HOOT INNOVATION

TECHNOLOGY AND PRODUCT ARCHITECTURE OF

TOKENIZED PRECIOUS METALS

HOOT LEGAL TEAM

Technology and Product Architecture of Tokenized Precious Metals.

By: Hoot Legal Team

3.1 Introduction to Tokenized Metals Technology

Tokenized precious metals are digital representations of physical gold, silver, and other metals on a blockchain. A robust technology and product architecture is critical to ensure that each token reliably corresponds to real metal in custody, while allowing secure, compliant, and efficient transactions. This module provides an in-depth look at how tokenized metal assets are created, issued, and managed from a technical perspective. We examine the blockchain protocols used, smart contract designs, custody models, and the infrastructure that supports these tokens. We also explore **custodial vs. non-custodial models**, highlighting the role of digital asset custodians and wallet frameworks in maintaining security. In addition, we discuss relevant token standards and how they are implemented in real-world use cases. Case studies from around the world – including the UAE – will illustrate successful and failed implementations. Finally, we address key considerations like scalability, compliance-by-design smart contracts, interoperability mechanisms, and the use of blockchain analytics for auditability and regulatory oversight. The content is technical and detailed, aimed at an audience of institutional investors, regulators, developers, and legal professionals interested in the **state-of-the-art as of 2025**.

3.2 Blockchain Platforms for Tokenized Metal Assets

Tokenized metal projects utilize a variety of blockchain platforms, each offering different trade-offs in terms of security, scalability, cost, and feature sets. The choice of blockchain impacts the ease of integration with other systems, transaction fees, and speed. Below we overview the major blockchain protocols used for tokenized gold and metals:

- **Ethereum (Mainnet)** – Ethereum has been the dominant platform for asset tokenization due to its mature smart contract capabilities and broad ecosystem. Many gold-backed tokens (like PAX Gold and Tether Gold) are implemented as ERC-20 tokens on Ethereum for maximum compatibility with wallets, exchanges, and DeFi protocols. Ethereum's security and decentralization are strong, but its network congestion and gas fees can be high. For example, PAX Gold (PAXG) chose Ethereum to leverage the large user base and liquidity, despite gas costs, making it **immediately interoperable** with a wide range of services. Ethereum's transparency also allows anyone to verify token contracts and balances via block explorers.
- **Polygon (Ethereum Layer 2 & Sidechains)** – Polygon offer higher throughput and lower fees while inheriting or complementing Ethereum's ecosystem. Some tokenization projects deploy on Polygon or consider **Layer-2 scaling** to improve accessibility for smaller transactions. For instance, an issuer could deploy an **ERC-20 gold token on Polygon** to enable cheap transfers for retail users, while still maintaining an Ethereum mainnet token. Multi-chain strategies are emerging: Paxos, for example, has indicated that PAXG's proxy contract architecture could allow deployment on Layer-2 networks or issuing bridged tokens if

demand arises. The key challenge for multi-chain or cross-chain tokenization is ensuring the total supply across all networks remains fully backed and **preventing double-counting of collateral**. Typically, issuers either natively issue on multiple chains (tracking total supply centrally) or use bridges to move tokens between chains. By 2025, we see a trend of token issuers cautiously expanding to Layer-2s and sidechains to combine Ethereum's trust with better **scalability**.

- **Stellar** – Stellar is a payment-oriented blockchain known for low-cost, fast transactions, making it attractive for asset tokens intended for frequent transfers or micropayments. Notably, the Kinesis platform uses technology derived from Stellar for its gold and silver tokens (KAU and KAG). Kinesis created a custom blockchain (forked from Stellar) where each KAU represents 1 gram of gold and each KAG 1 troy ounce of silver. Stellar's built-in decentralized exchange and **issuer-enforced trust lines** allow controlled issuance of asset-backed tokens. Issuers can require that wallets be authorized before holding tokens, which is useful for compliance. Projects like Kinesis leverage these features to ensure only fully KYC'd users hold the tokens, effectively making the token **permissioned on a public ledger**. Stellar's consensus protocol (Federated Byzantine Agreement) provides **high speed** (transactions settle in ~5 seconds) which is advantageous for using gold tokens in everyday payments. However, Stellar's ecosystem is smaller than Ethereum's, so interoperability with DeFi or external platforms can be limited.
- **Ripple XRP Ledger (XRPL)** – The **XRPL**, like Stellar, was designed for efficient payments and also supports issuing custom assets. XRPL has seen growing interest for tokenizing real-world assets, including precious metals. For example, in 2024, **Meld Gold** announced integration with XRPL to issue tokenized gold and silver, each token representing 1 gram of the metal held with reputable vault providers. **XRPL** offers a decentralized exchange and auto-bridging of liquidity, which could enable gold tokens to be traded against XRP or other tokens natively. It also features built-in compliance tools such as the ability for issuers to freeze assets or require authorization, similar to Stellar. By using XRPL's reliability and upcoming features (like federated sidechains and an EVM sidechain), token issuers like Meld aim to tap into both the crypto-native XRPL community and interoperability with EVM-based smart contracts. Ripple's broader network (RippleNet) typically refers to bank/payment integrations, but the **open-source XRPL** is where these tokens live. XRPL's consensus (Unique Node List mechanism) provides **fast finality** (~4 seconds). One limitation has been that XRPL's scripting is not as flexible as Ethereum's smart contracts; however, for straightforward gold tokens, XRPL's proven payment infrastructure is a good fit. It's notable that even large institutions are taking interest – for example, HSBC's recent tokenized gold offering is built on a private distributed ledger, but Ripple's custody technology (via its acquisition of Metaco) is being tapped for secure storage.
- **Enterprise and Other Blockchains** – Apart from public networks, some tokenization initiatives use permissioned or specialized blockchains:
  - **XinFin XDC Network** – XDC is an EVM-compatible blockchain optimized for enterprise and trade finance. In the UAE, the Dubai Multi Commodities Centre (DMCC) partnered with ComTech Gold to issue gold-backed tokens (CGO) on the XDC network. Each CGO token represents 1 gram of gold, with the physical bars held in DMCC-approved vaults and tracked via DMCC's Tradeflow platform. XDC provides low transaction costs and quick settlement, which are ideal for a high volume of small gold trades (each token is only worth the price of 1g of gold). The use of XDC also suggests an enterprise focus – aligning with trade finance systems and UAE's commodity trade infrastructure.

- **Tezos** – Tezos is a smart contract platform that some European institutions have explored for tokenization due to its on-chain governance and institutional-grade security. For example, Luxembourg-based VNX issued its VNX Gold token (VNXAU) on Ethereum and later expanded to Tezos and other chains. Swiss firms have even defined a token standard (DAR-1) on Tezos targeting asset tokenization. While Tezos is less commonly used for gold than Ethereum, it's **gaining traction in regulated token offerings** thanks to partnerships with Swiss banks and its formal verification approach to smart contracts.
- **Corda and Hyperledger (Private DLTs)** – Some gold token systems run on private or consortium ledgers. For instance, **Tradewind's VaultChain Gold** used a permissioned blockchain to record ownership of gold in the mint's vaults. This was not a public token tradable on decentralized exchanges, but an enterprise solution where participants (brokers, dealers, investors) had accounts on the platform. Another example is **HSBC's Gold Token** launched in Hong Kong (2024) – it runs on an HSBC proprietary distributed ledger and allows bank customers to buy fractional gold (each token is 0.001 oz) via the bank's online banking app. These private implementations emphasize integration with traditional systems (e.g., core banking, exchange clearing) and compliance, at the cost of open interoperability. They are important in showing how major institutions approach tokenized metals within a closed network environment.

Each blockchain platform brings unique advantages. Ethereum and similar public chains excel in **interoperability and liquidity**, letting gold tokens participate in the broader crypto economy (trading on exchanges, used as collateral in DeFi, etc.). Alternatives like Stellar or XDC offer **efficiency and enterprise integration**, which can be better for payments and trade use cases. Some projects even adopt a **multi-chain approach**, issuing the token on multiple networks to combine benefits – for example, a token might be issued on both Ethereum (for DeFi access) and a low-cost chain like Tron or Stellar (for retail payments). Tether Gold (XAUT) follows this approach by issuing tokens on Ethereum (ERC-20) and Tron (TRC-20) concurrently, giving users flexibility in how they transfer and use their gold. In all cases, the core principle remains the same: the on-chain token supply must correspond to an equivalent **real-world supply of physical metal in custody**.

3.3 Smart Contract Design and Token Standards

The design of smart contracts for tokenized metals focuses on ensuring **secure, compliant, and verifiable representation of ownership**. Key considerations include the choice of token standard (for fungibility and metadata), inclusion of administrative functions (minting, burning, pausing transfers), and any special features like fees or compliance rules coded into the contract. This section examines the prevalent token standards and smart contract architectures used in gold and precious metal tokens.

