Provenance Metadata Registries for Asset-Referenced Tokens

Thomas Hardjono[1] and Denis Avrilionis[1]

[1]Affiliation not available

February 26, 2025

Provenance Metadata Registries for Asset-Referenced Tokens

THOMAS HARDJONO, MIT Connection Science & Engineering, USA. hardjono@mit.edu
DENIS AVRILIONIS, Compellio SA, Luxembourg. denis@compell.io

The recent EU regulation on Markets in Crypto Assets Regulation (MiCA), represents a significant progress in establishing a multi-jurisdiction framework for crypto-assets that will enable the greater participation of consumers in the digital assets industry. One type of token recognized by MiCA is the *asset-referenced token*, where the value-bearing asset and the provenance metadata supporting the token's claim are located external to the token. We discuss a number of design considerations for the on-chain and off-chain metadata for MiCA's asset-referenced tokens, with the goal of evolving towards a framework where technical standards can be developed for the assets metadata and related smart contracts technology. The EU Data Spaces provides an interesting data management paradigm that could be used for the *decentralized registries* infrastructure needed to manage the provenance metadata for various assets.

February 11, 2025

Keywords: EU MiCA; tokens; real-world assets; data spaces; asset schemas, asset profiles, registries.

1 INTRODUCTION: THE TOKENIZED ASSET PROVENANCE PROBLEM

Interest in the tokenization of assets continue to grow. Traditional financial services firms are increasingly exploring the use of digital asset tokenization to improve the management their assets. Many financial institutions are contemplating tokenization as a disruptive tool to "democratize investing" – which may improve market liquidity, reduce corruption and provide a bridge between traditional finance and crypto markets [1]. The tokenization of physical real-world assets (RWA) may also inject new life into the blockchain technology space, where until this time blockchains have been used primarily for cryptocurrency speculation.

One of the current inhibitors of the tokenization of physical real-world assets is the problem of authenticating the physical items or goods. Merely recording data on the blockchain does not solve this problem. This introduces the notion of *authenticated provenance*, namely the verifiable provenance of these assets using the various end-user applications. Additionally, regulators and government authorities need to have sufficient visibility into the "supply chains" of these real-world assets that underlie the value-bearing tokens. They also need the technical capability to validate the assertions about the state of goods or services they are auditing and overseeing [2].

One of the key challenges in the tokenization of real-world assets lies in the space between the real-world (off-chain) and the blockchain world (on-chain). More specifically, there is a pressing need for "connected data" (or metadata) to be available that spans both the off-chain and on-chain worlds, and which enables the *verifiable provenance*. The data and metadata that links a value-bearing token (located on-chain) to the real-world physical asset (located off-chain) must be managed based on a robust technical framework that also enables visibility and control from the policy and legal layers.

The goal of the current work is to discuss a *reference framework* for the management of the *metadata* that supports the tokenization of real-world assets (RWA). This metadata range from the off-chain information from the digitized paper certificates, to the tokenized equivalent information that is needed by the smart contracts. The ultimate purpose of the framework is to enable provenance

Authors' addresses: Thomas Hardjono, MIT Connection Science & Engineering, Cambridge, MA, USA. hardjono@mit.edu; Denis Avrilionis, Compellio SA, Luxembourg, Luxembourg. denis@compell.io.

