International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-12, Special Issue-1, March-2024
https://doi.org/10.55524/CSISTW.2024.12.1.42
Computing for Sustainable Innovation: Shaping Tomorrow's World (CSISTW-2024) on 16th-17th February, 2024
Organized by B.N. College of Engineering and Technology, Lucknow, India

Platform for Art Marketplace Utilizing Blockchain Technology

Sakshi Srivastava[1], and Chhavi Bajpai[2]

[1,2]Assistant Professor, Department of Computer Science and Engineering, B.N. College of Engineering and Technology Lucknow, Uttar Pradesh, India

Correspondence should be addressed to Sakshi Srivastava ; sakshisrivastav33@gmail.com

ABSTRACT- Blockchain is a new technology that has the power to transform international trade and build dependable connections inside multi-party networks of business. There are several real-world applications for blockchain technology. One particular sector where it fits very well with the way art forensics and transactions are carried out, monitored, and documented is the art industry. This inspires us to continue building the ArtChain platform in order to support the art industry. We introduce ArtChain, an integrated trade system built on blockchain technology, in this article. From bottom to top, it consists of the deployment scripts, the front end, the back end, the services, the smart contract, and the chain connection. To the best of our knowledge, this is Australia's first blockchain-enabled art trade platform. For the purpose of art asset registration, provenance, and traceability, it offers a transparent, privacy-preserving, and tamper-proof transaction history. Our unbiased examination and assessment demonstrate the applicability and usefulness of the ArtChain platform.

KEYWORD-Art,Blockchain, Technology.

I. INTRODUCTION

Blockchain technology, commonly referred to as distributed ledger technology [1], is intended to facilitate verification-driven transaction services in an ecosystem that is typically untrusted. Because of the way blockchain technology is designed, data kept on the ledger cannot be changed, removed, or even added by one corporate entity without the approval of all other network users. This Technology is currently being used in a number of industry applications, including documentation and cross-organization workflow management in commerce and logistics [3], as well as blockchain-enabled traceability and provenance for food safety [2]. The art market is one of the biggest unregulated industries in the world, with $200 billion in annual transactions. It is responsible for one-third of all crimes, second only to drug and weapons sales [4]. Transparency and paperwork are lacking or nonexistent when tens of millions of dollars are exchanged. The art market currently faces the following difficulties and challenges: (1) lack of transparency regarding prices and provenance, as well as inadequate control over transaction data due to information asymmetry; (2) difficultness in determining the authenticity and appraisal of high-value artworks; (3) lack of transparency regarding the value of artworks at the primary art market and trading at the secondary auction market (both online and offline); (4) lack of recognition,public awareness and support for a significant number of artists;(5) it is challenging for the artists to receive royalties from the secondary market. Because of its intrinsic qualities, blockchain technology is ideally suited to increase transparency, maintain records, and decrease criminal activity in the stock market.[5][6].This article presents our project, Art Chain is a functioning product that is built on blockchain technology and has undergone testing. It is anticipated that by developing a new ecosystem for trading, transferring, and art keeping, it will offer a comprehensive response to these problems. Art Chain essentially strengthens the blockchain's foundational architecture to enable a trading platform for art assets at the commercial level. The platform's primary value proposition is found in:
Protection of Privacy A shared ledger and permissioned control system guarantee the transparency of every transaction, protecting privacy in the provenance and exchange of art.The ability to trace The blockchain ledger in conjunction with Counterfeit artwork is lessened with the use of individual artwork tracking in real-time. The inability to reverse An unchangeable digital record of the artwork is produced by registration of collectors' offline assets, which ensures the authenticity, origin, and worth of the artwork.Openness putting artwork on public exhibit for a larger group of knowledgeable investors while taking advantage of the open nature of the art world.

II. BLOCK CHAIN SOLUTION FOR ART TRADING

A.This section begins with the justification for using blockchain technology in an art marketplace, followed by a discussion of the advantages of this platform. Justification for Using Blockchain B. The following is a description of the main players or entities in our solution.•Artiste Both seasoned and up-and-coming artists have equal chances to have their works professionally evaluated and published. Tradeable items will be offered for publication. Galleries of art With the ability to track and find artwork in real time when it is registered on the blockchain, galleries can feel even more secure.