3.3.1 Fungible Token Standards (ERC-20 and ERC-1155)

Most gold and silver tokens are designed to be **fungible**, meaning each token of the same type is interchangeable with another (just as any two 1-ounce gold coins are interchangeable). The Ethereum ERC-20 standard is by far the most widely used for fungible tokens and has been the go-to choice for implementations like PAXG, XAUt, and others. ERC-20 defines a common interface for token contracts, including functions for transferring tokens, checking balances, and approving allowances. By conforming to ERC-20, tokenized metals can be easily integrated with exchanges,

wallets, and DeFi protocols out-of-the-box. For example, PAX Gold's contract implements the standard `transfer`, `transferFrom`, and `balanceOf` functions, enabling it to be listed on Uniswap, held in MetaMask, etc., just like any ERC-20.

In some cases, projects might consider ERC-1155, the multi-token standard, which can handle multiple token types (fungible or non-fungible) in one contract. ERC-1155 could be useful if a single platform wants to tokenize multiple metals (gold, silver, platinum) or different denominations under one contract address. It offers efficiency gains by grouping operations. However, to date most metal tokens have stuck with separate ERC-20 contracts per asset for simplicity. One real-world example of a multi-token approach is the Aurus platform, which tokenizes gold (AWG, 1g tokens), silver (AWS), and platinum (AWP), and also has a revenue token (AWX). Aurus could theoretically use ERC-1155 to manage all these under one contract, though their early implementations were ERC-20. The decision often comes down to **ecosystem support** – ERC-20 remains more universally supported, while ERC-1155 is newer and primarily used for gaming and NFT marketplaces (though it is fully capable of fungible token operation).

Another aspect of fungible token design is **decimal precision**. Precious metal tokens usually represent divisible ownership (e.g., one can own 0.5 of a 1-ounce token). ERC-20 allows setting a **decimals** parameter. Most gold tokens use 18 decimals like Ethereum's default, even if not all that precision is needed. PAX Gold, for instance, uses 18 decimals but effectively only goes down to 0.01 PAXG (which is 0.01 ounce, about $60+) as the smallest unit Paxos will sell or redeem. Tether Gold is divisible up to 6 decimal places (1 XAUF = 1 ounce, smallest unit 0.000001 oz), reflecting a high granularity (sub-milligram ownership) to accommodate various investment sizes.

3.3.2 Smart Contract Features and Upgradeability

Token issuers often include additional smart contract features beyond the basic standard to meet operational and regulatory needs:

- **Minting and Burning Controls:** Since tokenized metals must remain fully backed by physical reserves, the contracts typically include restricted functions to **mint** new tokens (when new metal is added to vaults) and **burntokens** (when metal is redeemed or removed). These functions are usually protected so that only the issuer or an authorized custodian address can call them. For example, Paxos's PAXG contract has functions that Paxos calls to mint new tokens when gold is acquired and burn tokens when someone redeems PAXG for gold. This ensures on-chain supply always matches off-chain gold. The rules for mint/burn are often off-chain (e.g., subject to KYC/approval), but the contract enforces that no one else can arbitrarily increase the supply.
- **Pausability and Freezing:** To comply with regulations and prevent illicit use, many token contracts include the ability to pause transfers or freeze certain addresses. Paxos built in the capability to **freeze tokens** held by specific addresses (blacklisting) or even pause all transfers in extraordinary circumstances. This is analogous to features in stablecoins like USDC or USDT, where an issuer can blacklist an address involved in crime or under sanctions. Tether Gold likely has similar functionality, given Tether's USD stablecoin contract supports address blacklisting. These functions raise decentralization concerns, but for regulated asset tokens, they are often a must-have to satisfy law enforcement and **OFAC compliance** requirements. Typically, they are used sparingly – for instance, PAXG has never been globally paused and freezes would only occur if mandated by authorities or court orders.

- **Fee Mechanisms:** Some token issuers incorporate transaction fees into the smart contract to cover custody or management costs. PAXG's original design included a tiny fee of 0.02% on transfers, which would be sent to a Paxos-controlled fee account. In practice, Paxos set this fee to zero in 2021 to make on-chain transfers free (apart from Ethereum gas). The ability to adjust fees via the contract gave Paxos flexibility to introduce or change fees if needed (within limits disclosed in their terms). Other tokens might charge issuance/redemption fees off-chain instead; for example, Tether Gold charges a one-time 25 bps fee at purchase or redemption (off-chain) but no on-chain transfer fees. If fees are imposed on-chain, smart contracts must be carefully coded to collect and disburse them without vulnerabilities.
- **Upgradeability:** Unlike Bitcoin, Ethereum allows smart contracts to be designed such that they can be upgraded or replaced, typically using proxy patterns. PAXG uses an **OpenZeppelin AdminUpgradeabilityProxy** architecture. This means the PAXG token address that users interact with is a proxy forwarding calls to a logic contract that Paxos can swap out for a new one if needed. The rationale is to enable improvements or emergency fixes (e.g., if a bug is found or if regulatory requirements change) without requiring token holders to swap tokens for a new contract. Many regulated token issuers favor upgradeable contracts for that safety net. However, this introduces trust that the issuer won't arbitrarily change token logic in harmful ways. Issuers mitigate concerns by disclosing this design and undergoing audits. Tether Gold's contract is not publicly stated to be upgradeable; Tether historically has deployed new token contracts (e.g., for USDT) rather than proxies, but the general principle is that some form of upgradability or replaceability exists if absolutely required (since ultimately the issuer can launch a new token and redeem old ones if needed).
- **Metadata and Allocation Tracking:** A unique feature in precious metal tokens is the need to map each token to specific physical assets (bars). While the ERC-20 standard itself doesn't include metadata about underlying assets, issuers maintain off-chain records linking tokens or addresses to bar serial numbers. For example, **Tether Gold's system associates specific gold bar serial numbers, purity, and weight to each on-chain address holding XAUF**. This means if you hold XAUT in your wallet, Tether's backend knows exactly which physical gold bars (or portions of bars) you own. Paxos does similarly; each PAXG token corresponds to an **allocated London Good Delivery gold bar held in Brink's vaults**, and Paxos provides a lookup tool where a user can input their Ethereum address and get the serial number, vault, and bar details of the gold backing their PAXG. This allocation is crucial for redeemability – when a holder accumulates enough tokens (e.g. 430 PAXG for a ~400 oz LBMA bar), they can redeem and receive that specific bar. The mapping is maintained off-chain but is an integral part of product architecture. Some projects have explored putting this data on-chain, but generally a centralized database is used with periodic audits for verification.

3.3.3 Compliance-Oriented Token Standards (ERC-3643 and ERC-1400)

While ERC-20 suffices for many purposes, compliance-by-design standards have emerged to cater to regulated assets and security tokens. These standards extend ERC-20 with built-in restrictions and identity management. A key example is **ERC-3643, the Official Smart Contract Standard for Permissioned Tokens**, which was previously known as the T-REX protocol by Tokeny. ERC-3643 enables the **issuance, management, and transfer of tokens that can only be held by verified (whitelisted) participants**, embedding KYC/AML compliance into the token logic. In essence, an ERC-3643 token contract checks an on-chain registry of identities or credentials every

time a transfer is attempted: if the sender or receiver is not authorized, the transfer is blocked. This is ideal for tokenized securities or any asset where the law requires only certain investors or jurisdictions to hold the asset.

ERC-3643 works by leveraging smart contracts for identity (often an ERC-734/735 identity registry) alongside the token contract. The standard defines roles like issuers, agents, and identity authorities. For example, an issuer could define that only addresses which have passed KYC and have a valid credential NFT (non-fungible token) can receive the gold token. If one of those addresses is later sanctioned, the issuer can revoke its credential, and the token contract would reject any transfers involving that address. By 2025, ERC-3643 has been adopted in several real-world asset tokenization projects, especially in Europe – over $28 billion worth of assets have been tokenized via ERC-3643 according to Tokeny. Its advantage is **fine-grained control and automation of compliance**: rules for jurisdictions, investor caps, lock-up periods, etc., can all be coded in. For precious metals, which often aren't legally "securities," ERC-3643 is not mandatory, but some projects might still use it to ensure only approved clients hold the tokens (for example, a gold token offered via private placement to institutional investors could use ERC-3643 to prevent any outside addresses from holding it).

Another notable standard is **ERC-1400**, a suite of interface standards introduced in 2018 for security tokens. ERC-1400 and related sub-standards (ERC-1404, 1594, 1644, etc.) provide methods for forcing transfers, partitioning tokens (to mark restricted vs free portions), and sending detailed failure data when transfers are blocked. Polymath and other security token platforms championed ERC-1400, but it remained an unofficial standard (Ethereum community did not ratify it as an ERC). By contrast, ERC-3643 achieved official ERC status in 2021, making it more widely recognized. Both standards aim to achieve similar goals of compliant tokens, albeit with different approaches. In practice, platforms like Tokeny (ERC-3643) and Polymath or Securitize (ERC-1400 variant) can both tokenize precious metals **as regulated instruments** if needed – for example, if a gold token is structured as a security offering or part of a fund.

