Secure NFT Framework For Media Tokens Using Steganography

Preetha S, Arvindh S Kumar, Nishitha B N, Guru Darshan S A
Department of ISE, B.M.S. College of Engineering, VTU, Bengaluru, India

Abstract

Non-Fungible Tokens (NFTs) have advanced significantly and have attracted investor's attention. Non-fungible tokens are also known as crypto collectibles. Analysis of cryptocurrencies and block chain technology recommends the importance and working of non-fungible tokens. Unlike bitcoin, where one coin is the same as another, NFTs are distinctive, each with diverse attributes. NFTs may be sold, gifted, bought, displayed and destroyed. The article provides a detailed understanding of concept, working of non-fungible tokens and its applications. An insight into various pros and cons of non-fungible tokens and viable solutions to some of the major challenges of the application are also discussed. This paper aims to address the security issue of imitation. We have proposed a secured NFT framework for media tokens using steganography.

Keywords: Block chain, cryptocurrency, crypto collectible, Non-Fungible Tokens, NFT, Steganography, Ethereum

I.   INTRODUCTION

In this era of new technologies, add-on is the Block chain technology and Cryptocurrency. In the year 2008 Satoshi Nakamoto developed a protocol for a peer-to-peer electronic cash system. Protocol became the foundation for distributed ledgers called block chains. Block chains laid the foundation for cryptocurrencies. Many cryptocurrencies are decentralized networks based on block chain technology—a distributed ledger enforced by a disparate network of computers. A defining feature of cryptocurrencies is that they are generally not issued by any central authority, rendering them theoretically immune to government interference or manipulation.

The most recent addition to the world of block chain and cryptocurrencies are Non fungible tokens (NFT). NFT is a unit of data stored on a digital ledger called a block chain that certifies a digital asset to be unique and therefore not interchangeable. It is a digital asset that represents real-world objects like art, music, in-game items and videos. They are bought and sold online, frequently with cryptocurrency and they are generally encoded with the same underlying software.

NFTs are changing the digital art platforms. Digital art is at least several decades old but, until recently, has not been collected in the same way as painting or sculpture – partly because it was impossible to distinguish an original from a copy. Now, with the advent of the Non-fungible Token

(NFT), art-world institutions are scrambling to adapt to a new type of transaction that is generating jaw-dropping auction prices.

The forever rose was a crypto art project that was produced by artist Kevin A bosch. It was sold on February 14th, 2018 on the occasion of Valentine's Day to a collective of 10 people for a total of 1 million. The special thing about this project is that the project was paid for in cryptocurrency.

The image is available to everyone on the net and everybody has access to copy or store the image, but the original image carries a certificate of ownership attached to it which makes it unique and this certificate is what makes it unique. Only the 10 members/owners of the image can sell, destroy or exchange their share of ownership. The sale was done and registered on the Ethereum block chain. Ethereum is a technology that lets you send cryptocurrency to anyone for a small fee. This art piece is referred to as a Crypto collectible. These are unique non- fungible digital assets such as art pieces stored on a block chain that is uniquely identifiable.

Crypto Collectible is different from cryptocurrency as cryptocurrency is fungible. A digital currency like bitcoin is equivalent in value to any other bitcoin just like the rupee is equivalent to any other rupee. There is no special value for cryptocurrency like Crypto collectibles as they are not unique and differentiated from one another. Since the images uploaded by artists on the internet could be freely copied, this destroys the notion of ownership to the art piece. Hence, crypto collectibles are required in the field of art as authenticity is an important factor and could be a turning point for the industry.

A comprehensive analysis of cryptocurrencies, block chain technical underpinnings and specifically of Non-Fungible tokens or "crypto collectibles" are discussed. Changes in these innovations can bring about in the art market and creative industries at large. The structure of the study is based on a resource analysis of creative industries, their value chains, various bargaining powers and revenue sharing of the industries' agents.

II.   LITERATURE SURVEY

The scripting language as implemented in Bitcoin has several important limitations such as Lack of Turing-completeness, etc. These limitations are overcome by Ethereum with their intent to merge together and improve upon the concepts of scripting, altcoins and on-chain meta-protocols [1]. Ethereum is open-ended by design, and we believe that it is extremely well-suited to serving as a foundational layer for a very large number of both financial and non-financial protocols in the years to come.

Studies in [2] discusses the impact of the dominance of US digital platforms when compared to European and Asian platforms. There is an in depth analysis of how dominance affects the welfare indirectly.

Bitcoin is a decentralized currency and payment system that eliminates the need for third parties and trusted authorities. This was not openly accepted by all governments naturally. A proper governance structure for Bitcoin can only be achieved by publicly acknowledging its political dimensions, and replacing the current technocratic power structure of the Bitcoin project with an institutional framework capable of understanding the politics inherent in each of its technical features [3].

