KYCT & Verifiable URI Protocol

Litepaper v1.2

kyct@ubirch.com

January 24, 2022

Contents

Contents 2

What is this for? 3
- What is UBIRCH KYC service? 3
- Why have we created the UBIRCH creator identity service? 3

Introduction of UBIRCH 4

Stakeholders 4
- NFT creators & sellers (identity providers) 4
- NFT buyers (identity seekers) 4
- NFT verifier (identity checkers) 5

The KYC Protocol 5
- Identity Verification 6
- Asset Registration 7
- Authenticated NFT Minting 7
- How do you verify the authenticity of the asset? 8

How cost-effective is this KYCT? 8

How can the KYCT be implemented/used? 9
- As identity-service in a Minting-Platform 9
- As identity token in transactions and in a wallet 9
- As part of a proof 9

Additional References 10

What is this for?

Two critical issues remain unsolved for a stable growth in the NFT community: Identity and proof of origin. We are offering a combined solution that leverages the well established UBIRCH trust-backend for proving that an asset belongs to a creator and was anchored at a specific time and also a way to prove that a creator is not only the owner of the crypto-identity but also a real person.

What is UBIRCH KYC service?

UBIRCH creator identity service is a new paradigm for the world of NFTs, whose makers are currently mostly unknown. Our mission is to bring an additional layer of security to NFTs and make them more accessible for real world users and transactions.

Why have we created the UBIRCH creator identity service?

Digitalization accelerated by the Corona pandemic has led to a significant increase in the overall crypto market. As of September 2021, the crypto market valued at approx. $2.2 trillion. This represents a year-on-year increase of 378%.[1] Non Fungible Token (NFTs) are partly responsible for this increase. These account for one percent of the total crypto market as of August 2021. That equates to $19 billion, and that number is growing.[2]

Even though the current times are transformative and exciting, there is still a problem with NFTs. On one hand, NFTs are a wonderful way for artists, collectors, and owners to represent their digital property and cut out the middleman, but on the other hand, NFTs have a lack of trust. This means that there is still a gap between the creator (maker) of an NFT and the buyer. And there is identity theft of all kinds, problems with proving ownership/origin of an asset in a legally binding contract and also ensuring digital art based on NFTs is currently a big problem. All these problems are market barriers and should be removed.

[3]

[1] https://coinmarketcap.com/charts/
[2] https://www.coingecko.com/de/nft
[3] https://twitter.com/laufman/status/1370715624058544128?ref_src=twsrc%5Etfw

The UBIRCH creator identity tackles this problem. We are closing this trust gap with our additional security layer. The creator identity service is built on top of the UBIRCH security layer. It implements creator identity verification as a security mechanism to prove the identity of a creator (maker), which also proves the authenticity of a created artwork.

Introduction of UBIRCH

UBIRCH is a digital data proof solution that brings security into data driven processes and establishes trust between multiple stakeholders. It's one cloud-based proof machine that enables everyone involved to verify the authenticity and integrity of data received. Founded and managed by experienced specialists in cryptography, blockchain and data-driven business models, UBIRCH is combining robust cryptography and modern blockchain technology into an innovative, easy to use SaaS product.

Together with a consortium of renowned companies, the Cologne-based company has developed and is operating the official infrastructure of the EU Digital COVID Certificate for Germany. But the UBIRCH infrastructure is not only being used by the government, UBIRCH has clients in Energy, Healthcare, Insurance and Industrial IoT that are relying on the integrity of the services every day. The UBIRCH system is built to combine the best out of two worlds - classic cryptography and blockchain technology.

Stakeholders

NFT creators & sellers (identity providers)

Creators who produce the NFTs - these can be artists, companies, design studios, or anyone familiar with creating an NFT. A creator typically has control over the manufactured asset. However, there is currently no proof of original ownership/origin, creating a very opaque market. In theory, buyers of the NFT can trace the path back to the wallet of the original minting process. But - how can you trust that a coin purse is actually the purse of the creator? Sure - if the artist is famous and has a twitter account, you can do a "twitter check", if not, you can't. We will explain the mechanism in detail to these verification partners so that they provide the right data. NFT creators do also have an interest in a reliable legally binding identity of a potential buyer of their art in case they are willing to sell.

