Realizing non-fungible token (NFT) through IBM quantum experience

Preprint · October 2021

DOI: 10.13140/RG.2.2.24920.01288

4 authors, including:

Subhash shankar Pandey
Central University of Jharkhand
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Bikash K. Behera
Bikash's Quantum (OPC) Pvt. Ltd.
183 PUBLICATIONS **1,246** CITATIONS
SEE PROFILE

Realizing non-fungible token (NFT) through IBM quantum experience

Subhash Shankar Pandey[1], Tadasha Dash[2*], Bikash K. Behera[2] and Prasanta K. Panigrahi[2]

[1]Central University of Jharkhand Cheri-Manatu Campus Ranchi-835222.
[2]Department of Physical Sciences, Indian Institute of Science Education and Research Kolkata, Mohanpur 741246, West Bengal, India.

*Corresponding author(s). E-mail(s): tadashadash08@gmail.com;
Contributing authors: subhashshankarpandeyy@gmail.com;
pprasanta@iiserkol.ac.in;

Abstract

In early 2021, non-fungible tokens (NFTs) have garnered incredible investor consideration globally. These non-fungible tokens consolidate the finest characteristics of blockchain technology with non-fungible resources to deliver unique and bona fide tokens, each with distinctive attributes. This paper presents a new protocol for preparing quantum non-fungible tokens where a quantum state representing NFT is mounted on a blockchain instead of physically giving it to the proprietor. We have also thrown light on the proficiency and security subjected to an attack employing a quantum computer. Our protocol has the potential to supplant classical NFT and provide its clients with a more secure and cheaper choice for recognition of their items.

Keywords: Blockchain, Non-fungible token, Proof of stake, IBM Q experience, Quantum state tomography

1 Introduction

Over the years, technology has revolutionized the way people communicate, shop, and pay for goods. Cryptocurrency is a digital asset, has gained massive popularity and trigger multiple projects in several sectors. This is a digital payment system that does not depend on banks or financial institutions to corroborate transactions [1],[2]. It's a peer-to-peer system secured by cryptography, which makes it nearly impossible to spend double. These coins are recorded in digital ledgers, distributed globally can be bought and sold via cryptocurrency exchanges. When you transfer funds, the transactions are registered in a public ledger, and your currency is stored in a digital wallet. Chaum proposed the first electronic cash scheme [3]. While numerous researches have been conducted on the real-world deployment of cryptocurrency, they have seen less functional as they failed to be decentralized. With the invention of Bitcoin[4], the situation has changed drastically.Bitcoin overcomes the problem with introducing distributed digital ledger technology where blocks codify each transaction and multiple blocks connecting each other on distributed ledger form a blockchain [5], [6].
Blockchain, the digital ledger technology, can securely store continuously evolving lists of data records in a decentralized and distributed network [7]. Blockchain technology (BT) promises trustability, auditability, immutability, identification, persistency, credibility, and transparency [8]. Apart from cryptocurrency, blockchain technology has a wide spectrum of applications in financial [9] and social services, risk management [10], healthcare facilities [11], the internet of things (IoT) [12] to public and social services, and so on. A blockchain usually consists of infrastructure, network, proof of stake, data and its applications.There are four kinds of blockchain networks — public, non-public, association and hybrid blockchains. A public blockchain is fully accessible. Anyone with a web and internet will participate in every transaction; however, private blockchain needs permission. One cannot be a part of the chain unless invited by the network directors. A hybrid blockchain combines centralized and decentralized features, and a sidechain may be a designation for a blockchain ledger that runs parallel to a primary blockchain.

Blockchain technology is facing significant problems with quantifiability, efficiency, and property [13, 14]. These have to be corrected if blockchain should become a technology that may be used responsibly. Quantum computing will provide higher implementation elements of blockchain technologies together with cryptocurrencies. Finally, as a result of quantum blockchain has the characteristics of quicker process speed and safer dealings supported quantum mechanics, it will have a vast range of applications and lots of research directions in the future.
The massive popularity of blockchain pave the path for the next iteration of blockchain technology, which garnered incredible investor interest in a brief period is unique digital assets named non-fungible tokens (NFT) [15].A non-fungible token can be characterized as a unit of digital information (token)

put away on a blockchain and is intrinsically not interchangeable with the other unit of the same item. Unlike Bitcoin, where each coin is the same as another, i.e., fungible, NFTs are unique, each one with distinct attributes even though they may look similar. These are a type of cryptographic tokens that are extremely powerful with fundamental properties unique, traceable, rare, programmable, indivisible. NFTs have a wide range of applications in collectibles, gaming, virtual art [16], identity, private equity transactions, and real estate deals [17, 18].The NFT market has gone vertical; in December 2020, the sale of NFTs was estimated at $12 million but blown up to $340 million within a short period of two months in February 2021 [19].