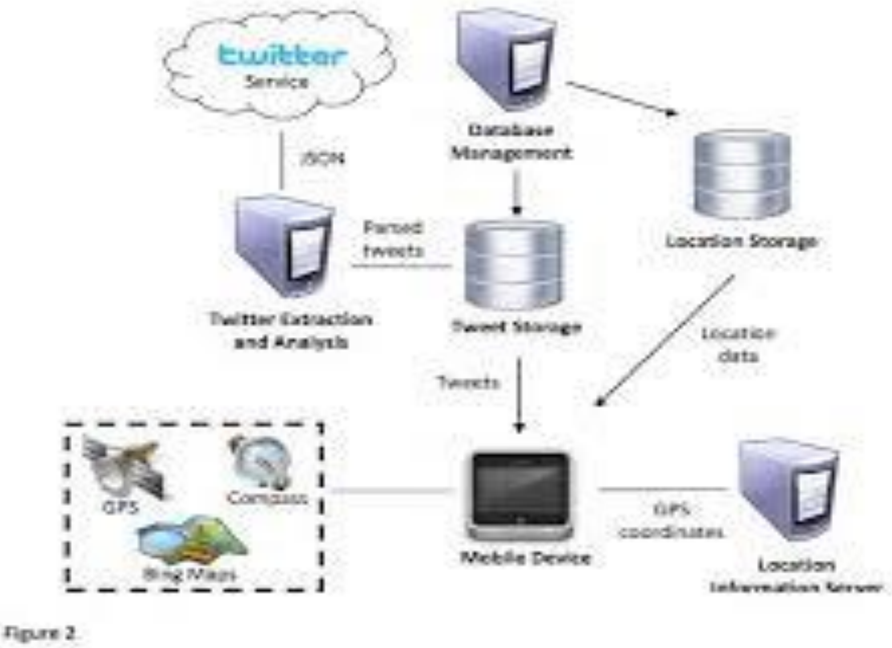

Figure 1: Architecture of System

- Auction house block chain**:** stored data can be synchronized with auction houses, creating new avenues for increased world level audience engagement. More traffic means more chances for all parties.
- gatherer online synchronization of offline art assets owned by collectors. This establishes ownership and safeguards the artworks' legacy for upcoming generations, guaranteeing that their worth will be maintained. Access to a global database featuring a wide range of filtering options.

- ***Advantages of a Blockchain-Powered Art Marketplace:***

First of all, it is easy to obtain traceable data and authentic artwork. When it comes to collecting art, provenance is quite important. Since it is common to suspect that a masterpiece may have been stolen or faked, a distributed ledger can be used to track the ownership transfer over time and act as a decentralized database protecting provenance information and other crucial details pertaining to artworks. This makes it possible to transfer ownership in trading quickly and unquestionably.Second, it is possible to obtain royalty payments for artists from the secondary market. Visual artists will receive a royalty of 5% on select commercial sales of their creations. The Resale Royalty Right for Visual Artists Act of 2009 established this entitlement. However, artists frequently do not receive the royalties since it is difficult to track resales in the present art market [7].Thirdly, the blockchain audit trail facilitates the identification of money laundering and tax evasion. Based on transparently provided data, add-on analytics or artificial intelligence services can estimate the current value of an artwork. Due to a lack of market history, primary market valuation is more challenging and speculative than secondary market valuation. This helps.Moreover, our system is intended to develop into an extensible, open infrastructure focused on the art sector. This implies that attendees will have the chance to build a wide range of art-related apps based on the principles of ArtChain for certain use cases.

III. OVERVIEW OF SYSTEM

A. This section begins by outlining the high-level architecture's primary components as well as the fundamental ideas around which it is built. Next, we describe the platform's trading procedure and the fundamental data model design. We also talk about the problems with security and trust.

