makes public all ledger nodes and their state in the network in real time. The transaction history (block content) and state information in ArtChain are publicly visible. However, in case of any privacy requirements for some transactions, such privacy information will be processed.

In the data model design, we carefully decide what data to be stored on-chain and what off-chain. The design has been evolved along business needs and regulatory needs. Currently, the on-chain data store contains information on artist, the hash of ownership, price, and history. The hash of ownership protects the privacy for owners who do not want to be known to the public, as well as in compliance with privacy regulations, such as the General Data Protection Regulation (GDPR)[3].

V. Performance Evaluation

We conduct an extensive performance testing of the system. We identify that the performance bottleneck of the system is the low-level I/O efficiency of the Ethereum client, i.e. Geth[4] in our system.

ArtChain private chain, based on POA consensus and 5-second block interval and deployed on 6 cloud nodes (8x2.5GHz CPUs, 32G memory), supports up to 1500 TPS, i.e., 1500 raw transactions on the chain, far more superior to Ethereum mainnet (about 15 TPS nowadays). Integrated user actions, like post new artwork or top up tokens, are usually comprised of a series of transactions/queries on the chain. ArtChain on average processes about 40-70 user actions per second.

[3]https://eugdpr.org/
[4]https://geth.ethereum.org/

A. Environment Setup

The private chain is composed of 3 Ali cloud servers (8x 2.5GHz CPUs, 32GB memory, 64GB hard disc), and 3 AWS cloud servers (8x 2.5GHz CPUs, 32GB memory, 8GB hard disc). Geth version 1.8.17, startup parameter is tuned as:

- --targetgaslimit 4294967295: increase the gas limit to 0xFFFFFFFF to seal as many transactions as in one block. Note this need to coordinate with the gasLimit in the genesis.json file when creating the chain.
- --txpool.lifetime 24h --txpool.accountslots 65536 --txpool.globalslots 65536 --txpool.accountqueue 64 --txpool.globalqueue 65536: increase $txpool$ so that it stores as many transactions both account specifically and globally as we submitted.

This paper employ web3.js[5] to communicate with the chain, and to monitor its performance, Wireshark[6] is applied to capture packet for analysis.

B. Throughput Analysis

Basically, blockchain throughput is limited by: a) How long it needs to generate a block, and b) How many transactions can be sealed in a block. And theoretical throughput = (number of transactions in a block)/(block interval). But in a large-scale network, the throughput is also restricted by the broadcast speed. An explicit example is Ethereum mainnet, with network congestion, its throughput dramatically degrades as nodes need more time to keep synchronized. This is why Ethereum is considered to have issues on network scalability.

As for our private chain, we tried following steps to tune up the system performance: (1) Speed up the block generation by changing the block interval when generating the $genesis.json$. To summary, the chain with 1-second interval shows the best performance, but 5-second is also acceptable. (2) Improve the gas limit of the chain. It does not shows significant improvement on the performance, because the gas limit is not the bottleneck of the system.

As our chain is only maintained by 6 cloud servers, we can ignore the effect of network scalability mentioned above. As long as the transactions are sealed, the nodes always have adequate time to keep sync. On the contrary, it is the node's hardware configuration that determines the system performance. We observe frequently crash of Geth client on the node with only 8GB memory originally. Using the node with 32GB memory, the performance is significantly improved, but the crash still occurs in certain scenarios.

Geth is thought as a memory monster whose design follows a "I use up what I have" idea, and will use up all available memory on the server. By default, our node servers disable the swap and will kill Geth process if it tries to use up the memory. Unfortunately, this always occurs. We observed it used up 8Gb memory when trying to create 70 new accounts. A suggestion is to enable the swap on the node, in terms of the sacrifice of the performance. Note the AWS cloud server has only 8GB disc space, and so the swap space is restricted on AWS servers.

[5]https://web3js.readthedocs.io/en/1.0/

[6]https://www.wireshark.org/

C. Test Results

1) Raw transaction test: The chain is configured with 5-second block interval and we get that (1) Transaction carries data of 50 bytes, it is a typical value for general transactions. (2) Establishes 2000 transactions in about 6-8 seconds per node. (3) Establishes 20000 general transaction queries in 2-5 seconds per node.

2) API based test: APIs such as $check\_user()$, $check\_transaction()$ and $check\_artwork()$ only query information from the chain and do not include any practical transactions. So they show as high throughput as general queries. It only depends on the processor and network performance. APIs such as $buy\_tokens()$, $post\_new\_artworks()$ and $freeze\_tokens()$ combine a series of queries and transactions, and these operations usually depend on the result of the precedent, so those APIs have bad parallel performance. For example, $post\_new\_artwork$ includes 16 low-level operations:

- 2x eth.sendTransaction
- 1x personal.unlockAccount
- 1x eth.estimatesGas
- 2x eth.gasPrice
- 6x eth.getTransactionReceipt
- 2x eth.subscribe
- 2x eth.unsubscribe

Some test results are listed below:

- Establish 116 times API $post\_new\_artworks()$ within about 18-20 seconds per node.
- Establish 58 times API $buy\_tokens()$ within about 5-6 seconds per node.

