Plutum

A Vision for a Decentralized Physical-Digital Bridge

Draft 1
July 2021

Cameron Fink
cameron@plutum.org

Ned Koh
ned@plutum.org

Sammy Weidenthal
sammy@plutum.org

Chris Kalra
chris.kalra@plutum.org

ABSTRACT Current solutions that attempt to offer non-fungible tokens (NFTs) that can be transacted in the real world fail in key areas, such as irreversibility, functionality, and transactability. We intend to offer a solution to these problems by developing a transparent, trustable, and functional protocol for creating and transacting tangible NFTs, also physical NFTs.

Nowadays, there exists a distinction between the computer-enabled realm and the physical world which surrounds us. The only real bridges between the separate spheres are services that have a reciprocating action in the "opposite world", such as Uber. Through Plutum, we intend to build a system that decentralizes connections between these two worlds and allows anyone to build a "link". This system acts as an open method for anyone to build a secure and verified link.

Plutum uses near-field communication (NFC), a standardized technology, and widely available NFC chips, to link NFTs on the blockchain to NFC chips that exist physically. Once created, due to the nature of blockchain, it is permanent. This allows physical items to be tracked on blockchain and have the advantages blockchain technology has. In effect, Plutum is building a decentralized bridge between the physical and digital worlds.

1. Preface

This whitepaper is intended to summarize how Plutum attempts to solve the key problems presented within this paper. It places the framework for how Plutum works, how Plutum intends to achieve the goals set out by this paper, and the road to get there. Within this paper, only core ideas and services are expressed. Frameworks and languages are not discussed.

This paper is not intended to be a formal and complete detail of all of functionality Plutum offers. While comprehensive, this paper is not final, and changes will be made.

2. Introduction

With the advent of non-fungible tokens (NFTs) came many applications that took advantage of the properties of NFTs, such as permanence and trustless transactionality. Examples such as CryptoPunks (Larva Labs, "Cryptopunks") and MarbleCards (Marble Cards, "Marble Cards") use NFTs as an authentication mechanism for artwork and to permanently store websites through a digital "bookmark". However, a clear limit on NFTs' capabilities has presented itself. To date, NFTs have only been able to exist digitally, or be used as a "token" that represents a physical object, such as Mattereum. We believe this creates opportunity for innovation at three points in the system:

TRUSTABILITY Many physical NFT systems personally hold the item that the NFT represents as a "token" or receipt of deposit. When we are obligated to trust these systems, it begs the question: how can we design more trustable systems that do not rely on a third party?

TRANSPARENCY Many cryptocurrencies that offer physical NFTs prevent full access to records of the item they represent, such. How do we build tangible, transparent systems? How do we design systems that enable physical verification?

CAPABILITY Digital NFTs can only be used in a digital ecosystem. In today's world, many lower-value transactions still take place physically (Raynil and O'Brien, 2019 Findings from the Diary of Consumer Payment Choice), and there are certain applications that cannot be replaced digitally. What applications can tangible NFTs present?

Plutum aims to provide a solution to the problems presented above. Through use of widely available NFC chips in conjunction with NFTs, Plutum enables true physical NFTs (PNFTs) that offer full capabilities as both digital and physical items.

Current solutions that offer physical-digital NFTs use NFTs as a receipt of deposit that represents a physical item stored in a secure location by a third party. While useful for digital transactions that mandate physical assets, this does not allow for blockchain to permeate in-person transactions. In addition, transfer of the NFT is not equal to transfer of the item, rather, just transfer of ownership. Plutum, however, uses NFC chips that can easily be implanted in items. This, in turn, requires physical presence of the item to transact the NFT. As a product of the physical item being at the location of transaction, Plutum can be effectively employed in in-person physical transactions. Thus, Plutum can offer a more transparent, trustable, and capable system, as physical ownership of the item is displayed at the time of transaction.

In addition, Plutum brings the benefits of blockchain into physical transactions. Blockchain has many advantages, such as permanence, transparency, and traceability. As Plutum uses blockchain in the validation and execution of transactions, it is able to bring these benefits into physical transactions. Plutum helps design stronger physical transactions for a better future.

3. Technology

3.1 SUMMARY Plutum uses NFC capabilities in conjunction with ERC-721 tokens, also called NFTs, that contain linking identifiers within each other to "tie" them together into one, cohesive object. We have termed this object a physical non-fungible token (PNFT).

