The TLDR & Ask

The article introduces another solution for verifiable credentials using Ethereum-based attestations and explores the trade-offs and limitations of ERC721 (NFTs) and Soulbound Tokens (SBTs).

How do you see attestations being used in the future of Verifiable Credentials?

Open some popcorn. This will take about ~10 mins to read.

Let's dive in ⇣⇣

ERC-721 (NFTs): The Current Standard & Limitations

NFTs have created a sensation in the industry, particularly for digital art and collectibles, leading to the wider adoption of NFTs for various purposes such as membership badges, proof of attendance, skill showcasing, and more. This surge in popularity has made ERC-721s the go-to choice for creating different types of verifiable credentials (VCs).

The Limitations of ERC-721 Verifiable Credentials

While NFTs can serve as VCs, they come with several limitations that can limit their effectiveness in certain use cases, especially as it pertains to one's identity, authorizations, and reputation.

Transferability:

ERC-721 tokens are like hot potatoes, they can easily be passed on to someone else. This can pose challenges for VCs. For example, a certificate NFT could end up in the hands of someone who doesn't possess the same level of knowledge or expertise, potentially leading to misuse and misrepresentation of the credential.

Irrevocability:

Once an ERC-721 token is handed over, it cannot be taken back. This creates potential risks in identity and reputation systems. For instance, if a credential is provided to a member who later becomes a bad actor or if the credential needs to expire after a certain time, it can't be revoked. Creative solutions like "seasons" or multiple tokens have been introduced as a workaround but are not ideal.

Lack of standardization:

ERC-721 tokens are like snowflakes, each one is unique with its own custom contract and metadata which makes it difficult to ensure compatibility and interoperability between different use cases.

Soulbound Tokens (SBTs): The Upgrade

Soulbound Tokens (SBTs) are a significant upgrade to the limitations of traditional NFTs as verifiable credentials. SBTs are unique digital assets that presumably cannot be transferred to other accounts or addresses. Once they are assigned to a specific account, they remain bound to it, hence the name "soulbound".

SBTs can be used to represent a user's identity and accomplishments, attendance, and more creating an on-chain identity and resume of behavior. This opens up new possibilities for DAOs, contributors, and governance designs, including improved sybil resistance and better community organization.

There are several amazing projects that are starting to integrate and explore SBTs as a verifiable credential alternative and the concept of soulbound tokens is promising, but it's building upon existing technology and still has its limitations.

Existing Limitations of Soulbound Tokens as Verifiable Credentials

SBTs are making a splash in the world of VCs with their improved security and utility compared to traditional NFTs. But, even with all their awesomeness, they still have a few quirks.

Transferability Risk

Despite being more secure than traditional standards like ERC-721, SBTs are not completely soulbound and can still be transferred. This can happen through private key sharing, multi-sigs, smart contract exploitation, or threshold ECDSA.

Examples:

1. The SBT is sent to my account A, but I just give you my private key, thus transferring (or at least sharing the ownership) together with you.

2. The SBT is sent to account A, but its private key is actually distributed between multiple parties via a threshold ECDSA DKG and signing scheme.
3. The SBT is sent to account A, but it's actually a smart contract that has an "owner" and a method to "change the owner". This is similar to how a team exploited EthCC conference tickets, by creating lots of contracts that can change who is eligible to use the tickets under the hood.
4. The SBT is sent to account A, but it's actually a multi-sig (similar to 3, but more conventional)

"When EthCC offered another batch of 300 tickets in March, the group devised a method to make the non-transferable NFTs transferable."

Limited Off-chain and Scalable Privacy Capabilities

Being restricted to the on-chain world, SBTs don't offer much privacy protection unless combined with zero-knowledge proofs. And while there are solutions to move SBTs to Layer 2 networks to reduce costs, not all use cases require on-chain storage. This can limit SBTs' effectiveness in certain applications.