To illustrate, a **UAE-based gold trading platform** might issue an ERC-3643 token representing gold ownership, tying each wallet to a verified user who has an account with the provider. Transfers between users who haven't done KYC would be impossible on-chain, thereby satisfying local regulations (such a model could be used in a Dubai or Abu Dhabi gold investment product sold to clients). On the other hand, **publicly tradable tokens like PAXG and XAUF deliberately do not use ERC-3643** because they want the tokens to be freely traded by anyone (after initial purchase). Instead, those issuers rely on off-chain compliance (KYC at purchase/redemption) and on-chain blacklist as a backstop.

In summary, smart contract standards and designs for tokenized metals range from **simple fungible tokens to complex compliance-aware tokens**. The choice depends on the regulatory context and desired user base. Table (for illustration) below compares key standards:

- **ERC-20:** Fungible, open transfer. Used by PAXG, XAUt, most public gold tokens.
- **ERC-1155:** Multi-token, flexible but less common for metals so far.
- **ERC-3643 (T-REX):** Permissioned token, on-chain enforcement of KYC/AML. Used in security token platforms; could be applied to gold if sold as a security or to restrict ecosystem.
- **ERC-1400 family:** Similar purpose as 3643, with modular approach to restrictions (unofficial standard, but used by some platforms).
- **Stellar/XRPL native tokens:** Built-in account authorization and freeze features (non-EVM but achieve similar compliance control).

- **Other proprietary frameworks:** Some enterprises may design custom smart contracts on platforms like Hyperledger Fabric (chaincode) for internal gold tokens with rules aligning to their compliance needs.

Regardless of standard, all token contracts undergo **extensive auditing and testing**, given the high value of gold tokens. To date, major gold tokens have had no smart contract exploits – a testament to careful design. For example, PAXG's code (audited by Paxos and external firms) has operated without incident since launch, and even older projects like Digix's DGX (launched 2018) never suffered technical breaches (Digix issues were business-related, not smart contract failures).

3.4 Custodial vs. Non-Custodial Models for Tokenized Metals

An essential aspect of tokenized commodities is how the physical asset custody is handled and how that interacts with the digital tokens. The terms **custodial** and **non-custodial** can refer to two dimensions here: (1) custody of the physical metal, and (2) custody of the digital tokens. We will clarify both:

- **Physical Custody of Metal:** Almost all tokenized gold/silver systems rely on a **custodial model for the underlying asset** – a trusted vault operator holds the physical gold bars that back the tokens. This is inherently custodial because someone must store the gold. The issuer or a partner (often a bank or vault service) acts as custodian. For example, Paxos Trust Company holds the gold for PAXG in LBMA-approved vaults (Brink's vaults in London). Tether Gold's gold is stored in a high-security vault in Switzerland through a custodian on Tether's behalf. In the UAE's ComTech Gold (CGO) case, physical gold is held in DMCC-approved vaults in Dubai and recorded via trade warrants. **Non-custodial physical models are rare** – about the only theoretical scenario is a fully decentralized network of gold holders each tokenizing their own gold (which introduces enormous complexity in standardization and trust). To date, no major token has physical gold scattered with individual holders due to verification issues. Instead, projects ensure custody is handled by entities with audits, insurance, and reputations (e.g., Perth Mint for PMGT, or vaults like Loomis, Brink's, Malca-Amit for others). However, within custodial models, there are nuances:
  - **Allocated vs Unallocated:** High-quality tokenized gold projects use **allocated gold** – specific bars or bullion allocated to token holders. This means the gold is not a pooled account subject to the custodian's creditors; it is the property of token holders. PAXG and XAUt both claim allocated gold backing (each token corresponds to identified bars). Some older or lower-tier products might use unallocated gold (a pool claim), which carries more risk.
  - **Single vs Multiple Custodians:** Some tokens use a single custodian for simplicity (e.g., Paxos with Brink's), while others like AurusGOLD (AWG) allow multiple vault providers around the world to contribute gold that mints the same standardized token. The latter is a distributed custody model: it reduces single-point failure risk but requires strong oversight to ensure each provider truly has the gold they claim (usually enforced by audits and chain oracles).
- **Digital Token Custody:** This refers to who holds the **private keys** that control the token on the blockchain. Here, **custodial** means a third-party (like an exchange or bank) holds the tokens for the user, whereas **non-custodial** means the user holds their own keys (e.g., in a personal wallet). One benefit of tokenized assets is that investors can choose non-custodial ownership of a hard asset – something not possible with traditional gold ETFs (where a fund or broker is always intermediary). For instance, an investor can buy PAXG and withdraw it

to their Ethereum wallet, holding the tokens with full control. This is **non-custodial digital ownership of gold** – the user doesn't rely on any broker to access or transfer it (though they still rely on Paxos for redemption to physical). Most public tokenized metals support this mode: after initial purchase from the issuer or an exchange, users can self-custody the tokens. On the other hand, some implementations keep digital custody with a platform. For example, **HSBC's Gold Token in HK is fully custodial on the digital side** – tokens are managed within the HSBC banking app, and the user cannot withdraw them to an external wallet. This sacrifices the decentralization aspect in favor of convenience and integration (essentially, it's like an ETF in function, just on a blockchain backend). Another case is Perth Mint's GoldPass system: GoldPass was a mobile app where users had gold balances; when PMGT (the Ethereum token) was introduced, it acted as a bridge – GoldPass holders could convert their gold balance into PMGT ERC-20 tokens. If they wanted, they could then move PMGT on-chain non-custodially. The two-tier model allowed both custodial and non-custodial options.

In practice, **custodial vs non-custodial token models often blend**. A retail user might buy tokenized gold on a crypto exchange (custodial) but then withdraw it to a personal wallet (non-custodial). Or vice versa, someone might move tokens into a custody provider like **Fireblocks** or **Coinbase Custody** for safekeeping. Fireblocks, as an infrastructure provider, enables institutions to self-custody in a secure way – it uses multi-party computation (MPC) and hardware isolation to protect private keys. A gold token issuer might itself use Fireblocks to manage their treasury addresses (for minting/burning) and to allow institutional clients a safe way to store tokens. For example, Paxos could hold its PAXG reserve keys in a custody tech solution and onboard partners like Neo banks via Fireblocks secure transfer network instead of requiring everyone to manage raw private keys.

Non-custodial ethos: Some gold token projects emphasize user control. Kinesis, for instance, issues KAU/KAG onto the Kinesis blockchain and provides a wallet where users hold the keys (Kinesis provides the wallet software but the user's account is secured by their credentials). If Kinesis (the company) were to fail, they set up structures (an independent vault receipt holding company) to ensure users still legally own the gold and can access it. This approach tries to maximize user protection by separating metal ownership and company operations – a step towards a trust-minimized model, though a base level of trust in the vaults and system remains.

Custodians and Insurance: All serious tokenized metal offerings involve insured vaults and regular audits. One advantage of tokenization is that it can impose discipline on the custodian via transparency. For example, the allocated bar list for PAXG or XAUt is published and can be spot-checked by users and auditors. Projects like Kinesis publish quarterly audit reports by independent inspectors (Inspectorate/Bureau Veritas) confirming that on-chain KAU/KAG supply matches gold/silver in vaults. These audits are akin to proof-of-reserve but done in traditional way. Increasingly, we see the integration of **blockchain-based attestations** – Chainlink's Proof of Reserve or similar – which we'll discuss later.

In summary, "custodial" vs "non-custodial" in tokenized metals is not black and white. **The physical metal** is held by custodians (vaults), except in fringe cases, so trust in those entities and their regulators is essential. But **the digital tokens** can be held in a self-custodied manner, giving investors direct control. Many offerings try to give the option of either holding tokens yourself or using a third-party custodian for convenience. This flexibility is a key benefit of tokenization – one can treat a gold token like a bank deposit (if left with an exchange or fintech app) or like cash under the mattress (if withdrawn to a **hardware wallet**). Both models coexist, and the architecture of

the product must account for secure operation in either scenario.

3.5 Digital Asset Custodians and Wallet Infrastructure

As institutional interest in tokenized assets grows, the role of **digital asset custodians** and secure wallet frameworks has become pivotal. These service providers ensure that private keys for token contracts and holdings are managed with enterprise-grade security, and they often integrate compliance features needed by institutions and regulators.

- **Custody Platforms (Fireblocks, BitGo, etc.):** Platforms like Fireblocks, BitGo, Copper, and Ledger Enterprise offer technology for secure storage and transfer of digital assets. They use techniques such as multi-signature approval processes, Hardware Security Modules (HSMs), and Multi-Party Computation (MPC) to safeguard keys. In the context of tokenized gold:
  - **Issuers:** The issuing company can use a custody platform to manage the keys that control minting/burning. For instance, if the mint authority key for a gold token is kept in Fireblocks, any mint transaction might require multiple senior executives to confirm in the Fireblocks system, reducing risk of a single rogue actor or hacker minting fake gold tokens. This adds a layer of internal control aligned with compliance (similar to how a vault might require dual authorization to remove gold).
  - **Institutional Investors:** A hedge fund or bank holding a large amount of PAXG or XAUT on behalf of clients will likely use a custodian like BitGo or a qualified custodian like Anchorage. These custodians often are regulated entities (NYDFS trusts, etc.) which satisfy regulatory requirements for safeguarding client assets. They also provide insurance on digital asset holdings, which could cover losses from theft. For example, if a Middle Eastern wealth management firm wants to allocate to gold tokens, they might hold those tokens through a custody account with a provider in ADGM or DIFC that uses Fireblocks's wallet tech under the hood. This way, the firm can report to regulators that assets are held with a secure, insured custodian.