We have presented a protocol for preparing a quantum non-fungible token. Rather than giving the proprietor a physical quantum state representing NFT, we mounted it on a blockchain made utilizing doubly hypergraph states, with the entanglement of the weighted double hypergraph state supplanting the conventional cryptographic hash functions. Our experiment was carried out on a cloud-based quantum computing platform, i.e., IBM Quantum Experience [20], available on the Web. It permits the clients to design and test quantum circuits utilizing an interactive graphical client interface both on a classical computer and quantum processors. IBM tests incorporate quantum cryptography, developing different quantum algorithms and applications [21–23].
Classical NFTs have a few downsides, such as high power consumption for mining and less security since all the classical frameworks are secure due to some puzzles that are hard to fathom. We can address all the issues utilizing quantum physics. Our protocol provides its users with a reliable, cheaper alternative to recognize their products. In order to develop an environmentally friendly, productive protocol, we utilized proof of stake. Our paper is organized in the following manner, sec.2 represents the protocol to create quantum NFT. Security and adequacy of the scheme are examined in sec.3. Experimental realization of our protocol is carried out in sec.4. Sec.5 concludes the paper with possible future directions.

1.1 Proof of Stake

A stake characterizes the esteem or money one tends to wager on a particular outcome, and the strategy is named staking. Proof of stake [24] (POS) may be a category of a mechanism utilized for blockchain. It works by choosing the validators in proportion to their stake within the associated cryptocurrency. We tend to append a blockchain group action to the blockchain itself, so it is frequently recognized. Validators perform this included factor to make it safely. We have proposed a mechanism to prevent a malicious user from being built up by imposing the compulsion that validators ought to have the number of blockchain tokens. It needs potential attackers to accumulate an outsized fraction of the tokens on the blockchain to mount an attack.
A validator stake is outlined by the product of the number of coins with the number of times a single user has controlled them. In layman's dialect, the

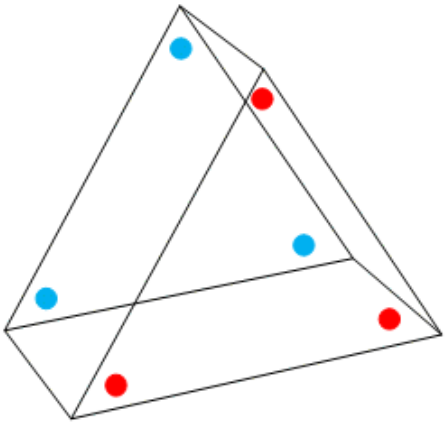

Fig. 1 Representation of entanglement between six qubits double hypergraph state

individual will mine or validate block transactions agreeing to the number of coins they hold. This proposes that the more coins closely held by a miner, the more mining control they have. It is an alternate to Proof of Work (POW) [25], the original consensus algorithm in blockchain technology, to make sure transactions and incorporate new blocks to the chain. For case, Peercoin, Nxt, Blackcoin, and ShadowCoin all work on proof of stake mechanism.
One of the significant advantages of Verification of Stake(POS) [26] is that they are energy efficient. Since all the nodes appear to be not competing against one another to associate a replacement block to the blockchain, energy is spared inside the proof of stake. Moreover, it is decentralized as rewards are proportional to the amount of stake. There is an issue of nothing at stake with this as there is no drawback to the nodes just in case they bolster numerous blockchains in the event of a blockchain split. Hence, each fork can cause multiple blockchains, and validators can work; additionally, the nodes inside the network can never reach a consensus.
To begin with, the operational execution of a proof-of-stake cryptocurrency was Peercoin [27]. There are sporadic proposals for Ethereum to alter from a POW to a POS mechanism.

1.2 Quantum double hypergraph states

Quantum hypergraph states are a collection of profoundly entangled multipartite quantum states built on a mathematical hypergraph. The quantum states are localized on the hypergraph's vertices, with the edges appearing joins to the other qubits, shaping a non separable many-body quantum state. The double hypergraph is comparative to the hypergraph state [28], but each vertex have a parallel vertex shown in fig. 1 . We propose a methodology for creating a fundamentally quantum blockchain, Using the entanglement of such states as a replacement for traditional ledger and hash functions. A fundamental clarification of a hypergraph state is shown below. A comparable quantum state may

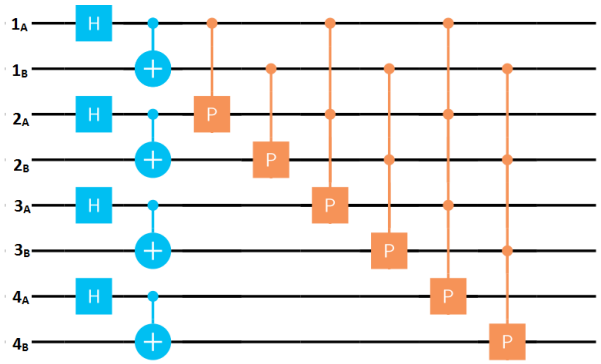

Fig. 2 Circuit to prepare quantum double hypergraph state.

be made from a mathematical hypergraph with k hyperedges (i.e., hyperedges connecting 2k qubits) and n vertices. The hypergraph's number of vertices breaks even with n, the double number of qubits within the quantum framework. All qubits are at first in a pair of bell states. One qubit of the bell state is class A and the second qubit is represented as class B. A controlled-phase operation with a phase angle of $\pi/2$ is then performed on each k-hyperedge of class A and B, shown in fig. 2. A double hypergraph with four vertices 1,2,3,4 where each vertex contains two qubits represented with class A and B. Each qubit of class A and B are entangled in a bell state with each other at their respective vertices. The weighted double hypergraph states can be created by adding phase to each qubit by local operation.