NFT buyers (identity seekers)

Basically anyone interested in purchasing an NFT. All buyers are looking for proof of ownership/title to verify that they are buying an NFT that came from the original creator.

NFT verifier (identity checkers)

Identity-Verifiers are the backbone of the verification process. They verify that the identification data provided by the NFT creator is valid before it is linked to a wallet. To ensure that the data is correct, there will be an incentive mechanism to ensure that verifiers provide the correct data.

The KYC Protocol

The core of the KYC protocol is the proof that a person or organization has control over a specific cryptographic id, crypto wallet or account. Depending on the identity requirements this may be an OpenID Connect account identifier (social media), a market account (Coinbase), a crypto wallet, or simply a cryptographic key pair. A social identifier or market account identifier may be used to prove the authenticity of posts to social media accounts, or market transactions, while wallet and cryptographic ids may be used to prove the authenticity of an asset. Ultimately the protocol creates a new token (KYCT) that acts as a trust anchor to validate the origin of any kind of asset used in on-chain or off-chain transactions.

For the sake of simplicity and relative impact, the following description will focus on cryptographic proofs. The proof of control over a certain account or wallet does not in itself prove the identity of the owner and is as such only of limited relevance. In short, we will support multiple levels of identification depending on the use case:

Officially Accepted Identification

- official ID/Passport, or eID[4]
- SSI (Self Sovereign Identity)
- Personal approved Identification Services[5]
- Organizational approved Identification Services[6]

Private Sector Identification

- Social Media Accounts[7]
- Market/Corporate Accounts[8]

Self Approved (control over an account)

- Email Address + public proof of control[9]

[4] A government backed ID solution, EIDAS conforming, or like Estonian e-ID
[5] Approved identification methods, such as Post-Ident, Web-ID, Verimi, etc.
[6] Approved identification methods such as Organizational D-Trust Certificate
[7] Google, Facebook, Twitter or other SAML/OpenID methods
[8] Proof of control over a market account, such as Coinbase
[9] Proof of control over an Email address or account via Twitter/reddit, etc.

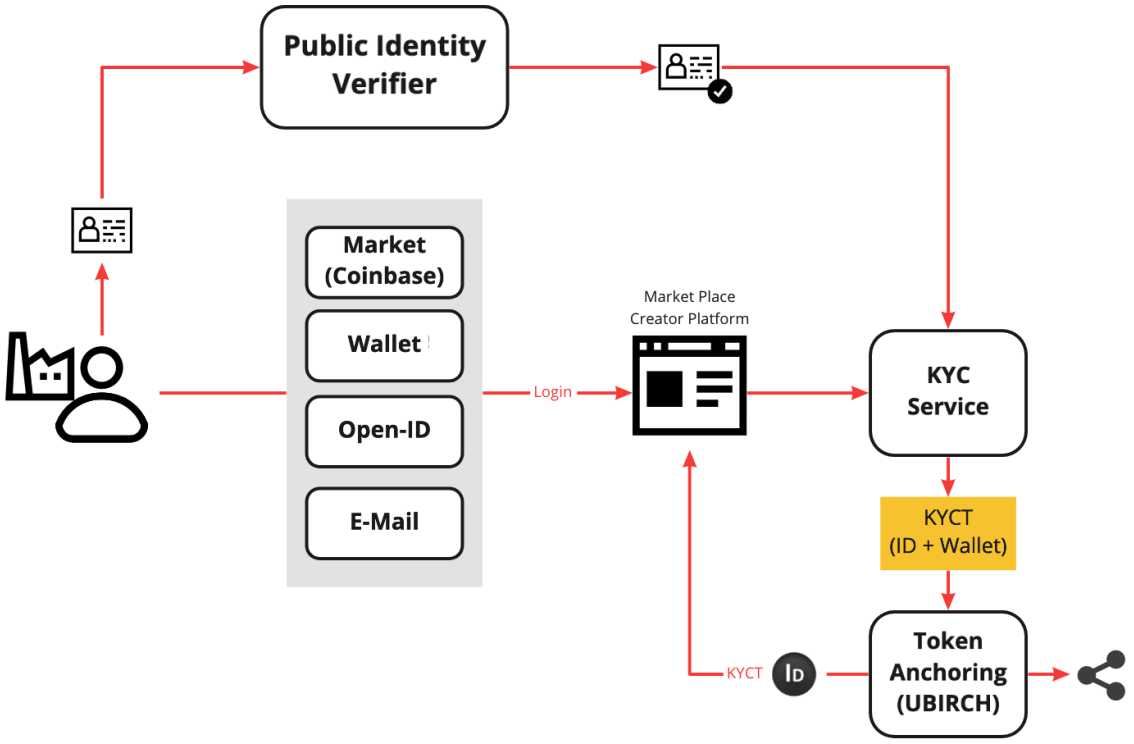
To prove that an asset is authentic effectively two steps need to be taken:

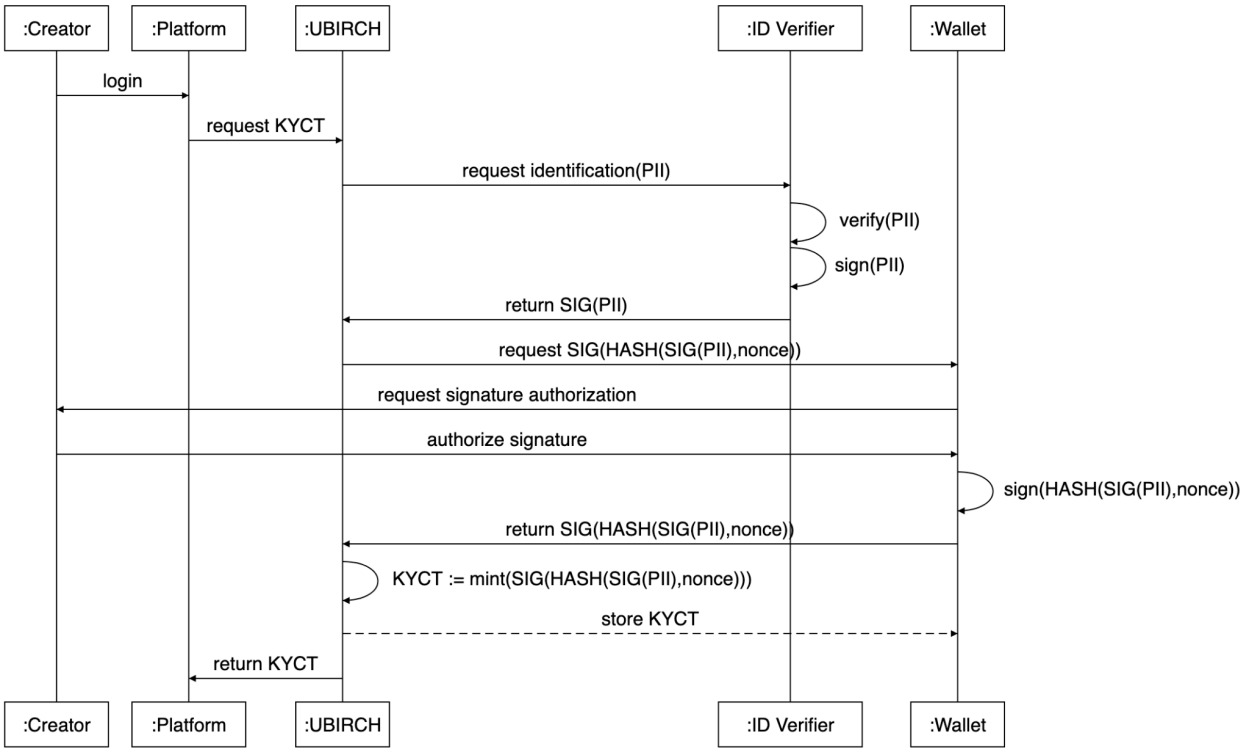
a) identification of person or organization in control of a cryptographic id
b) authentication of an original work using the cryptographic id

The following examples assume the integration of the KYC protocol in a market place or creator platform.