  Fireblocks in particular has positioned itself not just as a custodian but as **an infrastructure for tokenization**. It provides an API and console such that companies can **mint, burn, or transfer tokens programmatically** in a secure environment. Some tokenization platforms integrate directly: for instance, Tokeny (with ERC-3643 compliance tokens) has an integration with Fireblocks, allowing a seamless flow where tokens representing real assets can be created and delivered to investors through Fireblocks wallets. This kind of integration is crucial for **scalability of real-world asset tokenization** – it bridges the gap between blockchain and the operational systems of financial institutions.

- **Wallet Frameworks:** On the user side, having suitable wallets is important for adoption. For retail users, standard wallets like MetaMask, Trust Wallet, or Ledger devices support ERC-20 gold tokens without issue. For example, one can hold Tether Gold (XAUF) on a Ledger Nano hardware wallet just as they would hold ETH or BTC. But for institutional and enterprise users, specialized wallets or integrations are needed:
  - **MetaMask Institutional (MMI):** This is a variant of the popular MetaMask wallet that connects with custodial backends. A fund manager could use MMI such that when they initiate a PAXG transfer in the MetaMask interface, the transaction is actually routed to their custodian (like Fireblocks or BitGo) for signing. This marries usability with compliance (the private key is not in the browser, but with a custodian).

  - **Mobile fintech apps:** Some fintech apps integrate gold tokens under the hood but provide a traditional interface. For example, a digital bank in the UAE might let users "buy gold" in the app, which behind the scenes means allocating XAUT or PAXG to the user's in-app wallet. The user might not even realize a blockchain token is involved; the app and its custodial partner handle wallet management. **Tangem cards**(hardware wallets in a card form) have even been marketed for Tether Gold, where a user can hold a physical card that secures their XAUT holdings – bridging physical and digital convenience.

- **Interoperability and Standards:** Custodians and wallet providers often create standardized protocols for transferring tokenized assets. For instance, **SWIFT** (the banking network) has been trialing token transfer protocols and linking with blockchain custodians for settlement. While not specific to gold tokens, these developments affect how such tokens will be adopted by institutions globally. A tokenized gold bar might one day be moved from a vault in Dubai to a bank in London via a SWIFT message triggering on-chain movements between custody accounts – all happening within a few minutes, something impossible with physical gold today.
- **Regulatory Compliance:** Institutional custody solutions embed compliance checks – for example, **Travel Rule** compliance for large transfers. When an institution transfers a large amount of tokenized gold to another institution, they might be required to share sender and receiver identities off-chain. Solutions like Notabene or TRISA can be integrated at the custodian level to automatically share this information while the blockchain transfer occurs. Additionally, custodians maintain audit trails of all transactions and often whitelisting of withdrawal addresses, which adds security for handling tokenized assets.

In the UAE context, regulatory regimes in ADGM and DIFC require virtual asset custodians to be licensed. We are seeing firms in these free zones partnering with tech providers (like Fireblocks) to offer **custody services for tokenized assets**. For example, a Dubai-based vault might work with a digital custodian so that when they tokenize gold, the digital keys and workflows are handled by a secure custody tech platform, satisfying the regulators (who want to see robust systems) and clients (who want ease of mind).

In conclusion, **digital asset custodians and wallet frameworks** are the backbone that connects the blockchain layer of tokenized metals to the traditional financial world. They provide the trust and security required for institutional participation. By 2025, the landscape includes big banks developing in-house custody for tokenized assets (HSBC, for instance, via its partnership with Metaco, is launching custody tailored to tokenized gold and securities). This indicates that holding tokens like PAXG or XAUT is becoming as routine for a bank as holding physical gold in a vault – each just requires **appropriate safekeeping infrastructure**.

3.6 Integration with Oracles and External Infrastructure

Blockchain oracles and external infrastructure play a crucial role in the tokenized asset ecosystem by linking on-chain tokens to off-chain data and events. For precious metal tokens, oracles can be used for various purposes, enhancing transparency and functionality:

- **Price Oracles for DeFi:** Once gold is tokenized, it can be used in decentralized finance applications as collateral or for trading derivatives. This requires reliable price feeds. **Chainlink price oracles** are commonly used to feed the real-time price of gold (XAU/USD) or the price of specific tokens like PAXG into smart contracts. For example, lending protocols like

Aave or MakerDAO that list PAXG rely on a price oracle to know the USD value of collateral. Chainlink provides a decentralized feed of gold prices aggregated from many exchanges and market data sources, which prevents any single source from manipulating the value. This means a user can deposit PAXG in a DeFi lending platform and borrow stablecoins against it, with the protocol confident in the gold valuation. In 2023, Aave even discussed adding PAXG as collateral, highlighting how gold tokens integrate into the broader crypto financial infrastructure.

- **Proof of Reserve (PoR) Oracles:** Perhaps the most direct oracle application for asset-backed tokens is proving that the off-chain reserves indeed exist and match the on-chain supply. Chainlink has pioneered a **Proof of Reserve** service where independent nodes query data (like an auditor's report or a custodian's API) and push that on-chain. Paxos adopted Chainlink's PoR for both its PAXG gold token and USDP stablecoin. In practice, Paxos provides data about its gold holdings (total ounces in vault) to Chainlink oracles. A decentralized network of oracles then updates a **PAXG reserve contract** on Ethereum that any DeFi app or user can read, confirming if the supply of PAXG tokens <= gold ounces held. This was intended to give additional assurance to users "on-chain" without waiting for monthly attestations or trusting a PDF report. However, as noted by analysts, the Chainlink PoR is only as good as the data source – in Paxos's case, all the oracles pull from Paxos itself (which updates the numbers daily). It's still a useful tool for **automated monitoring**; for instance, a smart contract could refuse to accept new PAXG deposits if the PoR feed indicates a discrepancy, adding a programmatic safeguard against fractional reserve scenarios.
- **Asset Metadata and Tracking Oracles:** Some projects are working on linking physical asset tracking systems with blockchain. This goes beyond just trust in audits, toward **real-time verification**. For example, IoT sensors or RFID tags on gold bars could, in theory, feed data to confirm a bar's presence in a vault. **Meld Gold** has hinted at "patent-pending" technology for **minimized trust** in connecting physical metals to the blockchain. They aim to provide live accountability of metal held and even location data on-chain. While details are scarce (targeting release in 2025), this might involve oracles that report when a bar is moved or if it remains in the vault, thus reducing reliance on quarterly audits. Imagine a vault's security system automatically updating a smart contract with inventory counts – that could alert token holders if a bar was removed without a corresponding token burn. This level of automation in custody is still experimental, but it represents the next phase of **trust-minimization** for tokenized assets.
- **Settlement Oracles:** In platforms bridging traditional finance, oracles might signal when fiat payments are received or when regulatory approvals are given, triggering on-chain actions. For instance, a gold trading platform could use an oracle to watch a bank API – when a wire transfer of USD arrives for buying gold, the oracle informs a smart contract to release the equivalent gold tokens to the buyer. This kind of integration was part of early tokenization pilots connecting SWIFT or banking systems with blockchains.
- **Compliance Oracles and Identity:** In permissioned token systems (like ERC-3643 tokens), identity verification can be on-chain or off-chain. Oracles can update on-chain identity status. For example, if a user completes KYC/AML with a provider, an oracle service might be used to write an attestation to an identity smart contract (perhaps issuing them a verifiable credential or NFT that the token contract will recognize). Companies like Chainlink are also exploring **"decentralized identity oracles"** to prove that an address belongs to an accredited investor or has passed checks, without revealing private data on-chain.

- **External Data Oracles (Market and Events):** Although less directly related to physically backed tokens, some tokens might incorporate other external data. A hypothetical example: a smart contract for a tokenized metal index might need prices of gold, silver, platinum from oracles to rebalance a basket token. If someone issued a composite precious metals token (like a token representing 50% gold, 30% silver, 20% platinum), the contract would rely on oracles for each metal's price to determine backing ratios.

Chainlink dominates the oracle space, but others exist (Band Protocol, API3, etc.). Also, some tokenization platforms choose to rely on **trusted oracles (single source)** especially in permissioned environments. For instance, a private gold trading network might just let the custodian itself post daily holdings on-chain, signed by its key, which participants trust. This is simpler but introduces central oracle risk.

Integration with Traditional Infrastructure: Beyond oracles, integration includes connecting with trading platforms, custody tech, and even market makers. For example, token issuers often integrate with exchanges (both centralized and decentralized) so that there's liquidity. Market makers use exchange APIs and on-chain DEXs to arbitrage and keep the token's price aligned with spot gold. Additionally, companies like Chainlink and SWIFT are collaborating to connect capital markets to blockchains. While those efforts are broader than just gold, they pave the way for large-scale use of tokenized commodities in mainstream finance. A central bank or large fund could use such infrastructure to swap tokenized gold for tokenized cash in a single atomic transaction if the plumbing is set up via standardized oracles and messages.