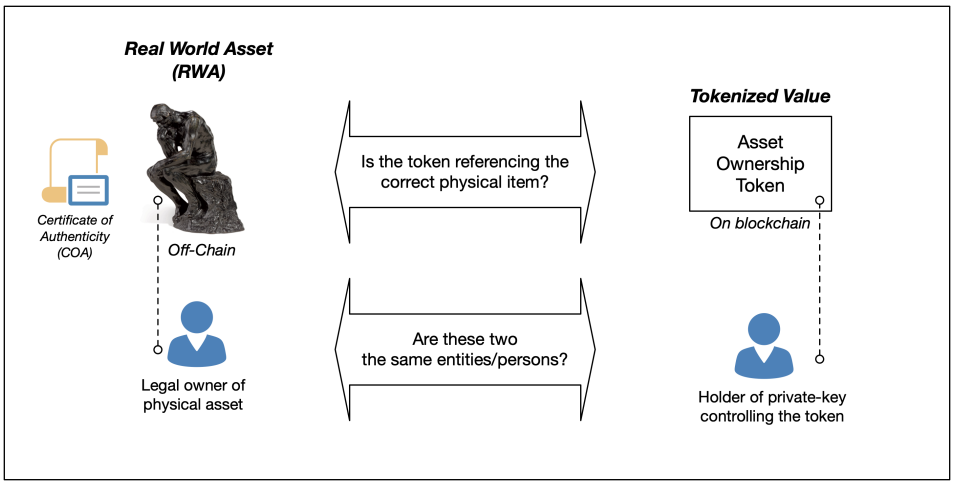

Fig. 1. Illustration of the problem with tokenizing real-world assets

of the real-world asset to be traceable and authenticated, from the on-chain token backwards to the various metadata information that assert *claims* (assertions) about the various aspects regarding the *state* of the physical real-world asset. Parts of the data and metadata that enables the verification of the provenance may require to be available in the public *data spaces*, as will be discussed below.

In approaching the problem of the tokenization of physical real-wold assets, we are constrained on two sides. On one side, there is a lack of deployed standards using modern machine-readable language (syntax) describing the real-wold physical assets. On the other side, the smart contracts that mint tokens on-chain require a standard *asset schema* to be accessible that acts as a guiding "template". Such a standard schema (for a given asset type) will enable two tokens on different blockchains to be comparable (compatible) because they are based on the same underlying asset description semantics as captured in the standard schema[1].

In the current work we discuss a number of design considerations for the assets-related metadata that are to be referenced by the MiCA asset-reference tokens (Section 2). In particular, we pay attention to the form of the metadata (on-chain and off-chain) for real-world assets. A high level discussion is given in Section 3. A major challenge with the metadata supporting the asset-reference tokens is the composition of the metadata construct, which needs to be accessible by smart contracts but at the same time provide the relevant links to enable the verifiable provenance of the metadata and the real-world asset. This is the topic of Section 4. Finally, the issue of the accessibility of the assets-related metadata (e.g. by the public) notably in the context of the EU Data Spaces is discussed in Section 5.

In the current we have sought to discussed issues in a general manner, avoiding as much as possible the technical terms which may be blockchain-specific. However, the reader is expected to have some basic understanding of the core concepts blockchain technology (e.g. smart contract code in a given blockchain has access to data only on the same blockchain).

[1]Preliminary work on standardizing the syntax for expressing asset definition schemas and their subsets (called "profiles") can be found in [3].

2 THE EU MICA REGULATION AND THE EU DATA SPACES

One of the recent significant advance in the regulation of digital assets was the European Union *Markets in Crypto Assets* regulation (MiCA) which was finalized in 2023 [4]. MiCA is significant because is represents the first framework to singularly seeks regulate the crypto-asset markets across multiple jurisdictions. It is purposely aimed at replacing the various domestic regulations for the crypto-asset markets that have been developed by many EU Member States. At the same time, many leaders in the EU have realized that the digital economy relies on the sharing of insights [5] that are computed based on data that are located cross different national boundaries of the EU member states. Increasingly, applications of artificial intelligence (AI) requires machine learning algorithms in the learning phase to utilize large amounts of quality data. On one hand, next generation transformers and large learning models (LLM) require access to data that may be physically distributed in silos. On the other hand, the EU GDPR has established data privacy rules to protect citizen's privacy across all EU member states [6].

Briefly, the EU MiCA regulation defines a crypto-asset as [4]:

> *"a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology"*
> (see Article 3(5)).

More broadly, however, MiCA has provisions aimed specifically at increasing the transparency and disclosure of information related to the issuance of crypto-assets to the general public. MiCA also defines a number of provisions covering the the authorization, operational supervision, and the the governance of crypto-asset service providers (CASPs). In the MiCA parlance, the CASPs are service providers who will issue *asset-referenced tokens* (ART) and/or *electronic money tokens* (EMT). Other provisions have also been written to prevent insider dealing, unlawful disclosure of inside information and market manipulation related to crypto-assets.

The asset-referenced tokens (ART) in MiCA is of particular interest in the current work because asset-referenced tokens promises opportunities for new types of tokens that are backed by real-world assets (RWA). The asset-referenced tokens ("ART tokens" for short) must carry pointers that "reference" verifiable provenance information (data) regarding the real-world assets located off-chain. We interpret the word "referenced" here to mean "pointing to" authentic (correct) data regarding the real-world asset, namely other documentation that assert or claim the true the existence the real-world asset. The trust model underling the asset-referenced tokens is therefore significantly different from electronic money tokens (EMT) in MiCA – including CBDCs or Stablecoins. In the case of the electronic money tokens the economic value is carried within (or directly represented) the digital token itself. Possession or control over the token on-chain (via cryptographic means or methods) signifies ownership.