- ***Advanced Architechture 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 Hyper ledger 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.We have chosen to implement a micro services architecture for the following advantages: (1) Facilitates rapid parallel development of different components within the application ecosystem; (2) Minimizes coordination time between diverse groups working on different components; (3) Offers clean and reusable interfaces when implemented correctly; (4) Minimizes the need for complex interactions between interfaces; (5) Lowers the risk and time involved in integration and chain testing. The architecture design is depicted figure 1.The system is divided into three layers: the trading backend, the user front end, and the Art Chain blockchain layer.

- **User Front End:**

consists of the following features: art Collection display; shopping Cart; user Wallet; managing Profile for user registration, login, and details; and CMS (material Management System) for creating and managing web material.

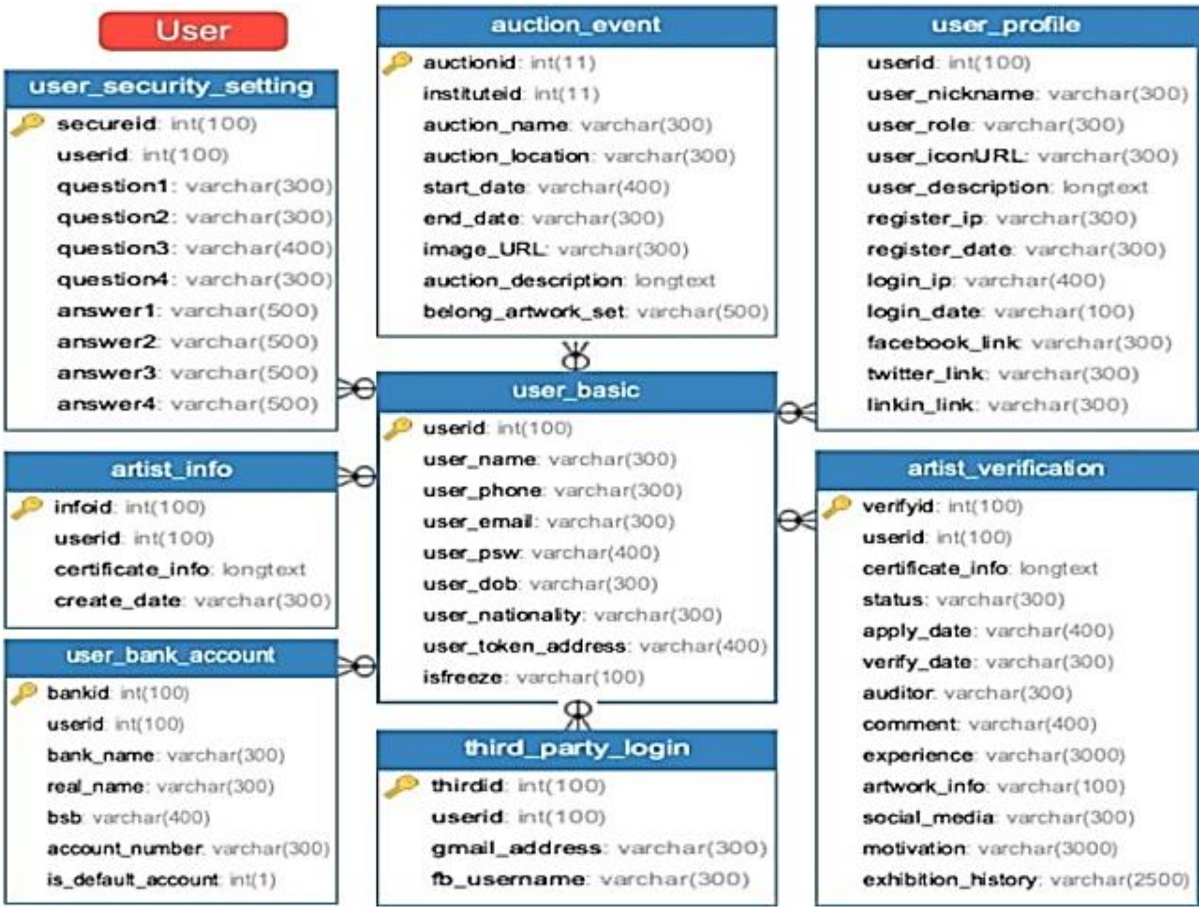

Figure 2: Data Model class of user

- ***Back-end:***

trading includes wallet management, shopping and bidding, and artwork management. Registration of artwork, ownership confirmation, and ownership transfer are all included in artwork management. Through the ArtChain grading system of professional institutions, artists and collectors register their artwork. After that, their artistic creations will be able to trade and interact with the environment.