API $add\_new\_user()$ contains a low-level operation of $personal.newAccount$, which uses significant memory and CPU cycles. A typical result is listed below:

- Establish 64 times API $add\_new\_user()$ within about 20 seconds per node.

3) Test on different block interval: We tested on different block intervals of 1 second, 2 seconds, 5 seconds and 15 seconds. The comparison of API based throughput with different block intervals is summarized in Figure 7.

As all the APIs are called at the same time during the test, we observe actually all transactions are sealed in one block. Our chain is fully capable of guarantee that. So besides the block interval difference, those calling procedures need almost the same processing time on the network and processes. That is why the different block interval practically results in different throughput.

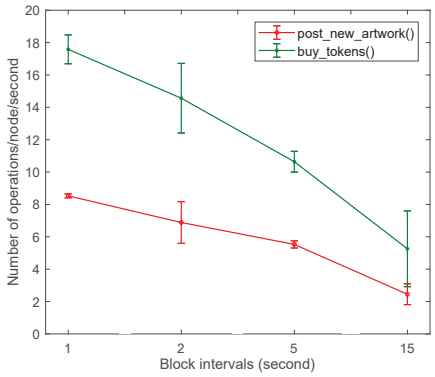

Figure 7. Test under different block interval

4) Test on node crash: Geth client crashes under certain scenarios. What we notice is that transactions like $personal.newAccount$(included in API $add\_new\_user()$) make Geth consume lots of memory. Got in tests:

- On the node configured with 32GB memory, Geth could support up to 70 concurrent $add\_new\_user()$ calls.
- Geth crash when submitting more than 70 $add\_new\_user()$ calls. It is killed by OS after using up all 8GB memory.

We then try to enable 32GB swap on the server, and find that Geth succeeds processing 96 concurrent $add\_new\_user()$ calls. During the process, it used up 32GB physical memory, and then 9.1GB swap memory. As a result, it uses as long as 914 seconds to establish all the calls. As a comparison, it needs only about 20 seconds for 64 calls without using swap memory. Performance degradation is obvious.

D. Bottleneck of the System

Based on our performance test, we find out that: (1) The performance bottleneck of our system is at the Geth IO execution. (2) The way to improve the system performance is to improve node hardware configuration.

According to [15], Ethereum uses LevelDB as the database to store key/value. The key to accessing database is irregular on account of the discreteness of hash. The LevelDB has an excellent performance in reading/writing continuously, while bad for the random key. Therefore, the time t for accessing LevelDB would be longer as the amount of data storage increases. In fact, the test results show that if n is large enough, the value of t will increase and the eciency will degrade largely for some data which not hit LevelDB cache at times.

Geth consumes huge memory on certain transactions, e.g., $personal.newAccount$, and will crash when receiving multiple concurrent memory-consuming transactions. A suggestion is to enable swap memory on the node to improve system stability, at the sacrifice of the performance (See performance degradation when memory is swapped). We suggest 4GB of swap space on the nodes, based on the performance test result. This improves the system stability and does not degrade the performance significantly.

VI. Related Work

In this section, we mainly review the work that closely related to this work, for more work about blockchain and the related applications, please refer to [1], [16].

Art as Digital Assets: Arts can be regarded as the digital asset to be stored on the blockchain platform. The blockchain inherently holds the property of authenticity, traceability, and irreversibility which can perfectly protect the digital assets for each masterpiece. Usually, the blockchain-based solution marks each masterpiece with an ID, may denote as token in smart contract. Similarly, many protocols are designed to trade the nonfinancial assets in form of tokens on the blockchain platform

Blockchain Solution: Since digital assets need properties both on authenticity and security, blockchain becomes the primary selection for the requirements. There are three options, including private blockchain, consortium blockchain and public blockchain. Due to the high security of the assets, the most suitable solution is the consortium methods, which relatively has a better trade-off between performance and security. The asset-based property is deployed on the application-layer of the blockchain, regulated by the rules defined in smart contract. There are plenty of applications successfully executed on top of blockchain [17] and subsequently the infrastructure [18] becomes more complete along with the development. Our solution provides a trading infrastructure for art, and it provides an paradigm for other high value commodities.

Privacy Protection: For the precious digital art assets, it is fundamental to protect the privacy of assets. There are two kinds of privacy in research, including identity privacy and transaction privacy. Identity privacy publicly links the real identity and transaction scripts, and there are several behavioral analysis strategies, including anti-money laundering and know your customer (KYC) to present the usage graph. Transaction privacy means the plain contents on the ledger, including the plain transferring value, account direction, and so on. Some adversaries may draw attentions to watch even monitor some accounts with huge amounts of property. Furthermore, there are several methods to achieve the high level protected blockchain. [19] employed the mixer to obfuscate the relationships among people. Maxwell proposed the Confidential Transaction and firstly achieved the implemented with the range proof scheme. [20] [21] finished the privacy preservation protocols based on ring signature. [22] sealed the plain amounts by using Paillier cryptosystem. [23] provides a complete solution to make the sensitive information unreadable for the public. Our

system relies on the original chain security and provides protection on the layer of web servers and back-end. This design decision comprehensively considers the performance and security for the whole integrated system as a trade-off.