2 Prototype design and development of Quantum NFT

We have proposed a protocol for Quantum non-fungible tokens. Our protocol can potentially replace the classical NFT with the assistance of entanglement of a double-weighted hypergraph state, where the sell-off and statement of the victor can be chosen either classically or with quantum auction protocol. After announcing a victor, we create a token concurring with the agreement; a token has a few random angles. Each block of the blockchain contains two qubits (entangled in bell state) first qubit stores the information of the proprietor and its information, and the second qubit stores the token's data (a token is a few random angles). We utilize the "weights," i.e., the phase carried by the hyperedges of the double-weighted hypergraph state, to encode the classical information. In this protocol, we created a unique, non-fungible quantum token and mounted it on the blockchain [29]. We do not grant any physical state or physical token to the owner; instead, we mount the owner's name or id and the asset's information on the blockchain. The owner is also part of that blockchain. Let us look at each step gradually.

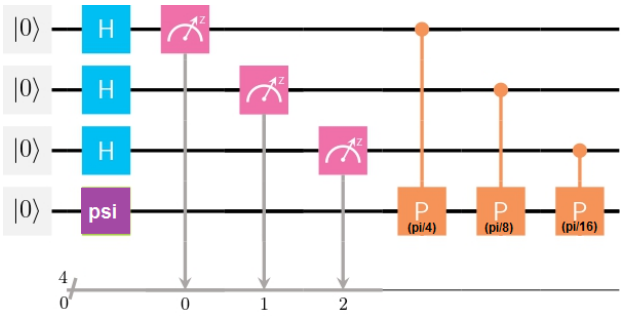

Fig. 3 Circuit to get random phase in q_3 where q_0,q_1 and q_2 is qubit to generate random number.

2.1 Creation of block of NFT

As we know, NFT does not contain any physical data such as painting, video, and photo. It only contains information of owner and art [30] (link of art or name of art). In our protocol, we have taken a bell state such that the first qubit of bell state contains information of owner and art whereas the second qubit stores information of token (token is some random phase). We consider the information as a string of binary which will have a decimal equivalent of p. Two qubits combine to make a peer state defined as $|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ and introduce the relative phase (p-value) of the system as,

$$|\psi_{1A,1B}\rangle = S(p_{1A}) \otimes S(p_{1B}) = \frac{|00\rangle + e^{i(\theta_{1A}+\theta_{1B})}|11\rangle}{\sqrt{2}}. \quad (1)$$

Where θ_{1A} and $\theta_{1B} \in (0, \frac{\pi}{2})$ is a function of P, $f(P)$, any bijective function can be chosen and known to the particular peer who is part of the block, and $\sum_i \theta_{iA} + \theta_{iB}$ and $< \pi \ \forall i$ Here, the number of the block added to the chain is represented by i. Now the state $|\psi_{1A,1B}\rangle$ carries information of owner and art in its first phase (1A) and token in the second phase (1B), this two set of qubits is the peer of the blockchain. There is a mutual agreement upon consensus between the peers.

Likewise, all the peers encode the classical information following the same function added by the first peer. The chosen function can be any bijective function only known to the particular peer in this blockchain. Let us look at the example if we consider our information input as 110 and function is $\theta_i = \frac{1}{2^{i-1}}\theta_1$ here $\theta_1 = \frac{\pi}{4}$ then 110 can be written as $\frac{\pi}{4} + \frac{\pi}{8} + 0$. This is how we can encode the name of owner and info of art. The length of info must be fixed,in our case we fix three digit binary number whose value will be around 50 to 100 to ensure enough space for information.

2.2 Creation of Token

To create a token that is a random and unique phase, we use a Hadamard gate to place a qubit in a superposition of zero and one. After this, we measure

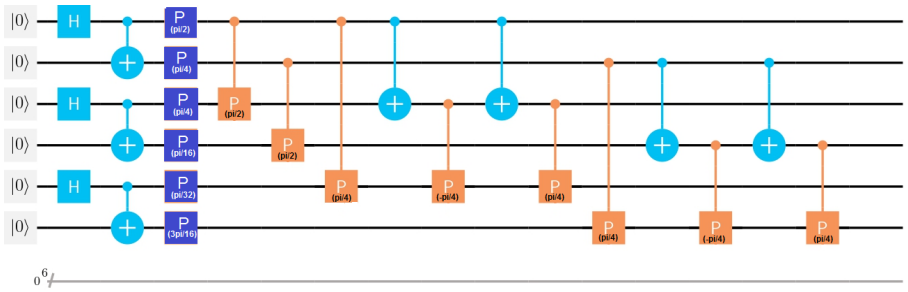

Fig. 4 Circuit for quantum 3-NFT(q_0,q_2 and q_4 carries information of owner and q_1,q_3 and q_5 is Token) prepared in IBM quantum experience(information encoded by applying suitable phase gate.

that qubit. The measurement is purely random zero and one [31] (here, the randomness of this number depends on the laws of physics). Then, depending on the measurement outcome, we apply the phase gate. The angle of the phase gate is decided by a function $\theta_k = \frac{1}{2^{k+i}}\theta_1$, where i is the position of the binary number, and k is the number of peers. In fig 3 we have to generate a random phase for the first peer using only three qubits where $\theta_1 = pi$. The number of Hadamard gates will decide the randomness of the phase. Hence the Hadamard gates must be substantial enough (around 20 to 50) to ensure randomness. Again this function takes care of uniqueness because the phase of the token depends on the number of blocks it belongs to on the chain.