Identity Verification

The first step for a creator is to log into an KYC enabled platform using the usual methods of email, OpenID or social media accounts. The platform then triggers an identification process that requires the user to use his cryptographic identity to sign a challenge which is used in combination with his login method to initiate the identity verification process (i.e. JWT challenge). The result is a document containing the minimum required information (i.e. name, alias, wallet address/public key, challenge, signature) about the identified individual or organization combined with the challenge signed by the verifier (the KYC token). In a final step, the proof of identification is then stored in a distributed ledger (token anchoring) to prevent modification from there on.





PII - personal identifiable information
nonce - random challenge

For the purpose of identification the KYC token can be an NFT by itself, containing the link to the proof in the URI field of an ERC721 token. However, this is not necessary, if the cryptographic key of the creator was used in the process as all works signed by this key can be authenticated by the KYCT.
The anchoring process described here is similar to the minting of a token or NFT and accomplished by the UBIRCH second layer solution. The result is a proof of identity token (KYCT) bonding a wallet address to the verified identity of the controlling entity.

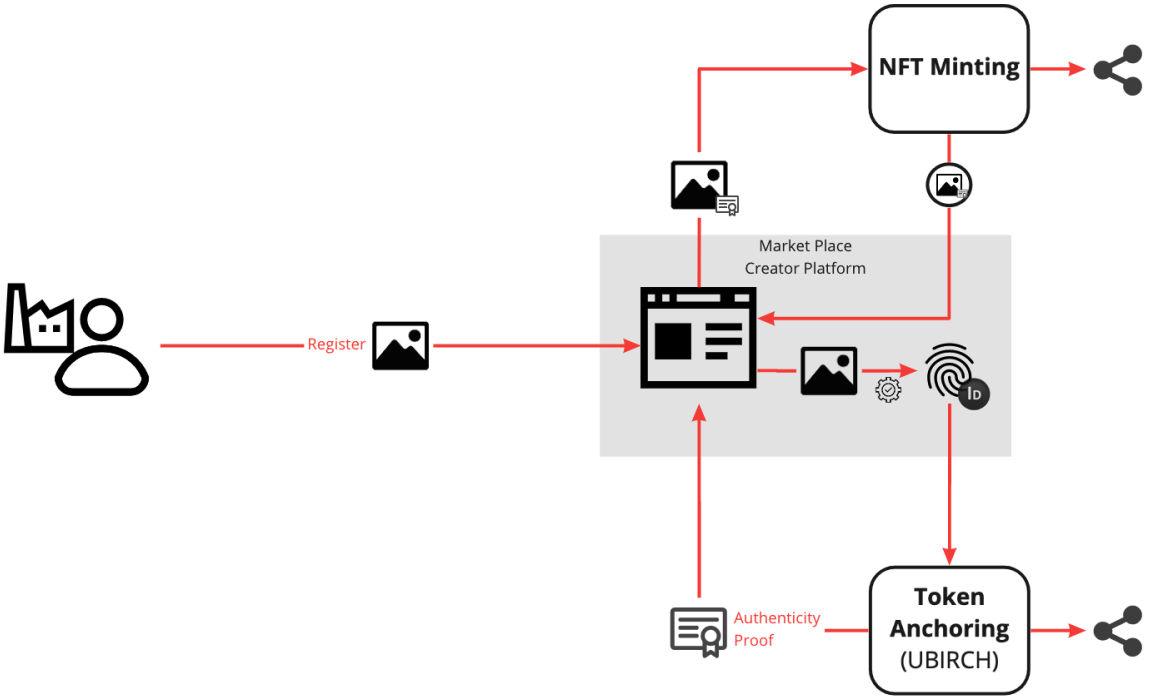
Asset Registration

A creator must register existing and new assets using his personal cryptographic id by signing the assets using his verified identities private key. This step is decoupled from the actual minting of an NFT as this step mainly focuses on the authentication of an asset. It establishes a bond between the creator and the product.
During the process, a hash of the asset is signed by the creator and stored as a proof on-chain similar to the notarization of a contract in the offline world.

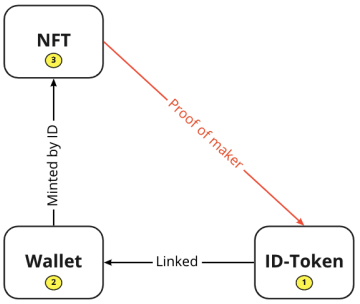
Authenticated NFT Minting

Authenticated and registered assets may now be used in the minting process by the creator or an authorized seller. To ensure only authentic assets are sold, the minting contract checks the

authenticity and may also check the identity of the assets creator. This will prevent the sale of copied assets and in case of creator verification also unauthorized seller activities.