In summary, **oracles bring outside trust into the blockchain and push blockchain assurances out to the real world**. For tokenized metals, this means:

- Keeping everyone honest about reserves (no hidden debasement of the token supply).
- Enabling smart contracts to "know" the gold price and other relevant info.
- Potentially monitoring the physical asset in new ways.
- Bridging payment and identity systems into the tokenization platform.

As of 2025, we have early but meaningful usage of these integrations: Paxos's use of Chainlink PoR for PAXG, Tether's publication of gold bar details tied to addresses (a manual oracle of sorts, via their website lookup), and projects like Comtech Gold leveraging DMCC's Tradeflow data (an off-chain trade finance registry) as a form of oracle-confirmation that each token is backed by a Tradeflow warrant. These components collectively enhance **transparency and trust** in tokenized precious metals beyond what traditional gold investments offer.

3.7 Scalability and Interoperability Considerations

Scalability refers to the capacity of the tokenization system to handle growing volumes of transactions and users. **Interoperability** refers to the ability of tokenized metal assets to operate across different systems and blockchains. Both are crucial as tokenized gold and silver adoption increases.

3.7.1 Scalability Challenges and Solutions

On Ethereum and similar public blockchains, the primary scalability issues are transaction throughput and cost. In periods of congestion, gas fees on Ethereum have spiked to levels that make small gold transfers uneconomical (imagine paying $50 in gas to send $100 worth of gold – not practical). This is one reason alternatives like Tron or Polygon have been employed by some issuers. For example, **Tether Gold launched on Tron** in addition to Ethereum, because Tron's fees are minimal and

it offers fast confirmation, catering to traders who value speed and low cost (Tron is popular in certain markets for those reasons). The trade-off is Tron is more centralized in governance than Ethereum, but for a custodial asset like gold, users may prioritize convenience.

Layer-2 Scaling on Ethereum is a major development by 2025. Rollup solutions (Optimistic and ZK-Rollups) can allow thousands of transactions for the cost of one on mainnet (batched). While PAXG and XAUt are not yet natively on rollups, we are seeing third-party bridges wrapping these tokens onto L2s. For instance, an exchange or custodian could move tokens onto Arbitrum or zkSync and then handle user transfers there. The token issuer would monitor that the total on L2 plus total on L1 equals the physical gold backing. In practice, official support is needed to avoid fragmented liquidity. Paxos, in strategy discussions, mentioned that they could consider deploying PAXG on other chains or layer-2 networks, or more likely support bridging solutions while ensuring proper controls. The key is to maintain a **single source of truth for total supply**. If bridging, typically the supply on Ethereum would be locked in a bridge contract and a mirror token issued on the L2 – this introduces smart contract risk (bridge hacks). If directly issuing on L2 (mint on L2), Paxos would then have to burn or lock tokens on L1 correspondingly. To date, issuers have been cautious, and most PAXG trading still happens on Ethereum L1 or through centralized exchanges.

Other scalability solutions include:

- **Permissioned Blockchains and Consortium Networks:** These often have higher throughput because they control node participation. The downside is they sacrifice the open access of public chains. For example, a consortium of banks could run a private chain for gold trading that handles hundreds of TPS, but then retail users can't directly join that network.
- **Sharding and New Protocols:** Ethereum's roadmap includes sharding (post-Merge, in the Proto-Danksharding direction) which should eventually increase capacity. Alternative L1s like Solana or Avalanche C-Chain offer high TPS, and theoretically a gold token could launch there to leverage it. We saw **PAXG list on BSC (Binance Smart Chain)** via a pegged token (Binance issued a BEP-20 wrapped PAXG). This gave users on BSC access to PAXG liquidity with low fees, though it required trusting Binance's peg. The existence of wrapped versions underscores demand for using these tokens on cheaper chains.
- **Batching and Off-Chain Trading:** Some platforms may batch multiple small transfers into a single on-chain transaction or use off-chain trade execution (like Lightning network style or state channels, though those are more complex with ERC-20s). So far, we haven't seen state channels for gold tokens, but a custodial exchange is effectively off-chain trading – many users can trade tokenized gold within an exchange's order book with only occasional on-chain settlement when deposits or withdrawals happen.

For user scalability, one must also consider how many transactions typical usage entails. Gold is often held as a long-term asset, not transacted daily like a currency. Thus, the transaction volume might remain moderate (mostly moves between custodians or occasional transfers). This is unlike something like a stablecoin which sees high velocity. So Ethereum's limits have so far been manageable – for instance, PAXG has on the order of tens of thousands of total transfers recorded, which is relatively low. If gold tokens started being used for micropayments or machine-to-machine settlements (a far future scenario), then scaling would need to be more aggressive (perhaps using a dedicated high-speed network or sidechain exclusively for that purpose).

3.7.2 Interoperability and Multi-Chain Strategy

Interoperability means a token can be freely moved or utilized across various blockchain networks and be integrated with different platforms. Achieving interoperability for tokenized metals involves a few strategies:

- **Native Multi-Chain Issuance:** The issuer maintains a presence on multiple chains. For example, XAUt exists on Ethereum and Tron natively, with the issuer controlling mint/burn on both. The total XAUt across both chains is collectively backed by the same pool of gold. If someone wants to convert XAUt from Ethereum to Tron, they cannot "beam" it directly; they would send to Tether for redemption and reissuance on Tron (or use a third-party bridge). Native multi-chain issuance gives flexibility but requires the issuer to secure keys on multiple networks and manage liquidity. Another project, **VNX Gold (VNXAU)**, started on Ethereum but also launched on Polygon, Avalanche, Solana, Stellar, and Tezos to appeal to users in those ecosystems. They call it a "multichain token fully backed by physical gold". VNX likely tracks the circulating supply on each chain and ensures the sum is matched by gold in vault. This approach increases reach (e.g., Tezos DeFi can use VNXAU, Polygon users can swap it cheaply) but it's operationally complex.
- **Bridges and Wrappers:** Rely on cross-chain bridge services to move tokens between networks. A user locks token on Chain A and gets a wrapped version on Chain B. This was common for assets like BTC (wrapped to Ethereum); for gold tokens, we have seen **Binance Bridge wrapping PAXG to BSC**, and **third-party bridges wrapping PAXG or XAUt to Polygon**. The risk is that a bridge smart contract could be hacked, which might inflate the wrapped supply without backing (if tokens are stolen from the bridge). To mitigate risk, some projects only trust well-known bridges or their own custody. For instance, a centralized exchange can serve as a "bridge" by letting users deposit on one chain and withdraw on another if they support the token on both.
- **Interoperability Protocols:** Initiatives like **Cosmos' IBC (Inter-Blockchain Communication)** or Polkadot's XCMP allow assets to move between sovereign blockchains that adopt the standard. If a tokenized gold were issued on a Cosmos chain (say, in the Terra or Cronos ecosystem), IBC could permit transfers to other Cosmos chains seamlessly. We haven't seen major gold tokens in Cosmos yet, but the framework is there for the future. Polkadot's ecosystem could see a similar thing if a parachain for commodities is launched – that token could be sent to any other parachain.
- **Interoperability with Traditional Systems:** Beyond blockchain-to-blockchain, tokenized gold should interoperate with traditional markets. We see early signs: for example, Switzerland's SDX (SIX Digital Exchange) and other stock exchanges exploring tokenized commodities that could be traded alongside traditional securities. **Singapore's Project Ubin and Japan's trials in 2023** show a push to make tokenized assets interoperable with existing trading and settlement infrastructure. They envision a scenario where a tokenized gold could be swapped atomically with a tokenized bond or cash on different ledgers, improving settlement times and reducing risk. Standards like **ISO 20022** (financial messaging) might eventually incorporate fields for digital asset identifiers, further blending these worlds.
- **Smart Contract Interoperability:** A technical nuance is ensuring the smart contract logic or regulatory controls persist across chains. If PAXG is only on Ethereum, its compliance features (freeze, etc.) only operate there. If it were on another chain, Paxos would need

analogous controls on that chain's contract. Similarly, if a gold token uses ERC-3643 on Ethereum (with on-chain identity), a different chain might not support the same standard, making it hard to mirror the restrictions exactly. This is why often multi-chain deployments keep it simple (ERC-20-like) and rely on off-chain oversight for compliance on the secondary chain.

Real-World Example – DMCC's Tradeflow integration: The DMCC's gold token (CGO on XDC) is a good case of interoperability between a blockchain and a legacy system. Each token is backed by a Tradeflow warrant (a digital document of title). Tradeflow itself is not blockchain-based; it's a centralized registry. But by linking each token to a warrant ID, they achieved interoperability of legal frameworks: the token cannot exist without the warrant, thus bridging DMCC's legal system with XinFin's ledger. If someone tries to move tokens without a corresponding warrant, the design would catch that inconsistency. In effect, the XDC smart contract likely references an external check (or the business process ensures no token mint without a warrant). This shows interoperability doesn't only mean chain-to-chain; it also means chain-to-legal record.