In equation 2 to 5, we show that if we use only three Hadamard gates, then there are eight possible combinations, and for each binary string, we have different phases.

$$|000\rangle = 0 + 0 + 0 = 0 \tag{2}$$

$$|001\rangle = 0 + 0 + \frac{\pi}{4} = \frac{\pi}{4} \tag{3}$$

$$|100\rangle = \frac{\pi}{16} + 0 + 0 = \frac{\pi}{16} \tag{4}$$

$$|110\rangle = \frac{\pi}{16} + \frac{\pi}{8} + 0 = \frac{3\pi}{16} \tag{5}$$

This is how we get a relative random phase. As the number of Hadamard gate increases, the uniqueness of the phase will increase exponentially. If we use about 20 to 50 qubits, it is tough to guess the phase. This consensus will also ensure the randomness as well as the uniqueness of the token.

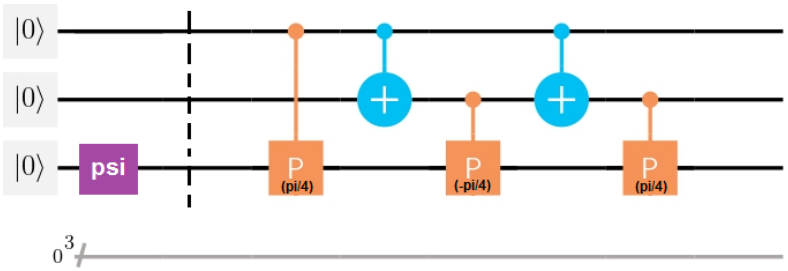

Fig. 5 Circuit for equivalent control control phase gate .

2.3 Verification of the blocks

This step of verification is necessary to ensure that blocks are added according to consensus. The entanglement of double weighted hypergraph state allows us this step of verification, and every block should pass this verification step before adding it into our blockchain. According to our consensus, the peer who creates a token and mounted the owner name with asset sends the copy of the state to all peers and also informs them about relative phase θ_{mA} and θ_{mB}.Now using QKD each peer verifies the state,

$$|\psi_{mA,mB}\rangle = \frac{|00\rangle + e^{i(\theta_{mA}+\theta_{mB})}|11\rangle}{\sqrt{2}}. \tag{6}$$

Where the relative phase should be $\theta_{mA} = (\frac{1}{n^{m-1}})\theta_{1A}$ and $\theta_{mB} = (\frac{1}{n^{m-1}})\theta_{1B}$. He or she conveys a single copy of the state with each peer within the framework. When the peers get the qubit, they measure it on a basis $|\pm_m\rangle = \frac{|00\rangle+e^{i(\theta_{mA}+\theta_{mB})}|11\rangle}{\sqrt{2}}$. In the event that the result of estimation is one, at that point they add the state in their native copy utilizing the $m1$ controlled-P($\frac{\pi}{2}$) gate to each qubit of the block as appeared in fig. 4. The protocol is aborted for the other measurement results, and the peer is designated as untrustworthy as a result. and can be penalized in line with proof of stake.

As we know that in IBM we don't have a control-control phase($\frac{\pi}{2}$) gate but we can apply some equivalent gate that shown in fig 5.

3 Security and Effectiveness

In our protocol, entanglement is used to ensure the security of the blockchain in which QNFT is encoded. Entanglement deals with blockchain security only after the addition of a block in the chain by the peer. The authenticity of the blocks is verified by the process discussed earlier. If the block does not succeed in the verification process, the corresponding peer who creates the block will lose the stake. The amount of stake is much higher than rewording, so the financial motivation will stop peers from doing untruthful work. In our convention, blockchain is represented by the entangled state, data is store in

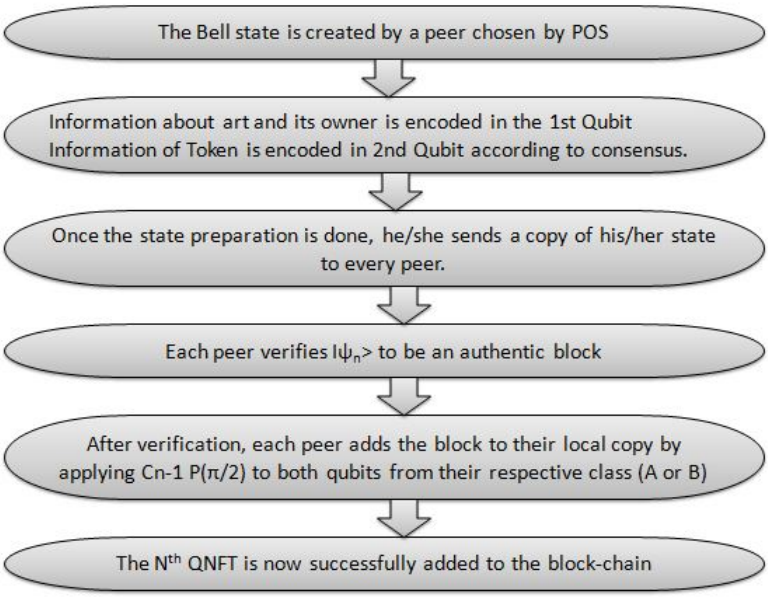

Fig. 6 Flowchart for creation of token and encoded into blockchain.

phase, and there is n copy of the same state shared with n peers. We do not have any public database; only θ_{p1} is shared with the assistance of QKD to all peers. In case we assume Eve altered with data, at that point, we can figure out the block that causes the collapse of the state and the peer whose state was annihilated. Once more, the state can be recouped as he/she knows the particular state without violating the no-cloning hypothesis.