Lack of Common Registry and Specification

Unfortunately, there is no central registry or specification for SBTs, which can lead to fragmentation in the market. Different protocols and builders have their own ideas about how SBTs should be used, causing confusion and hindering interoperability between systems and protocols.

Despite these limitations, SBTs are a promising technology with exciting potential, especially for communities and organizations looking for better identity, authorizations, and reputation systems compared to traditional ERC-721 tokens.

Attestations: An alternative path forward

"In order to decentralize more than just money and assets, the world needs a decentralized protocol/ledger for arbitrary attestations about anything." - Steve Dakh

, Co-Founder @ Ethereum Attestation Service

Attestations are simply statements or pieces of evidence about anything, made by anyone. They're digital records signed by an individual, company, or organization to verify information about another person, entity, or thing. They have a variety of uses, like identity verification, reputation building, proof of X, content authenticity, and even beyond VCs, like supply-chain tracking and compliance assurance, voting systems, ticketing, oracles, and more.

Think of attestations as a digital reference. Just like you trust your friends' opinions, you trust attestations from reliable sources. But if the "attester" isn't trustworthy, the attestation loses its value. The value of an attestation depends on the reliability of the entity making the statement. For example, a certificate of completion from a reputable university holds more credibility than one from an unknown online course provider or your friend.

Attestations play a crucial role in establishing trust in the digital world. In the absence of physical interaction or presence, it can be difficult to verify the information. Attestations provide third-party validation and secure confirmation of the authenticity of the information, making it easier for others to trust and rely on it.

The key features of an attestation

Authenticity:

Because the attestation is signed by the attester using their wallet, the attestation record can be verified as authentic.

Non-transferable:

Attestations are tied to a specific wallet address and cannot be transferred to another address.

Revocable:

Attestations can be designed to include the option of revocability, allowing the attester to revoke the attestation if necessary.

Expireable:

Attestations can have a predetermined expiration date, making them ideal for time-based credentials or membership subscriptions.

Immutable:

Once an attestation is made, it cannot be altered or deleted, ensuring the attestation remains trustworthy and verifiable.

Transparent:

On-chain attestations are easily verifiable and transparent, as anyone can verify the authenticity of the attestation. Off-chain attestations retain the attestation data and authenticity but offer greater privacy.

Composable:

Multiple attestations can be combined and linked to create a larger picture of the information being attested to. Think of attestations as lego blocks for trust.

Versatile:

Attestations can be used in a wide range of use cases, from supply-chain provenance to ticketing systems and voting systems, oracles, and beyond.

Interoperable:

Attestations are interoperable between different platforms and systems, making it easier for organizations and individuals to share their verified credentials and reputations across ecosystems.

Batchable:

Attestations can be made in batches, allowing for multiple attestations to be made at once, reducing the administrative overhead involved in the verification process.

Badgeless:

With attestations, you do not need custom art or graphics like most NFT or SBT solutions. However, you can easily use the attestation data and build a pretty UI if you want.

On or off-chain:

Attestations can be made on-chain, recorded on a blockchain, or off-chain. The choice between on-chain and off-chain depends on the level of transparency and privacy required for the particular use case.

Using attestations as verifiable credentials

Attestations have several use cases and are a great alternative or complementary solution for VCs. For example, you might authenticate access to your DAO with an NFT and then control roles and memberships with attestations instead of additional NFTs or SBTs.

Attestation Use Cases

Self-sovereign identity:

Individuals attest to and control specific attributes of their identity, social accounts, and more. This can be done on or off-chain.

Reputation systems:

Community members can make attestations to vouch for others in their network, including information such as trustworthiness, reliability, and behaviors.

Social graphs:

Users can make attestations to create a verified network of people they know and interact with, allowing them to build their circle of influence.

Authentication into a DAO or community group:

DAOs can make attestations to grant access to a specific address, allowing them to join a community instead of minting and distributing NFTs.