VII. Conclusions

In this paper, we presented the ArtChain, which is an platform designed with registration, tracking, protection, and provenance for artworks enabled by blockchain technology. We also discussed how to design, implement and deploy the blockchain platform in operation as a working product in practice. The proposed blockchain implementation and Experimental results showed that our system towards artworks can provide a complete blockchain-based solution with the property of irreversibility, authentication, traceability and transparency.

In future, we plan to work on anti-counterfeiting for the original works of art by integrating with the smart modules of IoT, and activating relevant smart hardware and other functionality (e.g. positioning/location tracking) as required by artists or collectors.

References

[1] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[2] F. Yiannas, "A new era of food transparency powered by blockchain," *Innovations: Technology, Governance, Globalization*, vol. 12, no. 1-2, pp. 46–56, 2018.

[3] Z. Wang, D. Y. Liffman, D. Karunamoorthy, and E. Abebe, "Distributed ledger technology for document and workflow management in trade and logistics," in *Proceedings of the 27th ACM International Conference on Information and Knowledge Management*. ACM, 2018, pp. 1895–1898.

[4] M. Zeilinger, "Digital art as monetised graphics: Enforcing intellectual property on the blockchain," *Philosophy & Technology*, vol. 31, no. 1, pp. 15–41, 2018.

[5] M. McConaghy, G. McMullen, G. Parry, T. McConaghy, and D. Holtzman, "Visibility and digital art: blockchain as an ownership layer on the internet," *Strategic Change*, vol. 26, no. 5, pp. 461–470, 2017.

[6] L. Lotti, "Contemporary art, capitalization and the blockchain: On the autonomy and automation of arts value," *Finance and Society*, vol. 2, no. 2, pp. 96–110, 2016.

[7] A. Whitaker, "Artist as owner not guarantor: The art market from the artists point of view," *Visual Resources*, vol. 34, no. 1-2, pp. 48–64, 2018.

[8] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Pbft vs proof-of-authority: applying the cap theorem to permissioned blockchain," 2018.

[9] M. Utz, S. Albrecht, T. Zoerner, and J. Strüker, "Blockchain-based management of shared energy assets using a smart contract ecosystem," in *International Conference on Business Information Systems*. Springer, 2018, pp. 217–222.

[10] G. Blossey, J. Eisenhardt, and G. Hahn, "Blockchain technology in supply chain management: An application perspective," in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.

[11] J. Tanner, "Summary of ethereum upgradeable smart contract rd," https://blog.indorse.io/ethereum-upgradeable-smart-contract-strategies-456350d0557c, accessed: 2018-11-30.

[12] S. Palladino, "The parity wallet hack explained," *July-2017.[Online]. Available: https://blog. zeppelin. solutions/on-the-parity-wallet-multisig-hack-405a8c12e8f7*, 2017.

[13] T. Wang, "A unified analytical framework for trustable machine learning and automation running with blockchain," in *2018 IEEE International Conference on Big Data (Big Data)*. IEEE, 2018, pp. 4974–4983.

[14] K. L. Brousmiche, A. Durand, T. Heno, C. Poulain, A. Dalmieres, and E. B. Hamida, "Hybrid cryptographic protocol for secure vehicle data sharing over a consortium blockchain," in *To appear in Proceedings of IEEE Blockchain 2018*, 2018.

[15] H. Zhang, C. Jin, and H. Cui, "A method to predict the performance and storage of executing contract for ethereum consortium-blockchain," in *International Conference on Blockchain*. Springer, 2018, pp. 63–74.

[16] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges." *IJ Network Security*, vol. 19, no. 5, pp. 653–659, 2017.

[17] B. Qin, J. Huang, Q. Wang, X. Luo, B. Liang, and W. Shi, "Cecoin: A decentralized pki mitigating mitm attacks," *Future Generation Computer Systems*, 2017.

[18] M. Wang, Q. Wu, B. Qin, Q. Wang, J. Liu, and Z. Guan, "Lightweight and manageable digital evidence preservation system on bitcoin," *Journal of Computer Science and Technology*, vol. 33, no. 3, pp. 568–586, 2018.

[19] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[20] S. Noether, A. Mackenzie *et al.*, "Ring confidential transactions," *Ledger*, vol. 1, pp. 1–18, 2016.

[21] S.-F. Sun, M. H. Au, J. K. Liu, and T. H. Yuen, "Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero," in *European Symposium on Research in Computer Security*. Springer, 2017, pp. 456–474.

[22] Q. Wang, B. Qin, J. Hu, and F. Xiao, "Preserving transaction privacy in bitcoin," *Future Generation Computer Systems*, 2017.

[23] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *2014 IEEE Symposium on Security and Privacy*. IEEE, 2014, pp. 459–474.