We use the classical threat[32] and risk assessment framework, which considers all elements of a system's security, including originality, integrity, non-repudiability, availability, and accessibility and their Quantum solutions shown in table 1.

3.0.1 Spoofing

Spoofing is the capacity to imitate another entity on the same framework (for case, an individual or a computer), which correlates to genuineness. All data is stored in an entangled state (double hypergraph state), and imitating entanglement is unattainable.

3.0.2 Tampering

Tampering is defined as the malicious alteration of NFT data in order to compromise its integrity. Tampering with information is only possible before

adding it to the blockchain, so all information is shared using QKD to avoid any attack.

3.0.3 Repudiation

The term "repudiation" refers to a situation in which the originator of a statement is incapable of disputing it, which is linked to the security highlight of non-repudiability [33]. To accomplice this, a hostile attacker might steal the hash data, or the hash information could connect with the assailant's address. In our convention, data is put away in a quantum state, and the no-cloning theorem says that cloning a quantum state is impossible, so our NFT is secure from this sort of attack.

3.0.4 Information disclosure

When confidential information is exposed to unapproved users, usually known as information leakage. With our protocol, in the event that an attacker wants to get information, he/she needs to apply a measurement operator that will lead to the collapse of the block and can effortlessly be taken note by the owner.

3.0.5 Tempering with relative phase

In case Eve wants to tamper data with relative phase, he needs to operate unitary phase transformation on qubit he wants to alter. Practically it is too difficult since qubit is in control of peers as each peer has a copy of the entire blockchain. However, in case he some way or another manages to do so, then this is distributed system, so he must alter with all the peers' qubits at the same time. This eavesdropping appears next to impossible for him since each peer applies a control swap operation to check the copy he/she has the same as others in case any peer is found faulty, reconstruction of its state can be done. The system is distributed, so if two or three peers compromised system is still secure, the compromised peer will be caught using control swap operation and rebuild.

The controlled swap operation [34, 35] is used to verify whether two states are the same or not. In this operation we use 3 qubits; q_0 is the test qubit and q_1, and q_2 are $peer_m$ and $peer_n$ respectively. If the test outcome is 0, then the test is successful; otherwise, it fails. With this controlled swap, we can compare two copies of the blockchain. This operation will not work for individual peers. A circuit for control swap test is shown in fig 7.

4 Discussions and evaluation

NFT have a few basic properties, we will discuss about whether our protocol fulfils all those properties or not.

Threat	Classical Security Issues	Quantum Solutions
Spoofing (Authenticity)	Authentication vulnerabilities might be exploited by a hacker. A user's private key might be stolen.	Information is secure with entanglement and tempering with entanglement is not possible
Tampering (Integrity)	Manipulation with data store outside the blockchain is possible.	All the data shared between the peers using QKD is very secure
Repudiation (Non-repudiability)	Binding of hash data with an attacker's address possible.	No cloning theorem says Quantum state can not be clone
Information disclosure (Confidentiality)	To link a particular NFT buyer or seller, an attacker can exploit the hash and transaction.	To exploit information attacker have to measure the state which will cause collapse of state

Table 1 Security issues with classical NFT and their quantum solutions

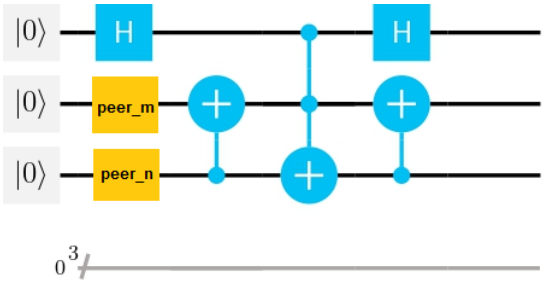

Fig. 7 Control swap test to test peer m and peer n is same or not.

4.0.1 Token has unique identity

A token is some random phase that builds using 200 to 300 qubits if we use only 20 qubits we have phase 1 in around 10 lakhs so it is extremely unlikely to have two tokens have the same phase even in 20 qubits so if we use such a large number it is nearly impossible that two tokens have the same phase, this is how we will ensure the uniqueness of token.

4.0.2 Token must be Non-Fungible

As the token is unique and the name of the owner and art is also attached to it due to this token can not be interchangeable. Non-fungibility does not mean one can not sell the art again rather it tells art is not interchangeable with each other, this is ensured by the uniqueness of token.

4.0.3 Proof of Ownership

The Token is Minted on the Blockchain and can be tracked to give the owner proof of ownership. In Section 2 we addressed in detail how we have added token in our blockchain, One block consists of two qubits. The first qubit stores

the information of the owner and its art, while the second qubit is reserved for tokens. According to our protocol, the owner is part of the blockchain as he/she is a peer of the blockchain. This gives the owner proof of ownership.