Going forward, interoperability standards like the **InterWork Alliance's Token Taxonomy Framework (TTF)** and others might allow a gold token on one platform to be understood and accepted on another platform or by a different institution. The goal is that a tokenized ounce of gold should be as universally recognized as a physical ounce is globally.

In conclusion, scalability and interoperability are being addressed gradually:

- Scalability through Layer-2s, alternative chains, and perhaps improved L1 performance (Ethereum 2.0 upgrades, etc.).
- Interoperability through multi-chain issuance and bridging, with careful attention to maintaining the 1:1 backing and regulatory controls across ecosystems.

The industry recognizes that **no single blockchain will be ideal for all use cases** – so tokenized assets will live in a multi-chain world. The challenge is to ensure a gold token on any chain can be trusted to represent the same thing: a claim on the same vaulted gold. The technologies and standards discussed are all aimed at preserving that equivalence while expanding access and utility.

3.8 Compliance-by-Design and Auditability

Tokenized precious metals operate at the intersection of finance and technology, so compliance and auditability are top priorities built into the product architecture. Here we cover how **compliance-by-design** is achieved through smart contracts and platform rules, and how **blockchain's transparency** combined with analytics tools enhance auditability of tokenized assets.

3.8.1 Compliance Mechanisms in Smart Contracts and Platforms

We touched on on-chain compliance standards like ERC-3643 in section 3.3.3. Those are explicit ways to enforce regulations (KYC/AML, investor eligibility) at the smart contract level. But compliance-by-design also encompasses the broader system design:

- **Whitelisting and Blacklisting:** Many gold token issuers maintain whitelists off-chain (for primary market) and blacklists on-chain (for secondary market exceptions). For example, to initially purchase PAXG or XAUF from the issuer, an investor must go through full KYC/AML checks and be whitelisted in the issuer's customer database. Only then will the issuer send tokens to their address. Once on-chain, the token may trade freely, but if an address becomes

problematic (sanctioned, associated with crime), the issuer can blacklist it to freeze assets. This two-tier approach (off-chain whitelist, on-chain emergency blacklist) has been effective for complying with regulations without stifling general market liquidity.

- **Transfer Restrictions:** In more tightly controlled offerings, the smart contract itself may restrict transfers except between whitelisted addresses. Platforms like Securitize, Tokeny, and Polymath set up tokens where every transfer checks a registry (usually via a hook in the token contract or a proxy). For instance, if a gold token was sold as a private security in UAE to approved investors only, the contract might block any transfer to an unapproved address, thereby preventing a secondary market unless it's also within the approved list. This is compliance-by-design in action, ensuring regulatory constraints (like private offering restrictions or Shariah compliance requirements) are automatically enforced by code.
- **Role of Identities and Credentials:** With ERC-3643, each token holder is linked to an on-chain identity contract (often an ERC-734 identity) containing verifications. The compliance rules (ERC-3643 or similar) ensure only identities with certain attributes (e.g., KYC done, country not blacklisted, not exceeding holding limit) can execute transfers. This effectively bakes in regulations to the token. For instance, a UAE-based gold token may restrict non-GCC (Gulf Cooperation Council) investors if that was part of its regulatory approval – such a rule could be implemented by only approving GCC investor identities. A real example is the **Masaood-backed gold token in ADGM**(hypothetical scenario): it might use a permissioned chain where each participant is a verified account under ADGM's regulatory sandbox, and the smart contract won't allow any unknown party to hold tokens. This ensures **compliance is not just a policy but a technical property of the token**.
- **Shariah Compliance:** In Islamic finance contexts like the Middle East, gold investments must adhere to certain principles (e.g., immediate settlement and full ownership, as gold is a Ribawi item in Fiqh). Tokenization platforms address this by ensuring the smart contract and legal structure reflect true asset ownership and redeemability. One example was OneGram in Dubai, which obtained a Shariah certification for its gold-backed cryptocurrency. While OneGram's implementation details weren't fully public, likely they had scholars review that each token represented actual allocated gold and that any transfer meant transfer of ownership of that gold (no excessive uncertainty or speculation). Comtech Gold (CGO) also advertises Shariah compliance, meaning their token is structured to meet those criteria, possibly by immediate linkage to a specific bar via a warrant and by enabling redemption. From a tech perspective, ensuring every token is 100% backed and redeemable and disallowing practices like lending that gold out (which could introduce riba or undue risk) are ways compliance is achieved in design.
- **Legal Entity and Governance:** Many token issuers set up the legal entities issuing tokens in compliance-friendly jurisdictions and under oversight. Paxos, for example, is a **NYDFS-regulated trust company**, meaning it undergoes audits, exams, and must maintain certain capital and risk controls. That trust status gives regulators confidence that PAXG is run properly (e.g., gold audits, segregation, insurance). Similarly, in the UAE, a project might be under the VARA (Virtual Assets Regulatory Authority in Dubai) or ADGM's FSRA, which would approve the token offering and require certain conditions. **Compliance-by-design** in those cases might include regular reporting to regulators, on-chain monitoring tools, and the ability to halt the project if needed. For instance, an ADGM regulated token could have an admin key held in escrow by the regulator that can pause the contract in an emergency (this is speculative, but technically feasible).

3.8.2 Auditability and Blockchain Analytics

One of the biggest advantages of tokenized assets over traditional assets is **transparent auditability**. Every on-chain transaction is recorded immutably, providing a clear trail of how the asset moves. This transparency, combined with specialized analytics tools, significantly enhances oversight and trust.

- **Public Ledger Verification:** Anyone can inspect the smart contract of a token to verify the total supply. For PAXG or XAUT, one can query the contract or use Etherscan to see how many tokens are in circulation and even track changes over time. This is far more transparent than, say, an ETF where one must trust monthly reports or custodian statements without granular detail. As of the latest data, PAXG's total supply could be observed (roughly 230,314 tokens in mid-2025), and that can be directly compared to Paxos's published gold bar list. Similarly, Tether Gold's supply (about 246,524 XAUT as per Messari) can be seen on-chain and should match the ounces of gold in vaults. This open auditability is a selling point for regulators – it's easier to supervise a tokenized commodity because you can independently verify that no extra "gold tokens" have been secretly issued.
- **Third-Party Audits and Attestations:** On top of code transparency, issuers provide audit reports. For example, Paxos publishes monthly attestation reports from a top accounting firm confirming the matching supply of gold for PAXG. These reports are often accessible via the company's website or filings. Some, like Perth Mint's now-defunct Gold Token, relied on the mint's internal audit processes plus government guarantees. However, as seen with Perth Mint, if the custodian has issues (diluted gold scandal, AML breaches), it can undermine the token's credibility. This underscores the need for **independent checks** – which is where on-chain proof of reserve or real-time audits could complement traditional audits.
- **Blockchain Analytics Firms:** Companies like Chainalysis, Elliptic, and CipherTrace have developed tools to monitor and analyze activity of specific tokens. They can flag if tokenized gold is being sent to darknet markets or high-risk exchanges. For instance, if a sanctioned entity tried to use a gold token, analytics could spot that, and the issuer could freeze the tokens. Chainalysis in 2025 even wrote about the importance of tracking permissioned tokens like those using ERC-3643, as it creates a more transparent market. With analytics, compliance officers can **trace the provenance of each token** – e.g., knowing that certain PAXG came from a particular exchange deposit. This is ironically more traceable than physical gold bars, which can have opaque histories. If someone laundered money by buying gold tokens, every hop is recorded, whereas laundering through physical gold (smelting and recasting bars) can erase traces. Thus, regulators may actually favor tokenized gold as it "leaves a breadcrumb trail".
- **Auditability for Investors:** Not only regulators, but investors benefit. A fund holding tokenized gold can easily prove its holdings. They just provide the blockchain addresses and any observer can confirm the balance and that those tokens are genuine. Contrast this with a fund holding physical gold – an auditor would have to literally go to the vault and count/assay the bars, or trust a custodian's word. Tokenization can streamline audits of financial statements.
- **Compliance Analytics:** Some platforms integrate rules engines that automatically monitor transactions and can implement compliance actions. For example, consider a scenario: a large transfer of gold tokens occurs that's out of pattern – this could be automatically flagged for

review as potential market manipulation or AML risk. If integrated with analytics, an issuer might have a dashboard showing all addresses with over a certain amount of tokens, their risk scores, etc., helping them ensure no concentration or suspicious activity that violates regulations. In jurisdictions that have transaction reporting requirements (e.g., suspicious activity reports, or thresholds like $10k for currency transactions in US), the on-chain data can be used to generate those reports.