This process will enhance trust in the market of NFTs as creators now have full control over their works and buyers can verify the authenticity and originality of the assets. It may not prevent fully a grey market, but will help market places to scan and remove unauthenticated assets or non-authorized offers.



Usually the lookup and verification is decoupled from the actual NFT and the assets. The KYCT indirectly allows the creator identification through the knowledge of a wallet address. For some use cases it may even be useful to include the KYCT hash into the asset to bond the proven creator identity and speed up the lookup process.

How do you verify the authenticity of the asset?[10]

For practical purposes the image hash of a picture can be immutably stored on-chain by the above described process. As a result the authenticated image hash plus metadata is transformed into a URI that can easily be included into an NFT. The format of this verifiable URI is implemented in a similar way like the hashed content-identifiers in IPFS (CID)[11] and contains a hash of the files content including meta-information about the used encoding and hashing-algorithms. It can also be represented as a JWT-Token[12] for easier processing. This URI may then be used in the minting process of an ERC721 token - but it can also be used as a self-contained verifiable anchor. To verify the authenticity of the asset and its creator the following steps may be followed:

1. Extract metadata verifiable URI from token.
2. Extract the image hash from metadata/image.
3. Calculate the linked pictures image hash and compare it to the hash from metadata.
4. Use the hash to request the stored KYCT from the chain.
5. Verify signature of the KYCT and check wallet address matches expected creator.

How cost-effective is this KYCT?

Creating and sending NFTs on Ethereum is more complex than ERC-20 tokens and their transactions. This complexity leads to higher gas fees. This means that creating an NFT is sometimes more expensive than the NFT itself is worth. On Ethereum, the fee is currently around $100, very high compared to Solana ($0.015) or layer 2 solutions like Polygon/Matic (<$1). The good thing about solutions like Solana is that the fees are much lower than minting on the first layer of Ethereum. However, the low fees are to be taken with a grain of salt on a network that is less trusted than Ethereum. There are also fewer users interacting on the various networks outside of Ethereum. This leads to fewer customers for the creator of an NFT and thus it is also more difficult to discover in the market. Our solution offers the best of both worlds - minting on the Ethereum blockchain, a trusted and proven network and the low fees of a 2 layer solution.

How can the KYCT be implemented/used?

The KYC-token can be implemented in NFT platforms and related technologies in several ways.

[10] PoC Example: https://medium.com/@stephannoller/why-verifiable-uris-can-make-nfts-safer-16904199bb0d
[11] IPFS Content-Descriptors: https://github.com/multiformats/cid
[12] JWT Web-Token Standard https://en.wikipedia.org/wiki/JSON_Web_Token

As identity-service in a Minting-Platform

In this case the KYCT can be a linked service where customers can get redirected to the KYCT platform in order to run through the identification process, create their respective identity token and come back to the platform with it. The platform can then utilize the identity token for further actions, e.g. minting NFTs or in selling/buying transactions etc. This integration can be handled both as a visible, web-based subservice or alternatively via a direct API integration.