The notion of *data spaces*[2] as understood within the EU context pertains to common data infrastructures and governance frameworks which facilitates data pooling, access and sharing. These data spaces would be open for the participation of all organizations and individuals, have a secure and privacy-preserving infrastructure to pool, access, share, process, and use data [9].

Given the backdrop of the EU data spaces, it is likely that some (or all) of the data (metadata) for authenticating the provenance of the RWA linked to an asset-referenced token maybe required to be available in a designated common data space.

[2]A similar notion has been developed in Japan following the OECD, referred to as the *Data Free Flow with Trust* (DFFT) [7]. The idea is that distributed data stores throughout Japan's institutions (public and private) need to be better interconnected in a secure fashion to enable data to be utilized for the public good. The "connectivity" of data for the public good is discussed at length in [8].

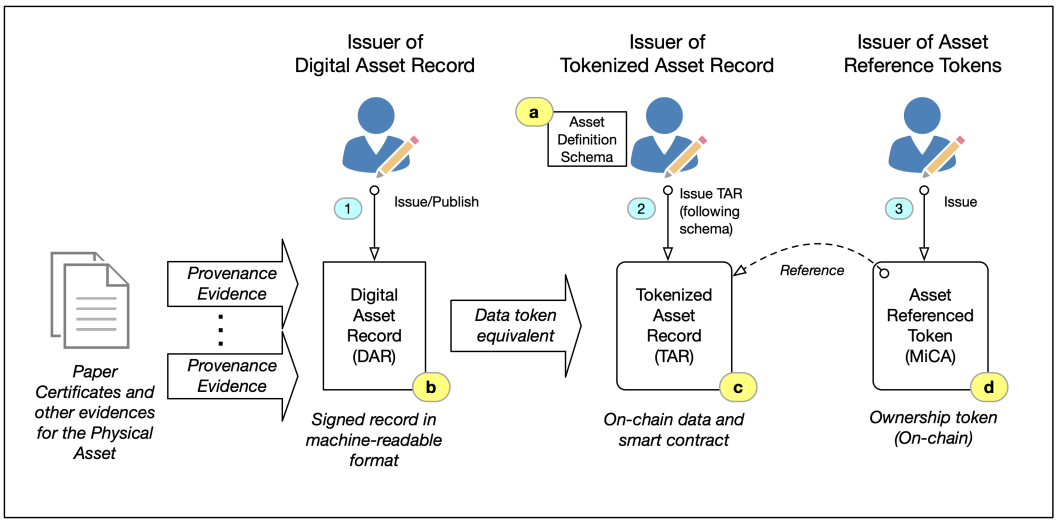

Fig. 2. Overview of the component metadata underlying tokenized real-world assets

- *EU data spaces core to the EU digital economy*: Since asset-referenced tokens may evolve to be sizable enough to influence the EU economy, the assets-related data (metadata) may be required to be accessible in the EU common data spaces (perhaps with additional access authorization).
- *Technical standards for assets metadata accessible in the EU data spaces*: The chain of trust and provenance – from the token backwards to the physical asset that exists prior to the token – must be captured and represented syntactically and semantically using technical standards that are meaningful for the whole of the Internet. These technical standards should be agnostic to the DLT/blockchain implementation and specific technological solutions.
- *Standard interfaces to access assets metadata in the EU data spaces*: The EU data spaces may require that the data (metadata) that is the basis for the chain of trust and provenance must be accessible through technical implementations of the data spaces. Decentralization and protected access (e.g. protected APIs) are important computing constructs that swerve towards this equal accessibility of data.

These points motivate the need to develop a coherent reference framework for managing the data (metadata) that underlie the validity of the claims carried with the the asset-referenced tokens. In the next section we discuss the fundamental concepts around the manageability of the data underling the asset-referenced tokens.

3 DESIGN CONSIDERATIONS FOR ASSET PROVENANCE METADATA

One of the major gaps today in the tokenization of physical real-world assets (RWA) is the lack of a technical reference model that enables physical assets to be tokenized with a complete *provenance supply-chain transparency*[3]. In other words, for a token to be recognized legally within a jurisdiction

[3]Several industry efforts are underway to develop a supply-chain transparency architecture and services for different sectors of the economy. These include semi-conductors, software/firmware bill of materials (BOM) [10], agriculture and food supply-chains and others. In the United States this effort has been driven by the recent White House Executive Orders (EO) covering the safety of the supply-chains [11] and the EO covering national cybersecurity [12]

there needs to be a complete chain-of-custody evidence for every step of the process. We refer to the set of provenance information for a tokenized asset as its *provenance metadata*, as shown in Figure 2.