4.0.4 Transparent operation.

Each peer has their own copy of the blockchain. All the NFT operations including mounting, purchasing, and selling are open to the public.

4.0.5 Availability, Tamper-resistance and Usability

As NFT is a distributed system, one or two fabrication does not affect the whole system. The system will always be available for the public to use. Entanglement ensures the security of the whole system, so tempering with it is not possible. Each block is instantaneously added to all copies of the blockchain, so each copy of the blockchain is up to date. which makes it user-friendly. We have carried out our experiment on IBM Quantum Experience. In spite of the fact that our protocol is planned for distributed ledger frameworks, we have executed our circuit on the IBM Quantum computer as a proof of concept. A set of circuits that work in like manner to complete our whole protocol. We have illustrated our blockchain circuit, which is a significant and principal portion of our entire protocol. This blockchain circuit is a 4-qubit system that incorporates a large set of quantum gates alongside our group of circuits. It contains two blocks of NFT. We run our circuit on 'IBM Q Casablanca,' a 7-qubit Quantum computer exclusively accessible to premium users. While testing, the most extreme number of shots, i.e., 8192, have been considered. We have gotten a density matrix pretty much closer to the simulated matrix, which once more we get by running our circuit through 100000 shots on the QASM simulator. It gives us a density matrix that is nearly equal to the theoretical density matrix. We have calculated quantum state tomography to discover fidelity between the simulated density matrix and the experimental density matrix. The fidelity of 0.80 is achieved.

4.1 Experimental realization

For our experiment, we have assumed the first block q_0, which holds the information about the owner and asset of the 1st nft, denoted as $\pi/16$. The random token q_1 is also $\pi/16$, and the second block q_2 taken as $\pi/32$, which is carries particulars of the owner and asset of the 2nd nft, random token q_3 is also taken $\pi/32$. All these values are according to the consensus. A city plot is the conventional representation of quantum states, in which the real and imaginary (imag) components of the state matrix are represented like a city. Fig.9 is the state city plot of the simulated density matrix, and fig 12 is the state city plot of the experimental density matrix.
fig 10 and fig 11 is the Hinton representation of simulated and experimental density matrix respectively. The element's size shows the value of the matrix

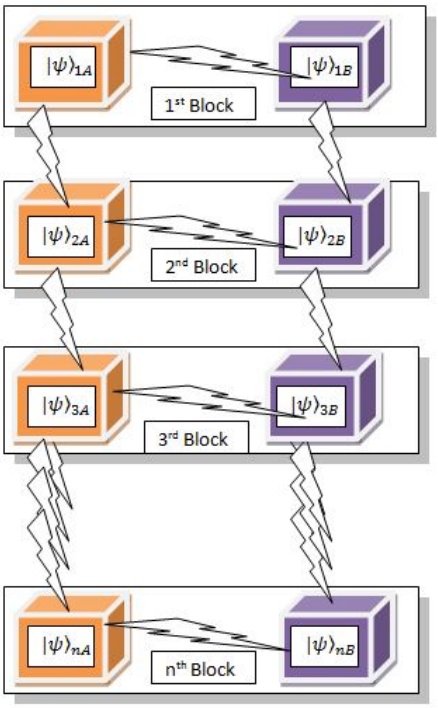

Fig. 8 Animation showing how peer connected to each other.

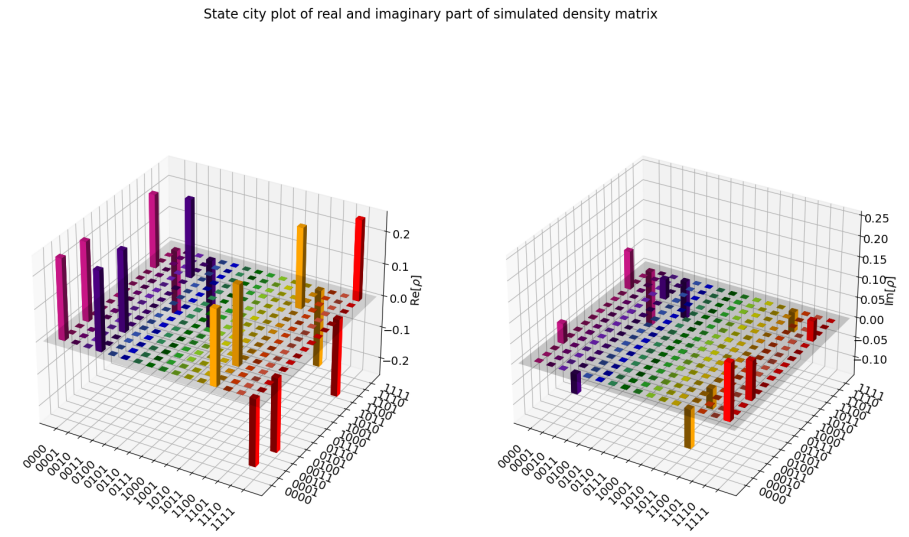

Fig. 9 City plots of real (left) and imaginary (right) parts of a simulated density matrix.