- **Smart Contract Audits (Code Audits):** Before launch, token smart contracts are audited by security firms. While this is not "auditability" in the financial sense, it is a compliance measure (best practice). Having audit certificates from firms like Certik, OpenZeppelin, or Trail of Bits adds credibility. Many issuers publish at least a summary of audit findings to reassure investors that the contracts are secure.
- **Real-Time Transparency vs Periodic Audits:** The combination of on-chain data and oracles is pushing toward real-time attestation of reserves. As mentioned, Paxos updates its on-chain reserve data daily, whereas formal audits are monthly. We may see a future where an auditor node is continuously checking vault databases and updating the blockchain as changes occur (like new gold added). Chainlink's Proof of Reserve for PAXG updates at least once per day, providing much faster verification cadence than monthly statements. Although Coindesk pointed out this is still based on Paxos's self-reported data, it's a step toward **continuous auditing**. Regulators are very interested in this concept – it could reduce the need for surprise inspections if the blockchain is always up-to-date with the state of reserves.
- **Auditability of Failed Implementations:** When a token project fails or ceases, the blockchain record can help unwind positions. For example, when Trovio decided to wind down the Perth Mint Gold Token, there were exactly 1,196 PMGT tokens in circulation. They could identify all 255 holders on Ethereum and coordinate redemptions. In a traditional system, reaching out to every entitled holder might be harder. Similarly, Digix's shutdown was facilitated by the fact they could verify how many DGX tokens were out and buy them back accordingly. This shows that even in failure, the transparency simplifies resolution and protects investors from someone claiming more than they had, etc.

Finally, regulators and auditors are increasingly savvy with blockchain. In the UAE, ADGM's regulator has a blockchain analytics lab, and VARA in Dubai is building technical capabilities to monitor on-chain activity. Global regulators (like the SEC, CFTC, etc.) have teams and contracts with analytics firms to keep an eye on crypto assets. For tokenized gold, they would monitor things like:

- Is the token being used for illicit transfers? (AML focus)
- Is the issuer maintaining the peg and not over-issuing? (Commodity/fraud focus)
- Are there manipulative trading patterns? (Market surveillance similar to exchanges)

Because precious metals can be a vehicle for money laundering historically (e.g., smuggling gold to move value), having a token that's traceable offers a new tool to law enforcement. For instance, if a crime syndicate tried to buy a lot of gold tokens to move money, blockchain analytics could potential map out their network and tie it back to known entities, something much harder to do with physical gold bricks.

Compliance-by-design and auditability thus reinforce each other in tokenized metals:

- The system is built to follow rules (design-phase compliance).
- The system is transparent and leaves an evidence trail (auditability).

- Both contribute to making tokenized gold a trustworthy and regulatable asset class, suitable for institutional and mainstream adoption.

3.9 Case Studies: Global Implementations of Tokenized Gold and Metals

To cement understanding, we analyze several case studies of tokenized gold and other metals. These examples illustrate how the technology and principles discussed manifest in real products, highlighting successes, challenges, and regional specifics. We cover global projects like **PAX Gold, Tether Gold, Perth Mint Gold Token**, as well as **UAE-centric initiatives** like OneGram and DMCC's token, among others.

3.9.1 PAX Gold (PAXG) – A Regulated Gold Token on Ethereum

Overview: **PAX Gold (PAXG)** was launched in September 2019 by Paxos. Each PAXG represents one fine troy ounce of a London Good Delivery gold bar stored in professional vault facilities in London. Paxos, a New York-regulated trust company, issues and manages PAXG, making it one of the most regulated gold tokens available.

Technology & Architecture: PAXG is implemented as an ERC-20 token on Ethereum with an upgradeable proxy smart contract design. The use of an **OpenZeppelin AdminUpgradeabilityProxy** means Paxos can upgrade the token logic contract (with proper internal approvals) while the token's address remains constant for users. Key features of the contract include:

- **Mint/Burn:** Restricted to Paxos addresses to ensure supply sync with gold holdings.
- **Fee Mechanism:** Initially included a transfer fee (0.02%), which is currently set to 0%.
- **Pausability/Freeze:** Allows Paxos to freeze addresses (e.g., in case of sanctions) and pause all transfers in emergencies.
- The contract uses 18 decimal places, though Paxos only issues down to 0.01 PAXG (i.e., ~0.01 oz) to retail customers.

The backend system of Paxos ties each Ethereum address holding PAXG to specific gold bars in Paxos's custody. Paxos provides a tool on their website where any holder can input their Ethereum address and retrieve the serial number, weight, and purity of their allocated gold bar(s). If a holder accumulates enough PAXG to own whole bars, they can redeem for those specific bars; smaller holders (e.g., 0.5 PAXG) can redeem via third-party gold retailers or sell their tokens for cash. Notably, direct redemption from Paxos requires a minimum of 430 PAXG (roughly one 400 oz bar plus some margin), reflecting the wholesale nature of physical redemption (smaller redemptions are handled via partners).

Custody and Audits: The gold is held in vaults managed by Brink's in London, and each PAXG is fully allocated. Paxos publishes monthly attestation reports from auditors to verify the matching supply. Additionally, Paxos has integrated Chainlink Proof of Reserve, updating on-chain data daily to show that PAXG tokens are fully backed by gold bars. This data is pulled directly from Paxos's internal records by decentralized oracles.

Use and Integrations: PAXG is listed on numerous exchanges (Binance, Coinbase, etc.) and is used in DeFi as collateral. It's integrated into lending platforms and was added to Aave in 2022, allowing users to borrow against PAXG. It's also accepted by some gold dealers for physical conversion. Because Paxos is trusted, PAXG has seen growing adoption – by 2025 its market cap is in the several hundred million dollar range, often making it the largest gold-backed crypto token.

Strengths: Highly compliant and transparent design (regulated issuer, audits, upgradeable contract for safety). It is relatively liquid and can be traded 24/7, unlike physical gold. PAXG has proven resilient, with **no security incidents or depegging** even during volatile markets.

Weaknesses: It is centralized – holders must trust Paxos and its custody chain. Paxos can freeze tokens, and redemption requires full KYC and large minimums. So while good for institutional holders, small retail holders may never directly redeem for gold and face onboarding via exchanges. Also, Ethereum's gas fees limit on-chain usage for micro-transactions (though that's where exchanges or L2 come into play).

Recent Developments: Paxos is exploring multi-chain; as of 2025, PAXG is still primarily on Ethereum L1, but they acknowledge potential to leverage other networks. Regulatory-wise, Paxos has remained in good standing, even as it had to wind down another product (BUSD stablecoin) due to U.S. regulatory pressure – notably, PAXG was not targeted, indicating regulators see fully backed commodities differently.

PAXG stands as a **gold standard** (pun intended) in tokenized metals: it marries blockchain tech with traditional trust frameworks effectively, and it paved the way for others by demonstrating that institutional-grade tokenized gold can work at scale.

3.9.2 Tether Gold (XAUT) – A Crypto-Centric Gold Token on Ethereum and Tron

Overview: **Tether Gold**, identified by the symbol **XAUT**, was launched in January 2020 by TG Commodities Ltd (an entity related to Tether). Each XAUF token represents one fine troy ounce of physical gold. Tether Gold is unique in that it's issued on **multiple chains (Ethereum ERC-20 and Tron TRC-20)** and is oriented towards the crypto trading community, leveraging the Tether brand known for stablecoins.

Technology & Architecture: On Ethereum, XAUT is an ERC-20 token; on Tron, it's a TRC-20 token (Tron's equivalent standard). The total supply is split between these networks (though not evenly; Ethereum holds the majority of supply). The smart contracts themselves are relatively plain fungible token contracts (comparable to Tether's USDT contracts). Some features:

- **Decimals:** XAUF uses 6 decimal places on Ethereum, meaning it's divisible down to 0.000001 oz (~0.03 milligrams of gold) – a much smaller fraction than PAXG's 0.01 oz. This caters to fine granularity (perhaps useful when gold was cheaper, or for very small investors).
- **Allocation Tracking:** Tether's system assigns specific gold bars to each address holding XAUF. They state that each on-chain address is associated with specific bar serial numbers and details, which holders can verify (likely by contacting Tether or through a tool). This implies an off-chain database for allocation similar to Paxos's approach.
- **Multi-Chain Coordination:** Tether has to manage issuance across Ethereum and Tron. They likely keep a master record of total XAUF and ensure not to exceed allocated gold when minting on either chain. When tokens move between chains, it's typically via a centralized swap process (users send on one chain to Tether and receive on the other). There isn't an autonomous bridge. This manual process hasn't hindered its adoption much, as many users simply buy the version they need on exchanges.

Custody: The gold backing XAUF is stored in **Swiss vaults** (in the earlier press releases, Tether noted the gold is in Switzerland). The custodian's name isn't publicly disclosed, but likely a reputable vaulting company in Switzerland. Tether charges no custody fees; instead, they take a one-time 25 bps fee on redemption or purchase via them. A minimum of 50 XAUT (50 ounces)

is required to redeem for physical gold, smaller than PAXG's 430 oz requirement, but still about $90k+ (as of 2023) making it viable mainly for high-net-worth individuals.

Regulation and Compliance: Unlike Paxos, Tether's issuer is not a regulated trust company, and XAUT has a more offshore status. That means there's somewhat more counterparty risk – one relies on Tether's word and contractual obligation that the gold is there. Tether has had controversies with its USDT reserves historically, but with XAUF they have tried to be transparent about gold backing (publishing bar lists, etc.). They are still subject to general laws (fraud, etc.), and likely have audits of the gold, but it's unclear if they publish routine audit reports. Users mostly trust the reputation and the incentives (Tether's business depends on maintaining credibility of their tokens).