- ***Art Chain:***

comprising the subsequent elements: (1) Royalty model: accountable for paying artists royalties when their artwork is resold. (2) POI model: oversee agreements for Proof of Interaction (POI), which serve as growth incentives for an ecosystem of applications.

- ***Section IV-A***

provides more information. (3) Rewarding Controller: utilizes the POI model to oversee participant rewards. The information is business-sensitive and outside the purview of this article.

B. The Data Model Design:

The distributed ledger has three main categories of data objects, which are shown as follows:

- ***User:***

includes all data pertaining to a user's wallet, auction events attended, profile, and login. With further details and validation, an artist is also a user. Figure 2b displays the detail, which includes the artwork's features, tag, ownership transfer history, and order details. These classes provide as a representation of the masterpiece's workflow. The specifics can be seen in Figure 3.

- ***Trading:***

Includes an order, the artwork, the buyer's contact details, and the delivery address. Trading Services and Profile Services are activated to retrieve the trade and customer information upon receipt of the user's trading request. Payment Services is in charge of processing payments after verifying the trading conditions. Subsequently, Reward Services is contacted to get and request the reward data. Shipment Services ultimately takes care of the shipment details.

Figure 3: Data Modal Class of art

C. Establishing Trust:

Art Chain collaborates with specialized or well-known players in the primary or secondary art market spaces, such as galleries, museums, and auction houses, to create the initial ledger nodes and offer essential functions like transaction block generation, ordering, and validation. Together, these ledger nodes and additional agent or routing nodes safeguard the blockchain network. We employ Proof-of-Authority (PoA) as the ArtChain network's trust paradigm. Instead of remaining anonymous as in mining-based chains, PoA is well suited to regulated businesses where entities—known as authorities—are in charge of maintaining the network.Well-known museums and art galleries serve as authorities in the ArtChain network to verify the authenticity and determine the value of an artwork for our practical purposes. We refer to them as SuperNode. Supernodes carry out blocking and verifying Any node that tries to participate in malicious behavior or is attacked will be quickly discovered by other nodes in the network as soon as it exhibits odd behavior (such as transmitting illicit transactions, engaging in traffic attacks, and tampering with data). The specific node will be promptly isolated by the network, which will also provide warnings. From a probability standpoint, ArtChain deploys ledger nodes across the primary and secondary art markets, including internet companies, cloud service providers, and a large number of art collectors and artists. This reduces the likelihood that the majority of nodes will be attacked or conspire to engage in malicious activities. In order to defend against a 51% assault and offer adequate redundancy, we initially set up 100 nodes. They are currently installed at Ali Cloud and AWS, and they do not activate simultaneously. We keep an eye on the behavior of the nodes and swap out the crashed nodes on the fly. The deployment will be expanded to be more decentralized on other clouds.

IV. EXTENSIBLE BLOCKCHAIN APPLICATION:

We introduce the ArtChain network's implementation in this part.Tokenization is first introduced, along with how our system uses it. Next, we go over how the upgradeable smart contract was designed and implemented to enhance functionality and address issues. Lastly, we go over maintaining confidentiality and privacy in accordance with legal requirements and commercial requirements.

A. Tokenization

Is the process of turning an asset into a blockchain-based digital token so that smart contracts can be used to transfer ownership of the asset.Smart contracts have features for automated transactions and formulae.for figuring out asset values and other particulars [9, 10]. Making a token is only one aspect of tokenization. Rather, it is about how the entire system is designed, which includes knowing the different rights and problems.In ArtChain, there are two different kinds of tokens: utility tokens and security tokens ACG2.

- **Network Maintenance:**

the consistency of ArtChain net- work 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 with in 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.