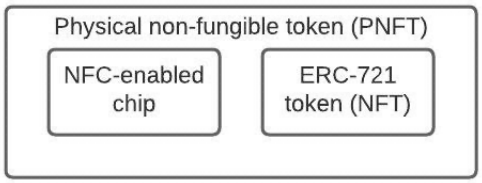

Figure 1

The diagram (Figure 1) above illustrates what a PNFT is composed of – fundamentally, it is simply the joining of two parts, an NFC chip and an NFT. As both parts are tightly and securely intertwined, they can be considered to be one object. PNFTs are at the core of Plutum and are the main "unit" that drives utility of the project. The services to be developed by the Plutum foundation all revolve around increasing the capability and utility of PNFTs, mainly through developing systems of transaction and use.

Each transaction that involves PNFTs has two participating parties; the owner, who transacts exclusively on the "sending" side of a transaction, and the receiver, who transacts exclusively on the "receiving" side of a transaction. Each one of these parties has a unique "address" that displays where their wallet is and provides instructions for blockchain transactions.

All PNFTs either created through Plutum or conforming to Plutum specifications can use the Plutum services, and all PNFTs can be transacted by anyone who has an NFC reader and an internet-connected device.

3.2 PNFT VERIFICATION While PNFTs are great in theory, a significant verification problem arises in practicality. The largest is the potential for NFC chips to be copied or impersonated, allowing a user with access to a wallet but not the item to transact the PNFT without owning the physical item, thereby defeating the bridge, and potentially disrupting true transactionality. However, we have developed a solution to this issue, preventing the impersonation of chips. Each NFT (ERC-721 token) will store the following metadata:

- Identifier – unique sequential number for each PNFT
- Tag – "plutum", marked in all PNFTs created by our service to mark them as Plutum PNFTs
- Public key – corresponds with a corresponding secret key on the NFC chip
- Name – a given PNFT item name/title
- Image – a given PNFT image

Each NFC chip will store the following data:

- Tag – "plutum", to identify each PNFT as Plutum
- Identifier – corresponds with the unique number of the NFT
- Secret key – corresponds with the public key on the NFT

Under this system, the data on each chip will be obfuscated and only be able to be read by the PNFT owner. As such, any NFC chip replicator will copy only the obfuscated text, which by itself is useless. In addition, the storage of the secret key on the NFC chip provides an additional layer of security, as only the PNFT holder (owner) can read the key to verify the chip prior to transactions taking place.

3.3 PNFT TRANSACTION Plutum PNFTs will be able to be transacted through standard systems, however, to prevent the disconnection of the PNFT, the physical chip must be present for transactions to occur. Transactions occur as a series of processes, where each step must occur and verify prior to the next step beginning.

1. Owner verifies ownership of the PNFT by verifying NFC chip against NFT on-chain
2. Owner verifies receiver's address, displayed as either an address or scanned as a shortened (quick-response, QR) code
3. Receiver scans NFC chip and temporarily stores data
4. Transaction formed and submitted to blockchain for inclusion in the next block and verification
5. Receiver receives PNFT, verifies received PNFT against prior scanned data

Verification for PNFT transaction occurs in two steps; first, the verification that the first item is the item listed within the NFT. This is to ensure that NFT and NFC chip stay tied with each other and cannot be transacted without both in the ownership of the owner. Then, once the transaction is formed through the reading of details both on the NFC chip and the digital NFT, it is submitted to the blockchain, where it is verified through traditional blockchain consensus mechanisms.

Note the in-person (tangible) exchange of the PNFT can occur at any point during the process but will most likely occur after step four but prior to step five.

If at any point during the process prior to the submission of the transaction, an error occurs in the building or verification of the transaction, the process terminates and must be repeated. Errors may occur if there are issues reading the NFC chip, if the NFC reader/device is broken, or if the NFC

reader/device cannot read the NFC chip for whatever reason.

3.4 PNFT CREATION Plutum will have a standardized ERC-721 contract (NFT) that is required for use of our applications and services.

The creation of PNFTs through our service will follow a standard process that fills this contract, which will be provided as a blank template to create PNFTs. This standardizes PNFTs, making it much easier to transact and utilize PNFTs. The creation process is similar to the transaction process in that each step must be completed and verified prior to the next step beginning.

1. Receiver scans NFC chip through applicable device
2. All details written to the contract
3. All details written to the NFC chip
4. Receiver prompted to title NFT and provide an image
5. Contract formed and submitted to blockchain for verification
6. PNFT returned to receiver's wallet

This process is followed for the creation of all PNFTs through Plutum services. PNFTs on Plutum are required to contain the identifier "plutum" to use Plutum services.

Through the completion of blank "template" contracts provided as open-source materials, anyone can create PNFTs that can use the Plutum services.

3.5 BLOCKCHAIN All Plutum services will operate on blockchain, providing an immutable record of all transactions that occur.