In this section we briefly discuss a number of design considerations for the management of the authenticated provenance metadata, both on-chain and off-chain.

3.1 Standardized asset definition schemas

In order for the value associated with two different asset-reference tokens (e.g. for a weight of gold) to be comparable, the metadata underlying the two tokens must refer to the same class of physical assets (i.e. valuable metals) and be structured in a compatible manner. In other words, the two metadata structures must be published using the identical (or near identical) information "template" that must itself by published by a legally authorized entity. We refer to this information template as the *asset definition schema* [3, 13]. Subsets of an asset schema that is narrower in scope are referred to as *asset profiles*. The notion of the asset schema is shown as Item-(a) in Figure 2.

Using the previous example, if two asset-reference tokens pertains to 1 kilogram of gold with 99.99 percent purity, then the asset schema must define this requirement. When the issuer of an asset-reference token (for 1 kg of gold) seeks to mint the token, the smart contract invoked by the issuer must refer to (include a hash of) the corresponding asset schema file. By invoking the smart contract, the issuer is asserting that it is the legal owner of the physical real-world asset (the 1 kg of gold).

The asset definition schemas determines what authenticated provenance metadata information about the real-world asset is needed, prior to approaching the blockchain. In Figure 2 this set of authenticated provenance metadata is referred to as the *Digital Asset Record* (DAR), and is shown as Item-(b) in Figure 2. The topic of the digital asset record will be discussed further in Section 4.

3.2 Independence of provenance metadata from ownership tokens

In order for an asset referenced token to retain value and change ownerships over-time, the authenticated provenance metadata that underlies the token must not be modifiable by the current owner of the token. This implies that the authority to publish the provenance metadata for a tokenizable real-world asset must be independent from the entities who exchange or trade the tokens. Using a mundane every day example, the land registry that records the existence of a piece of property (e.g. house) must be a different entity from the buyers and sellers of the property. For lack of a better name, in Figure 2 the digital asset record (as the digitized authenticated provenance metadata) is issued by the *DAR-Issuer* in Step-(1)

As alluded to before, the authenticated provenance metadata represented by the DAR is used to asses the truthfulness of the state of the real-world asset, such as its true existence in the physical world, its current location (e.g. held by a physical depository or escrow entity), and its current physical condition (e.g. as new, slightly damaged, etc).

To fully appreciate this subtle advance by the EU MiCA regulation, it is instructive to understand how the current electronic book entry mechanism is used to securitize paper certificates and how the centralized certificate depository entities are crucial to the function of the traditional *Delivery versus Payment* (DvP) model of trade [14, 15]. Historically, financial assets have been represented by "securitized paper" certificates and other similar certificates. The task of immobilizing physical assets and representing them as securitized paper has traditionally been the task of the depositories (e.g. DTCC [16, 17]). With the advent of digital computers and databases in the 1960s many of the paper-based securities have been "digitized" as *electronic book entries* in these databases. The traditional electronic book entry represents the digitization of paper securities within the computer system of the depository entity. It represents the electronic records of the legal ownership of

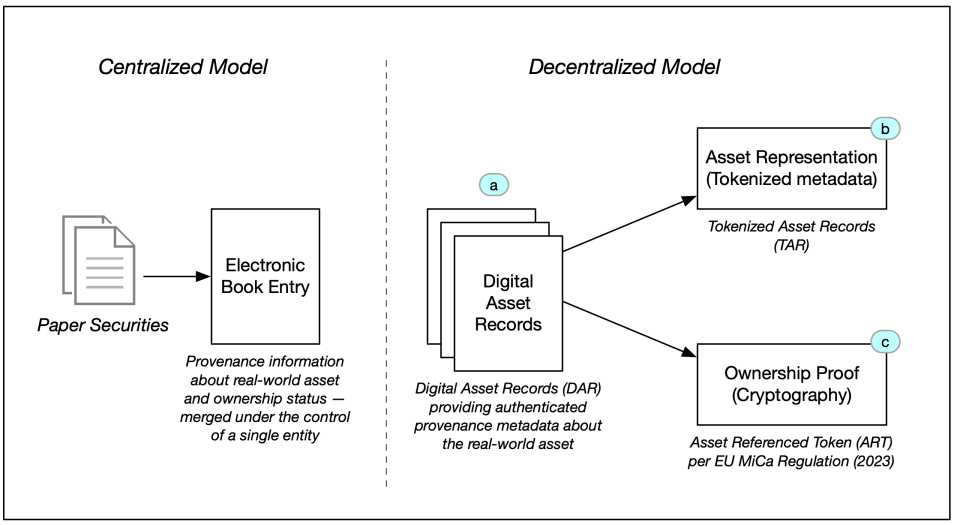

Fig. 3. Summary of the independence of provenance metadata (a) from asset referenced token (c)