To preserve the equilibrium and stability of the ArtChain network and the ecosystem of apps, the ratio of incentives for network maintenance to those for the ecosystem of ArtChain applications will be dynamically adjusted through the use of a negative feedback mechanism. The particular indicators and algorithms will be developed and run via open rules of contracts; they will be made public prior to the launch of any major pertinent apps. Relevant institutional users of the ecosystem (artists, auction houses, museums, and galleries) will be contacted.Only internally, the utility token ACGT is utilized to make art trading payments easier. It is a type of stable coin, meaning that its value or price will remain constant throughout time, making it less volatile. These coins preserve the fundamental characteristics of cryptocurrencies, such as decentralization and security, while also attempting to replicate the relative price stability of fiat currencies.An identical quantity of fiat currency (1 AUD) kept by a central custodian serves as collateral for each ACGT token. It is assured that token holders can exchange their token for fiat money at any time for the steady value.

B. Modifiable Smart Agreements

Once a smart contract is implemented into the blockchain, it cannot be changed in any way. Considerable effort has been put into proposing an upgradeable design pattern of the smart contract, taking bug fixes and functionality enhancements into account [11].

Typical techniques consist of:

- Keep logic and data apart
- A system of partially upgradeable smart contracts
- Keep logic and data apart in key-value pairs.
- Perpetual storage with proxy agreement

The proxy mechanism is the most adaptable of these techniques and ensures a 100% upgradeable system—that is, the logic might be altered entirely without affecting the current data state. We use the so-called Unstructured Storage Pattern in our system and refer to Zeppelin's proxy patterns [12].The following characteristics of the system are made possible by this pattern:

- The contract's upgrading is unknown to the general user.
- The logic contract's implementation is fully upgradeable.

Data is kept in a proxy contract. The updated logic contract could include new data fields without affecting the current data structure.

This architecture has also undergone a thorough security audit and been selected for the Zeppelin OS smart contract system.

C. Starting off Problem

We additionally address the initializing in our implementation. Using an initialize function in place of the constructor and making sure it is only run once for a required initializing process is our fix for it. Initializer Contracts are another source of ideas [13] [14].

D. Safety Management

Transaction security: The blockchain consensus, digital signatures, and end-user encrypted wallets used by the ArtChain network ensure the security of users' accounts and funds. Security services provided by the artwork trading platform are comparable to those provided by financial organizations. Through the effective integration of data storage, networking, and other resources, it merges data, applications, and transactions in blockchain clouds to establish a safe transaction environment.

Financial Management: ArtChain complies with all regulations and upholds high standards of integrity and moral business conduct.

V. SHOWROOM EVALUATION:

We test the system's performance in great detail. We determine that the low-level I/O efficiency of the Ethereum client, or Geth4 in our system, is the system's performance bottleneck.ArtChain Private Chain supports up to 1500 TPS, or 1500 raw transactions on the chain, which is significantly greater than Ethereum Mainnet, which currently only support roughly 15 TPS. It is based on POA consensus and has a 5-second block interval. It is deployed on 6 cloud nodes (8x2.5GHz CPUs, 32G memory). Integrated user actions often consist of a sequence of chain transactions or inquiries, such as posting new artwork or topping up tokens. An average of 40–70 user activities are processed by Art Chain every second.3https://geth.ethereum.org/4https://eugdpr.org

A. Environment Configuration

Three Ali cloud servers (8x 2.5GHz CPUs, 32GB memory, 64GB hard drive) and three AWS cloud servers (8x 2.5GHz CPUs, 32GB memory, 8GB hard drive) make up the private chain. Version 1.8.17, startup parameters adjusted:

• Targetgaslimit 4294967295:

to seal as many transactions as possible in a block, raise the gas limit to 0xFFFFFFFF.When constructing the chain, take note that this needs to work with the gas limit in the genesis.json file.

• Txpool. lifetime

24 hours 65536 --txpool.accountslots --globalslots.txpool.65536, 64 — txpool. accountqueue --txpool. global queue 65536: expand txpool to store the number of transactions we submitted, both worldwide and specifically for each account. In order to monitor the chain's performance, this study uses web3.js5, and Wireshark6 is used to record packets for examination.