Plutum itself first intends to operate on the Polygon (Matic) blockchain, a level-two solution for scaling blockchain transactions with far lower fees.

However, to spur both adoption, ease of use, and flexibility, Plutum intends to develop solutions and cross-chain bridges to enable functionality on alternate blockchains, such as Ethereum main-net and other smart-contract enabled blockchains.

4. Applications and Services

4.1 SUMMARY Plutum plans to offer a wide variety of services to aid in the transaction, creation, and utility of PNFTs. These services are divided into two classes: core and peripheral.

Core services are services and applications that are key to the functioning of Plutum and are critical to users' experiences. All core services will be developed prior to the beginning of development of peripheral services.

Peripheral services are services developed by Plutum with the aim of increasing functionality. Over time, peripheral services may become core services as they increase in importance and function.

4.2 ATHENA Athena is a core service that includes all the liquid-democratic aspects of Plutum, such as our governance token, PLTM, in addition to the portal that enables governance activity, the Athena Portal.

Athena will be accessible to anyone who wishes to use it, either through the Athena Portal, or through other solutions built using the Plutum Development Toolkit.

4.3 OSIRIS Osiris is a wallet and a core service that has full functionality to create and transact PNFTs using an NFC reader. While mainly targeted at mobile users, who can use built-in NFC readers, Osiris will also be offered to desktop or computer users through the connection of an external NFC reader.

Osiris on mobile devices will also have a wallet for PLTM, our governance token.

Osiris will also have an institutional version with multiple optimizations designed for stronger institutional and enterprise use and increased customizability.

5. Purpose and Use Cases

5.1 PURPOSE We designed Plutum to build a better future; fundamentally, our mission is to change the way we interact with our world every day.

We are building Plutum not because we want to turn a profit, not because we want to become some big corporation; in fact, we structure Plutum to prevent exactly that from happening. We are building Plutum because we believe that our technology has the potential to change our – everyone's – capabilities of connection, transaction, and interaction. And we're committed to investing in the next generation of technology.

This section outlines use cases and our purpose. It is designed to display how our technology can be used to change transactions. It is not inclusive of all cases. PNFTs have thousands of use cases to revolutionize the way we interact – we solely picked specific cases that we believe highlight aspects of our technology.

5.2 REAL ESTATE AND TITLE DEEDS PNFTs can be used as proof of ownership for properties through the attachment of NFC chips. NFC chips are widely available at a relatively cheap cost, and can take many forms – such as stickers, embeds, or cards. In the case of a title deed that's already exiting, an NFC sticker can be applied, turning the deed into a PNFT through our software.

Down the line, NFC chips could be embedded in paper, owing to their thinness and small size, and legal documents such as deeds could be printed on paper with embedded NFC chips.

In this case, blockchain helps to track the history of a document and logging transfer history. In addition, messages can be included with these transfers; this can be used to "sign" documents. In conjunction with the unique and unforgeable nature of addresses, we can entirely prevent forgery of signatures and create an entirely transparent, reliable system for signing legal documents.

5.3 COLLECTIBLES PNFTs have two clear use cases in the case of collectibles, both illustrating some of the clear benefits of blockchain technology.

Over time, many common collectibles have seen the development of verification and grading agencies that aim to quantify the quality of a collectible item, such as PCGS. While a service with demand, unfortunately, the traditional system leaves room open for failure. In 2020, counterfeit products created $31.05 billion in losses (Statista, "Sales Value Losses from Fake Goods, by Industry Worldwide 2020"). Traditional methods, such as mail or digital verification, leave too much potential for failure at some point in the system. However, due to the immutable nature of blockchain, it is impossible to fake authentication of the item.

PNFTs can be used to track and guarantee authentication, preventing potential buyers from being scammed or "blindsided" by a convincing fake product. In addition, through combination with other data sources, such as alternate authenticators or auction houses, we note the possibility to track the general reliability of an authenticator, and to rate their quality. Through the rapid retrieval of PNFT history data, sales of collectibles could be verified prior to anyone being scammed. Verification data can be considered a form of immutable, unchangeable certificate of authenticity, empowering buyers to make more intelligent decisions.

In addition, PNFTs can enable the sale of unique, numbered, and unforgeable collectibles or physical assets. As each PNFT has a unique number identifier, PNFTs are numbered by which point in the system they are in. In addition, PNFTs can be given titles that include numbers. This enables manufacturers to release verified limited series of collectible items, and to ensure they remain secure and authentic.

5.4 DIGITAL PAYMENTS By scanning PNFTs and querying the data from the blockchain, it would be possible to rapidly receive details of an item that may be transacted.