investments, such as stocks and bonds. In this traditional model, the owner does not receive the physical certificates of ownership. When the corresponding securities are traded, the new ownership is recorded in the books of the financial institution of the buyer (i.e. in the buyer's account). This has the advantage that the paper certificates need not be physically moved to the new owner. A system of registration is often used whereby the new owner can register their securities directly in book-entry form onto the registration system. The role of the depository entity during a trade (such as DvP) is to provide a guarantee to the buyer (e.g. buyer's financial institution) that the securitized paper truly exists and is owned by the seller. This guarantee is core part of the clearing process in cases such as DvP.

3.3 Smart contract accessible provenance metadata

In order to enable smart contract technology to mint asset referenced tokens on the blockchain, there needs to be a contract-accessible provenance metadata available on the blockchain. In practical terms, this means that the on-chain provenance metadata must be formatted according to the specific data model used by the target blockchain. Furthermore, the piece of software (i.e. separate smart contract) that records the provenance metadata on the ledger of the blockchain must be verifiable by anyone with access to the blockchain. The combined on-chain provenance metadata and the code responsible for recording it to the blockchain is referred to as the Tokenized Asset Record (TAR), which is shown as Item-(c) in Figure 2.

The current design of DLT systems and blockchains allow for *executable code* to be available on the ledger in the form of the *smart contract*. This feature is one of the attractive advances in blockchain technology, first implemented by the Ethereum Virtual Machine (EVM) design [18]. It is this smart contract capability that excites many from the traditional financial industry who see this capability as paving the way for a future "programmable money" (see [19, 20]).

4 TOKENIZING THE ASSETS-RELATED METADATA

In this section we provide some design considerations for the technical construct that bridges between the off-chain metadata related to the real-world asset with the on-chain smart contract

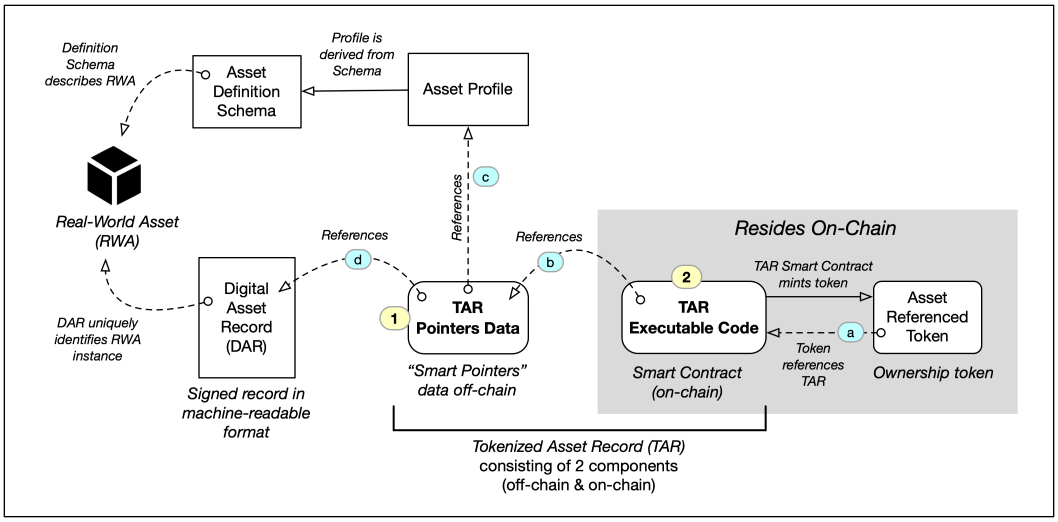

Fig. 4. Overview of the Tokenized Asset Record (TAR), consisting of: (1) the TAR pointers data, and (2) TAR executable code (smart contract) that mints the schema-compliant token

that "tokenizes" the relevant parts of that metadata into an equivalent information recorded on the blocks of the ledger of the blockchain. We then propose a new construct called the *tokenized asset record* (TAR) that is composed of an on-chain part and an on-chain part. The smart contracts utilizes the asset schema (or profile) to mint an asset reference token that is compliant to the asset schema.