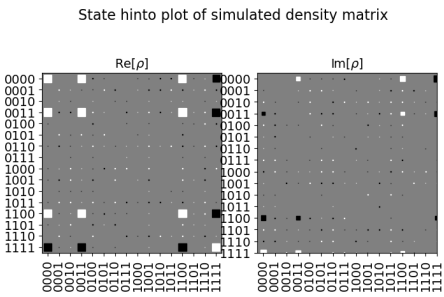

Fig. 10 Hinton plots of real (left) and imaginary (right) parts of a simulated density matrix.

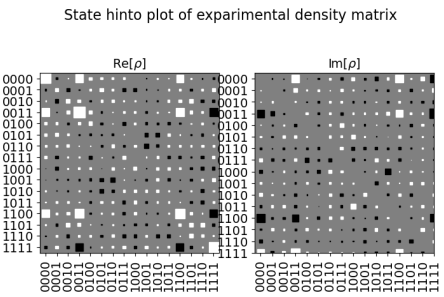

Fig. 11 Hinton plots of real (left) and imaginary (right) parts of a experimental density matrix.

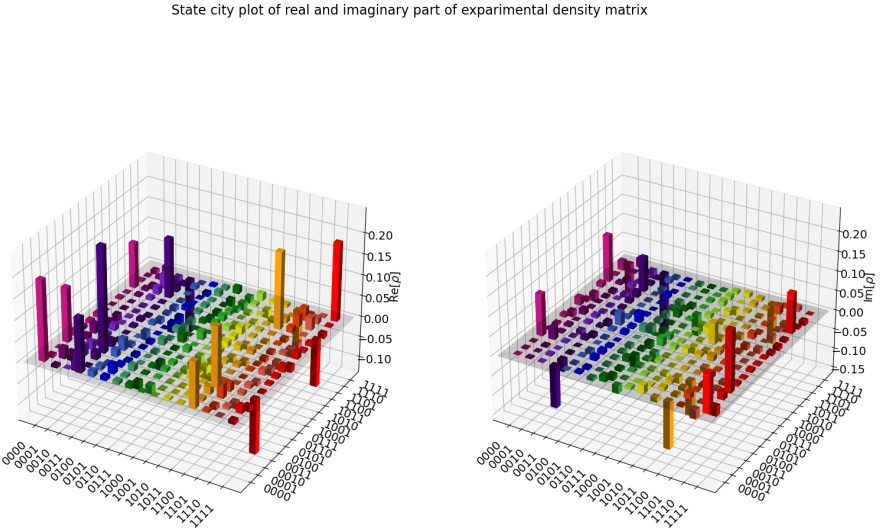

Fig. 12 City plots of real (left) and imaginary (right) parts of a experimental density matrix.

element in a state Hinton plot, which is similar to a city plot.

We have also plotted a blockchain containing three QNFTs, shown in fig 4. For this plot, we assumed the phases as($\pi/2$, $\pi/4$), ($\pi/4$,$\pi/16$) and($\pi/32$, $3\pi/16$) for the first, second, and third block respectively. The first phase of each block is information about the owner and assets, and the second phase of each block is the token. In order to add those blocks into our blockchain, we have to apply the respective control phase ($\theta = \pi/2$) operation. For the second block, we have to apply control phase operation that is directly available on IBM. However, in the third block, we have to apply control-control phase ($\theta = \pi/2$) operation that is not directly available on IBM. So we use the equivalent circuit shown in fig 5. Following the same manner, we can add multiple blocks to this

chain. Fig 8 is an animation showing how blocks are added where the orange color block represents information about the owner and the assets, and the blue color box holds the information about the token lighting symbol that shows entanglement between the blocks.

5 Conclusion

To summarize, We have designed a protocol for preparing a quantum non-fungible token. Rather than giving the owner a physical quantum state representing NFT, we mounted it on a blockchain created utilizing doubly hypergraph states, with the entanglement of the weighted double hypergraph state supplanting the conventional cryptographic hash functions. Our protocol incorporates proof of stake (POS) to end up more effective than proof of work (POW). With POS, a peer is chosen; the same peer is responsible for making fair tokens and sends that token to each peer. After confirmation, each peer will include the new peer in their particular blockchain. In fig. 6 we have appeared a flow chart elaborating step by step process of including QNFT to the blockchain. We have too tossed light on the adequacy and secureness subjected to an attack employing a quantum computer. We put up a quantum blockchain with two blocks on the IBM seven-qubit processor "IBM Q Casablanca," as a proof of concept, the fidelity of 0.80 is achieved.
The application of this protocol is exceptionally noteworthy. This protocol can replace classical NFT and, with the property of quantum physics, NFT proprietors will get a more secure stage for recognizing their assets. Eventually, NFTs pave the way to possibly digitizing the intellectual property rights and tokenizing the resources.

Acknowledgements

S.S.P would like to thank IISER Kolkata for providing hospitality during the course of project work and QUEST(DST/ICPS/QuST/Theme-1/2019/2020-21/01) for financial support. T.D acknowledges financial support by Dept. of Science and Technology, India –INSPIRE Fellowship (IF180118). We would also like to acknowledge the IBMQ Experience, through which all the experimentation has been carried out.