Community roles & authorizations:

Community managers can use attestations to assign roles and permissions to users within the community. This can include information such as the user's level of access, responsibilities, and allowed actions.

Voting systems on or off-chain:

Builders can use attestations to verify member eligibilities and identity to ensure that only authorized people are able to participate in the voting process. Further, attestations can be used to cast votes and provide a more transparent and suitable

record of the voting results on or off-chain.

Employment statuses & verifications:

Employers can use attestations to verify the work history of employees or DAO members, providing a trusted and verifiable record of their employment.

Credentials, certifications, and licenses:

Schools, dapps, certification boards, and other organizations can use attestations to verify the credentials, licenses, and certifications of individuals. These attestations can have expiration dates and can be revoked if necessary.

Quests & badges:

Dapps can use attestations to confirm the completion of quests, courses, or other achievements by a user's wallet.

Content authenticity & accuracy:

Both users and third-party organizations can use attestations to verify the authenticity and accuracy of content online, providing a trusted source of information for others.

Proof of X:

Proof of anything. E.g. An event organizer attesting to the attendance of someone or a financial institution attesting to the proof of funds of an individual and more.

Example of a DAO attesting to the role of a specific user:

A DAO can utilize attestations to assign roles and permissions to community members. This testnet example is showing a mock DAO is shown making an attestation to a User, recognizing their role in a guild.

The attestation specifies the DAO as the "From" address, the User as the "To" address, and includes details such as the guild name and role ID. It is further validated by the DAO's signature and includes a timestamp for when the role was granted, providing a verifiable and transparent record.

If the User changes their role or departs from the community, the DAO can revoke the attestation with ease which would have its own unique timestamp, leaving a clear and verifiable record of the change.

[

Screenshot 2023-02-09 at 10.43.56 AM

1471×994 151 KB

](https://ethresear.ch/uploads/default/original/2X/f/feb2a007f0715a39396d5faae9d07853a418f3ff.jpeg)

easscan.com

Attestation (0x3018126fa760bf208de94c69bca4072ed7503fdd363b16bbd61387624b1003dd)

Explore attestations and schemas on the Ethereum Attestation Service

Sample DAO attesting to a guild member's role using on-chain attestations on Ethereum Attestation Service (EAS).

Going beyond VC use cases with attestations.

Attestations have the potential to revolutionize many industries and create new solutions to age-old problems. Beyond identity-based solutions, attestations can be applied to a wide range of use cases, including:

1. Supply Chain Provenance:

Attestations can verify the origin and authenticity of products, promoting transparency and security in the supply chain. This can help prevent fraud and counterfeiting, and increase consumer trust in the products they purchase.

1. Political Transparency:

Attestations can be used to verify and track political campaign donations and spending, promoting transparency and accountability in political campaigns. This can increase public trust in the political process and reduce the risk of corruption.

1. Content Authenticity:

Creators can use attestations to prove the authenticity of their work, from digital art to blog posts, research reports, and more. Attestations by 3rd parties can also verify the accuracy of the information, increasing credibility for the creator and trust for consumers.

1. Voting Systems:

Attestations can be used to conduct secure, transparent, and tamper-proof voting processes. This can increase voter confidence and ensure that election results are accurate and fair.

1. Ticketing:

Attestations can be used for ticket verification, ensuring that only authorized individuals have access to events. This can reduce the risk of ticket fraud and scalping, and increase the efficiency of ticket management.

1. Proof of X:

Attestations can be made by various third-party entities to provide verifications and proof of anything, such as proof of funds, attendance, skills, personhood, nationality, authenticity, and more. This can streamline many processes and increase the accuracy and efficiency of data verification.

1. Off-chain oracles:

Attestations can be used to provide off-chain data for smart contracts, increasing the functionality and versatility of decentralized applications.

1. Prediction markets:

Attestations can be used to provide reliable data for prediction markets, increasing the accuracy and fairness of market outcomes.