The the *tokenized asset record* (TAR) consist of the two parts that operate together (see Figure 4):

- *TAR smart contract (executable code)*: The first part of the TAR is an on-chain smart contract that is designed specifically to follow the "template" that is specified by the asset profile (schema) in use. Its goal is to mint an asset reference token (ART) that is compliant to the schema or profile that is legally recognized within the given jurisdiction[4]. Among others, the smart contract must ensure that the relevant fields demanded by the schema or profile is present in the resulting token. The TAR smart contract is illustrated as Item-(2) in Figure 4.

  For example, if the asset schema pertains to the real-estate industry/vertical and the asset profile requires the ID-number of the physical real-estate property to be shown in the token, then the TAR smart contract must include this property ID-number in the resulting token on-chain.

  In order to know where to fetch a copy of the signed asset schema or profile, the TAR smart contract must rely on the TAR smart pointers.

- *TAR smart pointers (pointer data file)*: The second part of the TAR is off-chain data (file) containing the set "links" (e.g. references or hash values or URLs) that would enable the easy validation of the information fields within the minted token. These set of links is referred to as the *smart pointers*. This is shown as Item-(1) in Figure 4.

[4]For convenience of discussion, in the current work we assume that the jurisdiction that legally recognizes the physical real-world asset is the same jurisdiction that legally recognizes the asset definition schema and derived profiles for that real-world asset. However, this does not preclude cases where other jurisdictions also adopt or legally recognize the published asset definition schemas/profiles in the origin jurisdiction.

Unlike executable code, the TAR smart pointers must be resolvable links (e.g. URLs) whose endpoints are located off-chain. This is because much of the provenance metadata information for a physical real-world asset is currently located off-chain.

As mentioned above, *verifiable provenance* of an asset reference token is a fundamental requirement of the EU MiCA Regulation. The proposed design of the TAR in Figure 4 provides a possible solution to the need to trace the provenance of a token (based on a legally issues schema/profile) back to the physical real-world asset in a technically sound manner.

The process of verifying an asset reference token on the blockchain starts from the token backwards to the asset schema/profile, as shown in the reference links in Figure 4:

- Reference Link-(a): The token minted on the blockchain carries the *smart contract identifier* (contract address) on the blockchain, enabling any entity with access to the blocks of the shared ledger to look-up the smart contract on the same blockchain as the token[5]. This is shown as Link-(a) in in Figure 4 that connects the token to its minting smart contract on the same blockchain.
- Reference Link-(b): In order to locate the asset schema/profile (a signed file) on the Internet, the TAR smart contract by design carries the URL address of the TAR Pointers Data (a signed file). This means that a verification software that has read-access to the blocks of the shared ledger on the blockchain can read the URL address from the contract code and resolve that address to the TAR Pointers Data file somewhere on the Internet. The URL address is represented as Link-(b) in Figure 4.
- Reference Link-(c) and Link-(d): Once located, the TAR Pointers Data file contains the URL address of the asset schema/profile file (a signed file) and the URL address of the digital asset record (DAR) (a signed file). See as Item-(b) in the previous Figure 2.

5 DATA SPACES: DECENTRALIZED REGISTRIES OF ASSETS METADATA

Continuing from the discussion in the previous section and from Figure 4, there is a fundamental need for the relevant metadata information underlying a given asset referenced token to be accessible easily by parties who may a legitimate interest or requirement in validating the veracity of the claims made in the metadata. Therefore, some *metadata registries*[6] will be needed to manage the various metadata types from different sources throughout the lifecycle of the MiCA asset reference token. We believe that with the growing interest among the crypto-assets communities around the world in the tokenization of real-world assets [1], there is also a corresponding economic opportunity to develop, standardize and deploy the Web3 decentralized digital infrastructures to manage the various phases in the lifecycle of the assets-related metadata. In this section, we briefly discuss some general requirements for the metadata registers with the backdrop of the EU Data Spaces.

The following is a short list of general requirements – legal and technical – for the management of the metadata and the operations of the registries:

[5]We address the problem cross-chain asset transfers in a separate work [21, 22]. In essence, when a token is transferred from an origin blockchain to a destination blockchain using a transfer protocol such as SATP [23] both the token and TAR must be "moved" to the destination blockchain. The transfer-gateway in the destination blockchain must utilize the same contract code to mint the new asset reference token in the destination blockchain. This points to the need for the industry to develop a standard syntax citeHazardHardjono2016 for smart contract code that can be "compiled down" to different blockchains.