B. In-depth Analysis

Essentially, there are two factors that determine blockchain throughput: (1) block generation time; and (2) block sealing capacity. Furthermore, theoretical throughput is equal to (block interval / number of transactions in a block).However, in a large-scale network, the broadcast speed also limits the throughput. An obvious example is the Ethereum mainnet, whose throughput drastically decreases when there is network congestion because it takes longer for nodes to stay synchronized. Ethereum is thought to have network scalability problems as a result.

Regarding our private chain, we attempted to optimize the operation of the system: (1) When creating the genesis.json, alter the block interval to expedite the block generation process. In conclusion, the chain that exhibits the best performance has a 1-second gap, however a 5-second interval is equally suitable. (2) Enhance the chain's gas limit. It is not displayed. We saw that when it attempted to generate 70 new accounts, 8GB of memory was consumed. In terms of performance loss, it is recommended to enable the swap on the node. Keep in mind that the swap space on AWS servers is limited because the cloud server has only 8GB of disc space.

C. Test Outcomes

1. Raw transaction test:

We observe that (1) Transaction carries data of 50 bytes, which is a common value for regular transactions. The chain is configured with a 5-second block interval.

(2) Creates 2000 transactions per node in roughly 6–8 seconds.(3) In 2–5 seconds, each node establishes 20,000 general transaction queries.

2. API-based test:

APIs like check user(), check transaction(), and check artwork() do not include any real-world transactions; instead, they only query data from the chain.As a result, they get a lot of general inquiries.It solely depends on how well the network and processor perform.APIs with functions like buy tokens(), publish new artworks(), and freeze tokens() combine a number of searches and transactions; since these activities typically rely on the outcome of a previous transaction, they perform poorly in parallel. Post-new artwork, for instance, consists of 16 low-level operations:

- 1xpersonal.unlockAccount; 2xeth.sendTransaction; 1xeth.estimatesGas Price: 2xeth; Transaction Receipt: 6xeth; Subscription: 2xeth; Unsubscribe: 2xethThe test findings are listed below:
- Achieve 116 API post new artworks() establishments per node in around 18–20 seconds.
- Created 58 times purchase API C. 58 times API buy tokens() must be established in 5–6 seconds per node.
  A low-level operation of personal. New Account, which requires a substantial amount of memory and CPU cycles, is included in API add new user(). A sample outcome is provided below:
- Create 64 API add new user() calls in approximately 20 seconds for each node.

3. Experiment with various block intervals:

We conducted experiments with block intervals of one, two, five, and fifteen seconds. Every API is recalled simultaneously. We see that, in reality, every transaction is sealed in a single block during the test. That is entirely guaranteed by our chain. With the exception of the block interval difference, the calling procedures need about the same amount of network and process processing time. Because of this, varying block intervals essentially lead to varying throughput.

4. Test for node crashes:

Under certain conditions, the Geth client crashes. We observe that certain transactions, such as private ones. Geth uses a lot of memory since new Account (included in API add new user()) is used. Participated in tests:

- With a 32GB memory configuration, Geth could handle up to 70 concurrent add new user() operations.
- When submitting more than 70 add new user() calls, Geth crashes. After the OS used up all 8GB of RAM, it crashed.

We try to enable 32 GB on the server and discover that Geth is successful in processing 96 concurrent calls to add new users. 32GB of physical memory was consumed during the operation, and afterwards 9.1GB of Swap memory. Consequently, it takes up to 914 seconds to establish the calls. In contrast, 64 calls take just around 20 seconds when swap memory is not used. There is a clear decline in performance.

D. Bottle neck 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 Level DB as the database to store key/ value. The key to accessing database is irregular on account of the discreteness of hash. The Level DB has an excellent performance in reading/writing continuously, while bad for the random key. Therefore, the time t for accessing Level DB would be longer as the amount of data storage increases. Infect , the test results show that if n is large enough, the value of t will increase and the efficiency will degrade largely for some data which not hit Level DB cache at times.Geth consumes huge memory on certain transactions, e.g., personal. New Account, and will crash when receiving multiple concurrent memory-consuming transactions.