Energy consumed by mining bitcoin is massive this is because of huge computational power is required to solve the hashes and add transactions onto the block chain. Power required to run these massive mining facilities along with the power needed to maintain the cooling facilities required due to the massive heat output from the mining rigs is excessive. Reaching an average of about 3GW of electricity per month increases as the level of encryption increases in the coming future [4]. Many companies set up their mining facilities in really cold countries to avoid spending cash on the cooling systems. Hence making it cheap and also reduce the pollution emitted from the facility drastically. Rothwell, et al. [5] has discussed on how to monetize software's or services without having to charge premiums for the same.

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without a third party. A new system was proposed in [6] where the usual framework of coins was made from digital signatures. It provided strong control of ownership, but is incomplete without a way to prevent double-spending. A method was proposed for peer-to-peer network using proof-of-work to record a public history of transactions.

Salmon K, et al. [7] elaborated on how cultural and creative sectors have hacked it in the digital age to monetize their efforts. Art can be monetized in multiple ways such as physical form and digital transactions. The study in [8] analyses different value chains for visual arts, performing arts, books, music and so on. The study successfully achieves its objectives by compiling a lot of information on the value chains.

III.   APPLICATION

Non fungible tokens are similar to trump cards, baseball cards, paintings, rare stamps etc. The key characteristic of these tokens are that they are completely unique, cannot be replicated and there can be no copies. 'Non fungible' means cannot be replaced. Hence, the application of block chain is to find a way to digitally store, buy and sell the ownership of these tokens.

Non fungible tokens are more similar to Ethereum than bitcoin, as Ethereum are essentially smart contracts or digital contracts. Bitcoin is a fungible token whereas Ethereum is a contract that cannot be duplicated.   Table 1 depicts the difference between Fungible and Non fungible tokens.

Table 1: Fungible and Non fungible tokens characteristics

FUNGIBLE	NON FUNGIBLE
Identical and interchangeable	Non identical and Non interchangeable
Common	Rare
Divisible	Non divisible
Uniform	Unique

Different types of tokens in block chain technology help in understanding Non fungible tokens, some of them are

- *Utility tokens* - these tokens are like coupons that can be used to redeem a service from a company. Example - Fitecoin, Augur
- *Security tokens* - These tokens get their value from an already existing asset, such as an art work, a house or even a stock. Eg - Non fungible tokens
- *Commodity tokens* - These tokens are used as a virtual currency. For example, bitcoin, dogecoin etc.

Non fungible tokens are security tokens that gain their value from an existing asset. Some biggest NFT sales are

- The first tweet ever - Jack Dorsey (twitter co-founder) sold the first tweet ever.
- Grimes Digital Images
- Lebron James - Basketball card
- Dragon
- Beeple artwork

Non fungible tokens are essentially certificates of ownership of certain assets, mainly, digital art, digital collectibles, and music. There are multiple ways to achieve the creation of a certificate of ownership. Usually the asset itself such as a digital art stored in the block chain along with who owns it. However this can pose a problem of duplication, false claims of ownership and of course the risk of getting hacked.

A. Pros of Non fungible tokens:

1. Owning something unique - As NFTs are irreplaceable, owners have pride of owning something unique that no one else possess.
2. Monetization - With NFTs, things that never could have been sold can be monetized. An added advantage is that the creator gets a much needed validation.
3. Excitement - Block chain and NFTs are new technologies. There is a certain excitement when taking part in the technological evolution and advancement.
4. Growth in value - NFTs are a lot like stock and hence are an investment. This implies that these tokens can grow massively in value.
5. Record of ownership – It is the specialty of an NFT. The block chain system enables the clear ownership records of all the tokens and hence theoretically not allowing theft nor will the authenticity be questioned.

B. Cons of Non Fungible tokens:

1. Digitization of physical art is not possible. The reason to collect physical art is often in stark contrast to buying digital art. The feeling when looking at physical art is completely different to what we see in digital art.
2. When any record is entered into Ethereum, it consumes large amounts of energy and hence carries a rather big environmental impact.
3. Owning an NFT is not always exactly equivalent to a copyright. Hence this asset cannot be controlled. When a person owns an NFT, it means that they only own the token behind this original asset. This asset can be copy pasted all over social media even if the owner has paid millions for it. So it is hard to see the real value of these.