[6]We use the "registry" in the broadest sense of the meaning, without pointing to any specific technology that bay be utilized to implement a registry.

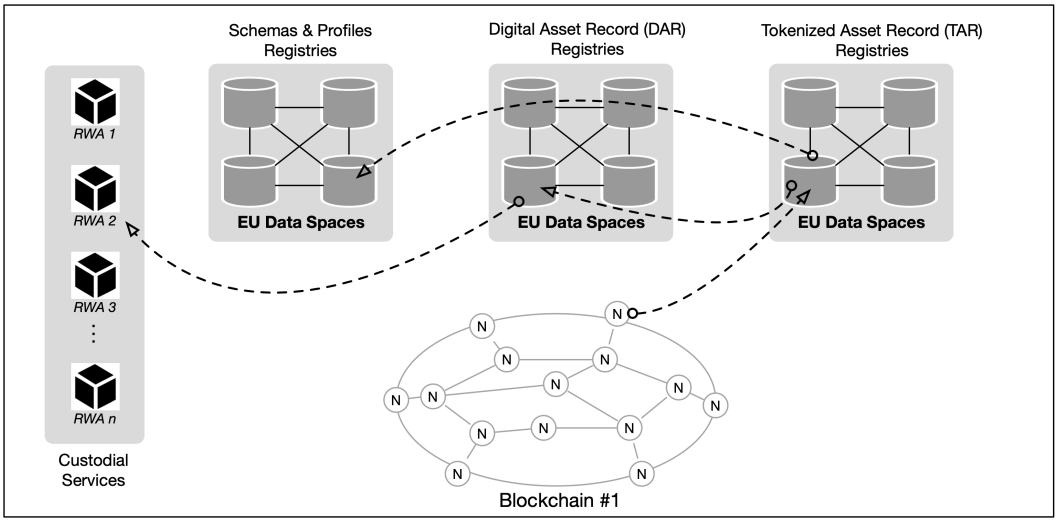

Fig. 5. Illustration of the ustlization iof the EU Data Spaces notion for schema/profile registries, DAR registries and TAR registries

- *Jurisdiction-based asset definition schemas*: The top-level asset definition schema should be issued and signed by the relevant authority in a given jurisdiction. Once published, these definition schemas are expected to be only rarely updated.
- *Independence to published industry-specific asset profiles*: Communities must be provided with the freedom to issue and manage their own industry-specific asset profiles, indicating the jurisdiction of validity and the carrying the identifier of the top-level asset definition schema upon which the profile is based.
- *Clear identification and authorization of issuers*: All entities who issue and manage asset definition schemas, profiles, digital asset records (DAR), and tokenized asset records (TAR) must have an unambiguous digital identity and authorization evidence.
- *Persistence of all versions of published assets-related metadata*: All versions asset definition schemas, profiles, DARs and TARs must be made accessible and persistent in the long-term. When a revision of a schema/profile is published, the prior version must remain equally accessible. This is because asset referenced tokens may still be circulating which were minted based on a previous (older) version of a given schema/profile.
- *Standardized registry access protocol and interfaces*: The metadata registries must provide a standard set of access interfaces (e.g. REST APIs), operations and management protocols, independent of the technology used to implement the registry.
- *Service reliability and persistence*: The metadata registries must have a high degree of reliability, and must persist the schemas/profiles, DARs and TARs over a long duration of time (i.e. years or decades). The legal requirements in some jurisdictions (e.g. taxation rules in the US) man demand these artifacts to be available for several years (e.g. seven years).

6 CONCLUSION

In the current work we have provided some design considerations for the provenance metadata and their management for the asset referenced tokens defined in the 2023 EU MiCA regulation. The *asset definition schema* – written in a machine-readable format – provides the basis for expressing the tokenizable real-world assets in a given jurisdictions. The *asset profiles* is a narrowing of a schema, which may be utilized by different industries or communities. The off-chain records of the instances of the real-world asset is digitized and represented as the *digital asset record*. In order to bridge between the off-chain metadata and the on-chain metadata, a composite *tokenized asset record* is proposed. The first part of the tokenized asset record is an off-chain file containing a collection of pointers or URLs for tracing other relevant metadata for the on-chain token. The second part of the the tokenized asset record is a smart contract that mints the MiCA asset referenced token representing the real-world asset.

The current work also proposes the establishment of decentralized *metadata registries* for these various asset schemas, profiles, and records. These registries must be designed to enable and incentivize new services that can develop, standardize and deploy the Web3 decentralized digital infrastructures to manage the various phases in the lifecycle of the assets-related metadata.