References

[1] Rauchs, M., Hileman, G., et al.: Global cryptocurrency benchmarking study. Cambridge Centre for Alternative Finance Reports (2017)

[2] Liu, Y., Tsyvinski, A.: Risks and returns of cryptocurrency. The Review of Financial Studies **34**(6), 2689–2727 (2021)

[3] Chaum, D.: Blind signatures for untraceable payments (1983). In: Advances in Cryptology (1982)

[4] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260 (2008)

[5] Böhme, R., Christin, N., Edelman, B., Moore, T.: Bitcoin: Economics, technology, and governance. Journal of economic Perspectives **29**(2), 213–38 (2015)

[6] Franco, P.: Understanding Bitcoin: Cryptography, Engineering and Economics. John Wiley & Sons, ??? (2014)

[7] Meng, W., Wang, J., Wang, X., Liu, J., Yu, Z., Li, J., Zhao, Y., Chow, S.S.: Position paper on blockchain technology: Smart contract and applications. In: International Conference on Network and System Security, pp. 474–483 (2018). Springer

[8] Beck, R., Müller-Bloch, C.: Blockchain as radical innovation: a framework for engaging with distributed ledgers as incumbent organization (2017)

[9] Treleaven, P., Brown, R.G., Yang, D.: Blockchain technology in finance. Computer **50**(9), 14–17 (2017)

[10] Fu, Y., Zhu, J.: Big production enterprise supply chain endogenous risk management based on blockchain. IEEE access **7**, 15310–15319 (2019)

[11] McGhin, T., Choo, K.-K.R., Liu, C.Z., He, D.: Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications **135**, 62–75 (2019)

[12] Novo, O.: Blockchain meets iot: An architecture for scalable access management in iot. IEEE Internet of Things Journal **5**(2), 1184–1195 (2018)

[13] Lin, I.-C., Liao, T.-C.: A survey of blockchain security issues and challenges. Int. J. Netw. Secur. **19**(5), 653–659 (2017)

[14] Casino, F., Dasaklis, T.K., Patsakis, C.: A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and informatics **36**, 55–81 (2019)

[15] Dowling, M.: Is non-fungible token pricing driven by cryptocurrencies? Finance Research Letters, 102097 (2021)

[16] Trautman, L.J.: Virtual art and non-fungible tokens. Available at SSRN 3814087 (2021)

[17] Regner, F., Urbach, N., Schweizer, A.: Nfts in practice–non-fungible tokens as core component of a blockchain-based event ticketing application (2019)

[18] Mofokeng, N., Fatima, T.: Future tourism trends: Utilizing non-fungible tokens to aid wildlife conservation. African Journal of Hospitality, Tourism and Leisure **7**(4) (2018)

[19] Chohan, U.W.: Non-fungible tokens: Blockchains, scarcity, and value. Critical Blockchain Research Initiative (CBRI) Working Papers (2021)

[20] Ibm quantum experience. URL: https://quantum-computing.ibm.com/

[21] Linke, N.M., Maslov, D., Roetteler, M., Debnath, S., Figgatt, C., Landsman, K.A., Wright, K., Monroe, C.: Experimental comparison of two quantum computing architectures. Proceedings of the National Academy of Sciences **114**(13), 3305–3310 (2017)

[22] Alvarez-Rodriguez, U., Sanz, M., Lamata, L., Solano, E.: Quantum artificial life in an ibm quantum computer. Scientific reports **8**(1), 1–9 (2018)

[23] Sk, R., Dash, T., Panigrahi, P.K.: Quantum information splitting of an arbitrary three-qubit state by using three sets of ghz states. IET Quantum Communication (2021)

[24] Kiayias, A., Russell, A., David, B., Oliynykov, R.: Ouroboros: A provably secure proof-of-stake blockchain protocol. In: Annual International Cryptology Conference, pp. 357–388 (2017). Springer

[25] Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H., Capkun, S.: On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 3–16 (2016)

[26] Vasin, P.: Blackcoin's proof-of-stake protocol v2. URL: https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper. pdf **71** (2014)

[27] Xue, T., Yuan, Y., Ahmed, Z., Moniz, K., Cao, G., Wang, C.: Proof of contribution: A modification of proof of work to increase mining efficiency. In: 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), vol. 1, pp. 636–644 (2018). IEEE

[28] Rossi, M., Huber, M., Bruß, D., Macchiavello, C.: Quantum hypergraph states. New Journal of Physics **15**(11), 113022 (2013)

[29] Banerjee, S., Mukherjee, A., Panigrahi, P.K.: Quantum blockchain using weighted hypergraph states. Physical Review Research **2**(1), 013322 (2020)

[30] Ante, L.: The non-fungible token (nft) market and its relationship with

bitcoin and ethereum. Available at SSRN 3861106 (2021)

[31] Tamura, K., Shikano, Y.: Quantum random number generation with the superconducting quantum computer ibm 20q tokyo. IACR Cryptol. ePrint Arch. **2020**, 78 (2020)

[32] Shostack, A.: Experiences threat modeling at microsoft. MODSEC@ MoDELS **2008** (2008)

[33] Zhou, J., Gollman, D.: A fair non-repudiation protocol. In: Proceedings 1996 IEEE Symposium on Security and Privacy, pp. 55–61 (1996). IEEE

[34] Moulick, S.R., Panigrahi, P.K.: Quantum cheques. Quantum Information Processing **15**(6), 2475–2486 (2016)

[35] Behera, B.K., Banerjee, A., Panigrahi, P.K.: Experimental realization of quantum cheque using a five-qubit quantum computer. Quantum Information Processing **16**(12), 312 (2017)