Specialty ERC-721 contracts could be built that contain other metadata designed for specific purposes, such as the sale of items. They could contain static items, such as price, and could be used to transact the entire PNFT

using only one payment method – cryptocurrency for the price and for the gas.

In a post COVID-19 world, digital payment systems have become more common than ever before. Plutum enables digital payment services with more complex interactions, such as item tracking during the earliest stages, receiving, and pre-verification of the first transfer stage possible. More complex interactions could allow retailers to better personalize services, potentially increasing conversion rate and general satisfaction with the sales process.

5.5 BENEFITS OF BLOCKCHAIN PNFTs bring many of the benefits that blockchain has into real life, but there are a few notable ones that we have chosen to highlight for their marked importance.

5.5.1 SECURITY Blockchain systems offer increased security, as the only viable method of forgery is a 50% attack, which is widely considered to be nearly impossible. 50% attacks require a minimum of near 50% of the total computing power verifying transactions under once center of control, from which they can verify false transactions. Considering the highly unlikely – if not impossible – nature of this attack, blockchain systems offer nearly impermeable security in terms of transaction forgery. With increased security come derived benefits – those that rely on the security of blockchain – such as authenticity and provability.

5.5.2 PERMANENCE Given the sequential nature of blocks in a blockchain system, blocks other than an arbitrary number of recent and unproven blocks, are permanent. Validity of transactions is further guaranteed as more blocks verify more transactions, and in the course, verify past transactions through inheritance – by verifying the most recent block, prior blocks are also verified as each block builds upon one another. With this, past blocks are considered permanent. Typical block time is short, so transactions can typically be considered permanent within a few minutes of the transaction submission. This permanence, in combination with transparency, furthers the use of PNFT technology for the purpose of authentication and tracking.

5.6 FUTURE Please note any technology mentioned in this section (5.6 Future) is just "pipeline" – things that we believe are made possible by Plutum and are not things that we plan to develop now. As mentioned above, PNFTs have immense applications in authentication and tracking technology. While not guaranteed, with development, this technology could be used to enable far-fetched technological developments. With the use of items such as switches, it would be possible to build models with parts that you can interact with tangibly, having digital impacts.

One potential use case for technology like that would be to build video games where you can assemble a character in real life, tangibly placing pieces, that then can be tracked and placed on a hybrid physical-digital world.

At its core, Plutum builds a tangible internet, a tangible system of digital interacts – a tangible world with digital impacts. This does not exclude the possibility to build a digital world with tangible impacts.

While unrealistic and undoubtedly difficult to build, Plutum lays the foundation for systems of interaction that could use digital interactions to manipulate physical objects and vice versa. At this point, we are only planning to build a system that allows for physical interaction with digital objects, however, there exists the possibility – in theory – to build systems that allow for complex, smart digital interactions with physical objects.

6. Conclusion

As mentioned above, this paper is not final, and does not preclude anything from the future of Plutum. However, this paper does lay out a vision, a guideline, for how we plan to develop Plutum and what we see in its future.

Throughout this paper, we only took the opportunity to discuss where we're going,

but not what we are. Plutum is the opportunity to create huge change in our world, for the positive. We believe that Plutum will revolutionize the future of commerce and rewrite the narrative of transactions.

In the course of building Plutum, we plan to build tools and applications to reach our goals, but primarily, we plan to fulfill our mission. Plutum aims to bring the benefits of blockchain into tangibility; among them, you can count transparency, authenticity, and security. In addition, we are building a stronger future that empowers the consumer and designs for flexibility. We are building Plutum because we believe in the future; what we consider to be the "open era" of computing. As we accelerate towards a digital-dependent era, we believe that physical interaction with our products and the items we use will be more important than ever. And with this, we write this paper to lay a foundation for the work we are doing, the products we are building, and perhaps, the future we are designing.

Works Cited

"CryptoPunks." *Larva Labs*, www.larvalabs.com/cryptopunks#.

Kumar, Raynil, and Shaun O'Brien. "2019 Findings from the Diary of Consumer Payment Choice." *Federal Reserve Bank of San Francisco*, Federal Reserve Bank of San Francisco, 26 June 2019, www.frbsf.org/cash/publications/fed-notes/2019/june/2019-findings-from-the-diary-of-consumer-payment-choice/.

"MarbleCards - Whitepaper." *MarbleCards - Collect the Web*, marble.cards/whitepaper.

"Sales Value Losses from Fake Goods, by Industry Worldwide 2020." *Statista*, 18 May 2020, www.statista.com/statistics/1117921/sales-losses-due-to-fake-good-by-industry-worldwide/.