REFERENCES

[1] J. Lopez, T. Fujiwara, and S. Smith, "Tokenization Signals Business Opportunities," Gartner, Research Report G00811601, June 2024.

[2] S. Sicular, "How to Detect Fakes in a Zero-Trust World Using Artificial Intelligence and Blockchain," Gartner, Research Report G00730302, June 2023.

[3] D. Avrilionis and T. Hardjono, "SATP Asset Schema Architecture for Asset Exchange," Internet Engineering Task Force (IETF), Draft Specifications, December 2024. [Online]. Available: https://datatracker.ietf.org/doc/draft-avrilionis-satp-asset-schema-architecture/

[4] European Commission, "Regulation (EU) 22023/1114 of the European Parliament and of the Council of 27 April 2016 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937," *Official Journal of the European Union*, vol. L150, pp. 1–166, June 2023.

[5] T. Hardjono and A. Pentland, "MIT Open Algorithms," in *Trusted Data - A New Framework for Identity and Data Sharing*, T. Hardjono, A. Pentland, and D. Shrier, Eds. MIT Press, 2019, pp. 83–107.

[6] European Commission, "AI Factories," (Site accessed 14 January 2025). [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/ai-factories

[7] Japan Digital Agency, "Data Free Flow with Trust (DFFT)," (Site accessed 14 January 2025). [Online]. Available: https://www.digital.go.jp/en/policies/dfft

[8] A. Pentland, *Social Physics*. Penguin Books, 2015.

[9] European Commission, "Common European Data Spaces," (Site accessed 14 January 2025). [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/data-spaces

[10] A. Regenscheid, "Platform Firmware Resiliency Guidelines," National Institute of Standards and Technology, NIST Publication SP 800-193, May 2018. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-193/final

[11] The White House, "Executive Order on America's Supply Chains," February 2021. [Online]. Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/

[12] ——, "Executive Order on on Improving the Nation's Cybersecurity," May 2021. [Online]. Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[13] D. Avrilionis and T. Hardjono, "SATP Asset Profiles for Asset Exchange," Internet Engineering Task Force (IETF), Draft Specifications, December 2024. [Online]. Available: https://datatracker.ietf.org/doc/draft-avrilionis-satp-asset-profiles/

[14] BIS, "Delivery versus Payment in Security Settlement Systems," Bank for International Settlements, BIS Report, September 1992. [Online]. Available: https://www.bis.org/cpmi/publ/d06.pdf

[15] M. L. Bech, J. Hancock, T. Rice, and A. Wadsworth, "On the future of securities settlement," Bank for International Settlements, BIS Quarterly Review, March 2020. [Online]. Available: https://www.bis.org/publ/qtrpdf/r_qt2003i.htm

[16] DTCC, "Project Whitney: Case Study," Depository Trust & Clearing Corporation, DTCC Report, May 2020. [Online]. Available: https://perspectives.dtcc.com/articles/project-whitney

[17] ——, "Project Ion: Case Study," Depository Trust & Clearing Corporation, DTCC Report, May 2020. [Online]. Available: https://perspectives.dtcc.com/articles/project-ion

[18] V. Buterin, "Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform," Bitcoin Magazine, Report, January 2014, https://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211/.

[19] I. Aldasoro, S. Doerr, L. Gambacorta, R. Garratt, and P. K. Wilkens, "The tokenisation continuum," Bank for International Settlements, BIS Bulletin No. 72, April 2023. [Online]. Available: https://www.bis.org/publ/bisbull72.htm

[20] BIS, "Blueprint for the future monetary system: improving the old, enabling the new," Bank for International Settlements, BIS Annual Economic Report, June 2023. [Online]. Available: https://www.bis.org/publ/arpdf/ar2023e.pdf

[21] T. Hardjono, A. Lipton, and A. Pentland, "Towards an Interoperability Architecture Blockchain Autonomous Systems," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1298–1309, June 2019. [Online]. Available: doi:10.1109/TEM.2019.2920154

[22] T. Hardjono, "Blockchain Gateways, Bridges and Delegated Hash-Locks," February 2021. [Online]. Available: https://arxiv.org/abs/2102.03933

[23] T. Hardjono, M. Hargreaves, N. Smith, and V. Ramakrishna, "Secure Asset Transfer Interoperability Architecture," Internet Engineering Task Force (IETF), Draft Specifications, June 2023. [Online]. Available: https://datatracker.ietf.org/doc/draft-hardjono-sat-architecture/