IV.   METHODOLOGY

The problem of copy pasting however needs a rather complicated solution. The solution we propose is Steganography for media tokens. Figure depicts the proposed method for media tokens to overcome problem of imitation.
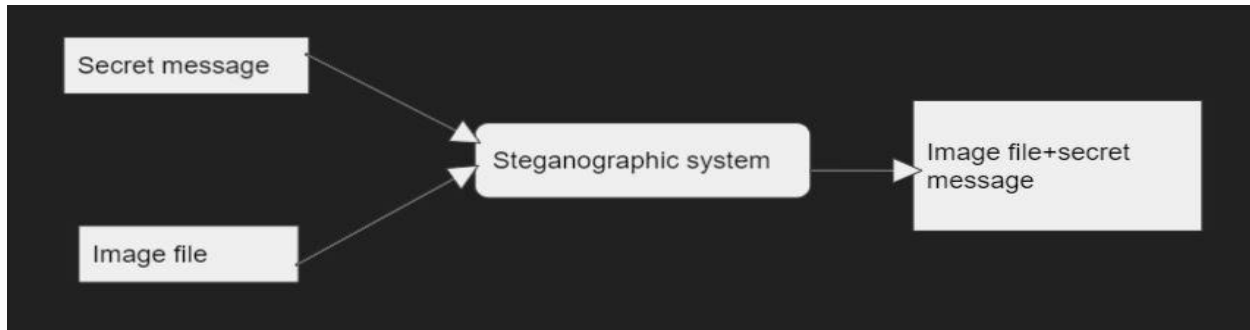
Fig 1: Proposed method for media tokens.

Algorithm to use steganography

- Input is taken from the user (the image and the message to be hidden).
- Message is hidden inside the image by changing the bits in unused data (such as whitespaces) in the image.
- The reverse process is done for message extraction (in python) and the output is displayed through the prompt.

Algorithm is implemented using python. The media token can be encrypted with a secret key using the above method, and then be stored along with the token in the block chain which is made visible only to the owner of the token. When the encrypted media, say an image, is copy pasted or screenshot the .png type image gets converted into .jpg, hence disorienting the original bit value of the image itself.

Since the secret key is encrypted within the bits itself, that will get jumbled up as well. This will denote that the image is not an original. This method however has its own drawbacks. If the creator of the token intended the bits to be part of the uniqueness of the piece, this would not work. And there are ways to decrypt the message as well.

V. CONCLUSION

Block chain technology can bring out immense benefits to the art and creative industries as it is mostly based on licensing, data management of the digitized and digitizable information goods. Its potential is high enough to compete with the preexisting internet based models and at the same time, it's creating a path for new business models in context with management of a token by a team of creators. Block chain technology may be the future but may not replace centralized architectures. Block chain may become ubiquitous as well which can help unlock the hidden or unknown potential of the technology resulting in various changes like the dramatic reduction in the cost of transactions.

Non fungible tokens are possibly the future of art collection and antiquing. Paintings are famous for selling for millions of dollars. There has been a massive growth in the digital art field, it is only pertinent to have a valid medium to sell these just like paintings. NFTs provide the same. NFTs are also a huge plus to musicians as their pieces are non-fungible as well and can be a huge investment. As the interest grows in a particular song or video, the value of the token increases as well and can be sold for a massive amount.

With NFTs, the pros outweigh the cons and there are some practical use cases as well, hence it is one of the most important technologies that has been initiated. The objective of this paper was to review Non fungible tokens and its pros and cons and propose a viable solution to the challenges faced by NFTs. The objective of this paper has been achieved.

VI.   FUTURE WORK

A more reliable technology can be implemented to retain the originality of the non-fungible token instead of steganography, or rather improve the efficacy of this solution itself by increasing the complexity of the encryption. The problem of energy consumption can be dealt with by using measures such as greening the data centers that host the Ethereum servers. This can be done using appropriate power usage metrics, cooling methods, temperature control etc.

REFERENCES

1. Buterin, Vitalik. "A next-generation smart contract and decentralized application platform." *white paper* 3.37 (2014).
2. Ciriani, Stéphane, and Marc Lebourges. "The market dominance of US digital platforms: antitrust implications for the European Union." *Available at SSRN 2977933* (2018).
3. De Filippi, Primavera, and Benjamin Loveluck. "The invisible politics of bitcoin: governance crisis of a decentralized infrastructure." *Internet Policy Review* 5.4 (2016).
4. De Vries, Alex. "Bitcoin's growing energy problem." *Joule* 2.5 (2018): 801-805.
5. Rothwell, Richard. "Creating wealth with free software." *Free Software Magazine* (2008).
6. Nakamoto, Satoshi. *Bitcoin: A peer-to-peer electronic cash system*. Manubot, 2019.
7. Salmon, Kurt. "Have the cultural and creative sectors found the formula for development in the digital age?." *Forum d'Avignon*. 2015.
8. De Voldere, Isabelle, et al. "Mapping the creative value chains." (2017).