4. Test for node crashes:

Under certain conditions, the Geth client crashes. We observe that certain transactions, such as private ones. Geth uses a lot of memory since new Account (included in API add new user()) is used. Participated in tests:

- With a 32GB memory configuration, Geth could handle up to 70 concurrent add new user() operations.
- When submitting more than 70 add new user() calls, Geth crashes. After the OS used up all 8GB of RAM, it crashed. We try to enable 32 GB on the server and discover that Geth is successful in processing 96 concurrent calls to add new users. 32GB of physical memory was consumed during the operation, and afterwards 9.1GB of Swap memory. Consequently, it takes up to 914 seconds to establish the calls. In contrast, 64 calls take just around 20 seconds when swap memory is not used. There is a clear decline in performance .Based on the outcome of the performance test, we recommend 4GB of swap space for each node. This increases system stability without noticeably lowering performance.

VI. LINKED WORK

This section primarily reviews the work that is closely related to this study; for other research on blockchain technology and its uses, see [1], [16].Digital Assets in Art: One could consider the arts to be the digital asset that will be kept on the blockchain. The properties of authenticity, traceability, and irreversibility that the blockchain possesses by nature may completely protect the digital assets for every artwork. The blockchain-based approach often assigns an ID to each work of art, which may be used as a token in a smart contract. In a similar vein, other protocols are made to exchange non-financial items through tokens on the blockchain network.

- **Blockchain Solution:**

Blockchain is the main choice for meeting the requirements because digital assets need to be properly secured and authenticated. Private blockchain, consortium blockchain, and public blockchain are the three alternatives. Owing to the assets' high level of security, consortium solutions are the best option since they offer a better balance between security and performance. The asset-based property is implemented on the blockchain's application layer and is governed by smart contract rules. Many applications have been successfully implemented on top of blockchain [17], and as a result, the infrastructure [18] is growing along with the development. Our approach offers an infrastructure for art trading as well as a model for other valuable commodities.

- **Privacy Protection:**

It is essential to safeguard the privacy of digital assets, especially those that are valuable.Identity privacy and transaction privacy are the two types of privacy that exist in research. The true identity and transaction scripts are publicly linked by identity privacy, and various behavioral analysis techniques, such as know your customer (KYC) and anti-money laundering, are used to display the usage graph. Transaction privacy refers to the unvarnished data on the ledger, such as the unvarnished value transfers, account directions, and so forth. Adversaries possessing vast amounts of property may attract notice and even be monitored. Moreover, there exist other techniques to attain the high-level protected blockchain. [19] used the mixer to hide the connections between individuals. Maxwell first achieved the implementation of the range-proof technique and proposed the Confidential Transaction. The ring signature-based privacy preservation procedures were completed by [20] [21]. [22] used the Parlier crypto system to encrypt the simple amounts.[23] offers a comprehensive way to render the private data unintelligible to the general public. It offers protection at the web server and back-end layers and is based on the original chain security. This design choice carefully weighs the trade-off between the integrated system's overall performance and security.

VII. CONCLUSION

In this study, we introduced the ArtChain, a blockchain-enabled platform that provides provenance, monitoring, protection, and registration for artworks. We also talked about the design, implementation, and deployment of the blockchain platform as a functional product. Our system regarding artworks can give a comprehensive blockchain-based solution with the properties of irreversibility, authentication, traceability, and transparency, as demonstrated by the experimental findings and the proposed blockchain implementation.

In the future, we want to focus on preventing the counterfeiting of original artwork by integrating with IoT smart modules, turning on pertinent smart hardware, and adding additional functionality (such location tracking and positioning) in response to requests from collectors or artists.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest

REFERENCES

[1] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: a survey,” International Journal ofWebandGridServices,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 Knowl- edge 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 B.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.DeAngelis, 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. Stru¨ker, “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,andH.Cui,“Amethodtopredict the performance and storage of executing contract forethereum consortium-blockchain,” in International Conferenceon Blockchain.Springer,2018,pp.63–74.

[16] I.-C. Lin and T.-C. Liao, “A survey of blockchain security issues and challenges.”IJNetworkSecurity,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, anddigitalpseudonyms,”CommunicationsoftheACM,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,andT.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, C.**Tromer**, and M. Virza, “Zerocash: Decentralized anonymous payments from bitcoin,” in 2014 IEEE Symposium on SecurityandPrivacy.IEEE,2014,pp.459–474.