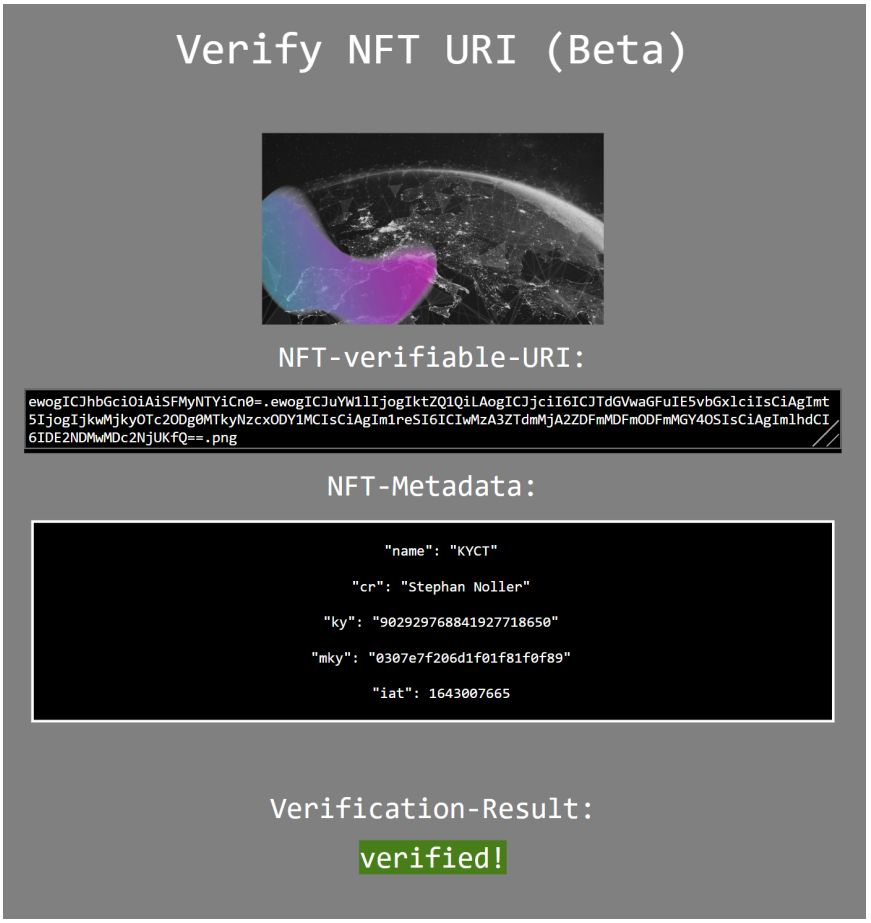
As identity token in transactions and in a wallet

Another layer where the KYC-token can be used is as an actual ERC721 token in a user's wallet. For this the user has to visit the KYCT platform once, run through the registration process and then use the additional service to mint this identity token into his wallet of choice. The token will then be minted and transferred as a frozen token, so that it cannot be transferred to another wallet anymore. From that point on the user of the wallet can always demonstrate that his/her identity has been proven by showing that token and making it accessible for verification if needed. The real identity does not have to be revealed in such cases, just if the user wants, he/she can prove on the KYCT-platform that he/she is actually this legal person.

As part of a proof

A third use-case is relevant whenever some assets/artwork have to be proven to be authentic or in the ownership of a specific person. This can be the case while trading the asset, but it is also a relevant need if legal claims have to be made, e.g. if an asset got stolen or abused.
In all these cases the user can prepare a legal claim by presenting the combination of crypto-proofs that he/she has available for the asset, the KYC-token, the connected wallet and all registered proofs of the legal identity like passport, bank-account or similar that can be used to build a legal case.

Example



Example of an Image and its according verifiable URI - represented as a JWT-Token. The Metadata is encoded into the URI and can easily be extracted. A KYC-Token is part of the Meta-Data and can be used to verify the identity of the creator. The Image-Content is represented by a perceptual hash.

Additional References

- Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects [https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/01.01.01_60/ts_119461v010101p.pdf]
- Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges (Tech ReportV2) [https://arxiv.org/pdf/2105.07447.pdf]
- Decentralized Identifiers (DIDs) v1.0 [Decentralized Identifiers (DIDs) v1.0 (w3.org)]
- Verifiable Credentials Data Model v1.1 [Verifiable Credentials Data Model v1.1 (w3.org)]

- IdToken: the new decentralized approach to digital identity [https://dl.gi.de/bitstream/handle/20.500.12116/33174/proceedings-15.pdf]
- Know Your Customer (KYC) Implementation with Smart Contracts on a Privacy-Oriented Decentralized Architecture [https://www.mdpi.com/1999-5903/12/2/41/htm]
- https://checkmynft.com/

Disclaimer

This paper is for general information purposes only. It does not constitute investment advice or a recommendation or solicitation to buy or sell any investment and should not be used in the evaluation of the merits of making any investment decision. It should not be relied upon for accounting, legal or tax advice or investment recommendations. The opinions reflected herein are subject to change without being updated.