1. Land Registries and Title Documents:

Attestations can be used to verify land ownership and title documents, simplifying the transfer of property ownership and reducing the risk of fraud.

1. Health Records:

Attestations can be used to store and verify health records, ensuring the privacy and security of sensitive information and increasing interoperability between healthcare providers, access to care, speed for claims, and more.

These are just a few of the many exciting use cases of attestations. As the technology continues to evolve and mature, it's likely that new and innovative solutions will emerge, further demonstrating the versatility and power of attestations.

A future outlook on verifiable credentials and decentralized identity

As blockchain adoption continues, VCs and decentralized identity are set to play a big role in the secure exchange of information and safeguarding your digital reputation.

1. Take more control of your data:

One of the key benefits of VCs and decentralized identity is the potential to give individuals greater control over their personal information. With VCs, individuals can selectively share only the necessary information and have the assurance that their data is being stored securely. This shift towards user-owned data will allow individuals to have more control over their personal information and reduce the risk of data breaches and unauthorized access.

1. Abstraction of your identity:

The use of VCs also has the potential to change the way we think about our digital identity. Currently, individuals often use a single digital identity across multiple platforms, but in the future, the abstraction of identity could allow individuals to use different VCs for different roles they play in life. For example, a person may use one verifiable credential for work purposes, and another for personal purposes. This shift will enable individuals to maintain their privacy and security while still being able to participate in various aspects of their digital lives.

1. Better UX with your digital identity:

As the technology evolves, the user experience of accessing, managing, and sharing VCs is expected to become more intuitive and user-friendly. This will increase the overall adoption and use of the technology.

1. Expect further integrations with existing platforms:

VCs and decentralized identity are likely to become more integrated with existing systems (web2 & web3) and platforms, making it easier for individuals and organizations to utilize the technology within their existing infrastructure.

1. Security and decentralization will be favored:

As technology advances, VCs and decentralized identity systems will enhance security, protecting sensitive information and reducing the risk of breaches and fraud. The shift towards decentralization will also reduce dependence on centralized identity providers and further leverage attestations to enhance identity.

How to get started with Attestations

Getting started with attestations is easier than ever, with new technologies like the Ethereum Attestation Service and L2s starting to explore this market.

The first step is to identify where greater trust and authenticity can improve your projects. This could be around the users in your system, but can also extend beyond user authenticity to any type of verification process or area where trust is needed. Take some time to consider what information needs to be attested to and how it can benefit your project. From there, you can start exploring the various attestation services and technologies available, and choose the one that best fits your needs and requirements.

Ethereum Attestation Service

EAS is the recommended way to start your attestation journey. The contracts are elegantly simple and full of utility.

EAS is a public good for making attestations about any topic, on-chain or off-chain. It is engineered to serve as the base layer for attestations enabling a more interoperable and composable attestation future.

It's completely open-source, permissionless, tokenless, and free to use. EAS comes with an attestation explorer (similar to Etherscan) and you can even make attestations and build your own schemas using a no-code solution on the explorer site.

EAS Website

Attestation Station on Optimism

The Attestation Station is a smart contract for attestations that operates on Optimism. Its main objective is to provide an open and easily accessible platform for developers creating applications based on reputation. By allowing anyone to make attestations about addresses, it builds a vast library of both qualitative and quantitative data, which can be utilized across the OP ecosystem.

Conclusion

As the world becomes increasingly reliant on digital solutions, verifiable credentials and attestations are playing a crucial role in building trust and ensuring the accuracy of information.

It's important to remember that ERC-721, SBTs, and Attestations are not necessarily competitive solutions, but rather complimentary or compatible depending on the use case.

Attestations are still in their early days and there is a lot of room for growth and innovation. The opportunities are limitless, and we encourage everyone to start exploring and experimenting with attestations to see what new solutions they can create. Whether you're a builder, a user, or simply curious, now is the time to start discovering the potential of this exciting technology.