XAUT is **Shariah compliant** (like most allocated gold tokens) – Tether sought a fatwa certification to tap into Gulf region investors, as indicated by them highlighting no interest or lending on the gold and direct ownership.

Market and Usage: Tether Gold quickly gained popularity among crypto exchanges. It trades on platforms like Bitfinex, BTSE, and others, often paired against USDT or USD. By 2023, its market cap was roughly on par with PAXG (~$500M), and by 2025 it grew further. Because it's available on Tron, it has penetration in user bases that prefer Tron for its speed/fee (some parts of Asia, for example). Tangem, a hardware wallet company, even made dedicated Tether Gold physical wallet cards, indicating an attempt to market to gold bugs who want a tangible element to their crypto.

In terms of DeFi, XAUF is less integrated than PAXG, partly because Tron lacks a major DeFi ecosystem, and on Ethereum PAXG had first-mover advantage with regulators. However, XAUT is used in CeFi, for example as collateral on some lending desks or as a gold-backed savings product by fintechs.

Case Study Note: During the 2022–2023 period of high inflation and market turmoil, gold tokens saw increased interest as stablecoins were under scrutiny. Tether Gold benefitted from the "Tether" brand recognition – some crypto users preferred it assuming if they trust USDT, they can trust XAUF, and it diversifies their holdings with an inflation hedge. However, PAXG had a slight edge with institutional uptake due to Paxos's regulated status.

Uptake in the Middle East: XAUT has reportedly been used by some investors in the Middle East as a way to hold gold outside traditional banking. It's accessible globally, but specifically, the Gulf region's affinity for gold combined with growing crypto adoption made XAUT attractive. Being stored in Switzerland also adds to comfort (neutral jurisdiction, robust vaulting industry).

Challenges: Tether Gold's main challenge is proving its reserves and integrity continuously to a skeptical audience. They have so far kept their reputation in the gold token side clean. Another challenge is liquidity is somewhat fragmented (Ethereum vs Tron supply). Also, since it's centralized, like PAXG, any regulatory action against Tether or their bank could impact redemption.

Outcome: As of 2025, Tether Gold has been **successful** – it provided a viable alternative to PAXG, often with slightly lower fees and easier access for crypto-native users. The coexistence of PAXG and XAUT has expanded the overall tokenized gold market. They compete but also validate each other (the fact that both maintain their peg to real gold and have grown shows the concept is sound).

3.9.3 Perth Mint Gold Token (PMGT) – A Cautionary Tale

Overview: **PMGT** was launched in late 2019 as a partnership between Perth Mint (one of the world's largest gold refiners, owned by Western Australia's government) and a fintech startup

InfiniGold (later renamed Trovio). PMGT tokens were ERC-20 tokens on Ethereum, each backed by a 1 troy ounce GoldPass certificate from the Perth Mint. GoldPass was Perth Mint's existing digital gold certificate platform; users held certificates representing gold in Perth Mint vaults, guaranteed by the government. PMGT essentially tokenized those certificates: 1 PMGT = 1 ounce of GoldPass gold.

Technology & Architecture: Technically, PMGT was straightforward as an ERC-20 token. Trovio managed the smart contract and acted as intermediary. When a GoldPass user wanted PMGT, Trovio would create (mint) PMGT tokens and lock the corresponding GoldPass certificates. Conversely, PMGT could be redeemed by burning the token and receiving a GoldPass certificate, which could then be redeemed at Perth Mint for physical gold or cash. This model tied a private system (GoldPass) to a public blockchain token. The smart contract likely had controls to only allow minting when a GoldPass is locked and only allow trusted parties (Trovio) to call mint/burn.

Custody & Backing: The gold was entirely in Perth Mint's custody, fully insured and guaranteed by the WA government. This was a strong value proposition – effectively risk-free gold storage from a credit perspective (similar to a sovereign guarantee). The project touted that it was the **first government-guaranteed gold token**. Audits of Perth Mint's gold holdings were routine internal ones; GoldPass had its own auditing processes.

Adoption: Initially, interest was high among crypto circles: a reputable mint issuing a token was big news. However, PMGT struggled to gain liquidity. By 2021, it was listed on very few exchanges (one notable one was Independent Reserve in Australia). The supply remained tiny – as of early 2023, only 1,196 tokens were in circulation (1196 ounces of gold, ~$2.3 million worth). This was negligible compared to PAXG or XAUT.

Compliance: PMGT likely fell under Australian regulatory oversight indirectly (Perth Mint is heavily regulated for precious metal dealings, and InfiniGold would have needed an AML program). Perth Mint also secured a Shariah certification for GoldPass, which extended to PMGT by association, aiming for Islamic market appeal.

Challenges and Failure: A series of events led to PMGT's downfall:

- In 2021-2022, **Perth Mint was embroiled in controversies.** It was found to have sold some gold to China that didn't meet Shanghai Gold Exchange purity standards (though still 99.99% – the issue was trace impurities). This caused reputational damage. Then, Perth Mint self-reported historic breaches of a U.S. commodity code regarding storage of client gold, implicating a regulatory oversight (they had inadvertently operated something akin to a pooled fund without a license). AUSTRAC also investigated potential AML issues at the Mint.
- These issues undermined trust in Perth Mint's management and raised concerns over GoldPass and by extension PMGT. In March 2023, Trovio announced it would **cease support for PMGT** entirely. The decision was directly linked to the controversies hitting Perth Mint; as a startup, Trovio likely didn't want to be tethered to a partner facing legal and compliance uncertainty.
- Trovio began an **"orderly unwind"** of PMGT. Holders were given a timeframe to redeem their tokens for GoldPass or sell them. Independent Reserve exchange delisted PMGT around that time.
- The government guarantee that was once a strength couldn't salvage it, because the **opera-**

tional failures and legal breaches at the Mint created too much uncertainty.

Outcome: By mid-2023, PMGT was effectively defunct – a rare example of a tokenized commodity project terminating not due to technology failure, but due to **governance and compliance failure** of the underlying custodian. It highlighted that even with top-notch tech and backing, the human and legal elements can break down. For the broader industry, it was a caution that **counterparty risk is real**: a blockchain token is only as good as its backing. If the backer has issues, the token can quickly lose credibility, regardless of audits or guarantees.

It's worth noting that despite the turmoil, token holders were not financially harmed in the end: they could redeem their tokens (the gold was there). The risk was more that if not wound down properly, they could have been stuck with illiquid tokens. Fortunately, transparency of the blockchain (knowing the small number of holders) helped coordinate the wind-down.

3.9.4 DigixDAO and Digix Gold (DGX) – Early Pioneer, Eventual Wind-Down

Overview: Digix was a Singapore-based project that launched one of the first gold-backed tokens, **Digix Gold (DGX)**, as early as 2016-2017. Each DGX was 1 gram of gold. Digix gained fame for an ICO (**DigixDAO**, DGD tokens) which raised funds to govern the platform. DGX was fully reserved by gold stored in Singapore and Canada.

Innovation: Digix introduced the **Proof of Asset (PoA) protocol**. They would acquire London Bullion Market Association (LBMA) certified gold bars, mostly small 100g bars for granularity. For each bar, they created a PoA asset card: essentially a set of documents (invoice, vault receipt, audit certificate) uploaded to IPFS (a decentralized storage) and hashed on Ethereum. DGX tokens were then issued against that bar in 1g increments. Every quarter, Digix hired an auditor (e.g., PwC or Bureau Veritas) to audit the vault and then they'd update the PoA documents. This was a novel **compliance-by-transparency** approach – anyone could inspect the documents proving the existence and custody of the gold.

Technology: DGX was an ERC-20 token, but they had additional logic to tie it to specific PoA cards. Transfers of DGX triggered events that could be tracked to know which bar they came from. It was somewhat complex, but conceptually sound. Digix also had a fee model: a minimal demurrage (storage fee) that accumulated and could be reclaimed by burning a tiny fraction of DGX over long periods (representing storage costs). They also allowed redemption of as little as 100 DGX (100g) for physical gold.

Adoption and Challenges: Digix got early adopter interest and was listed on a few exchanges. However, due to the novelty and possibly the team's focus on the DAO side, DGX never gained mass adoption. By 2020, larger players like Paxos and Tether entered with better capitalization and regulatory standing. DGX trading volume stayed modest. Meanwhile, the governance token DGD had its own saga: in 2020, DGD holders voted to liquidate the DAO's treasury and effectively dissolve the governance structure. This was because the DAO didn't lead to the growth envisioned and holders preferred getting remaining ETH in treasury back (which actually caused DGD's price to jump before redemption – a side story in crypto governance).

Post-2020, Digix tried to continue DGX operations, but momentum was lost. By early 2023, Digix Global announced ceasing operations, transferring redemption responsibility to a partner (Nexus) for remaining token holders. DGX was delisted from major exchanges like Bitfinex in 2021 due to low usage.

Outcome: Digix's closure was again not due to a security failure – it was business-related. They pioneered many ideas (first ICO on Ethereum, first gold token, on-chain audit trail), but perhaps scaled too slowly and got overtaken. It shows that being first is not always enough; regulatory compliance (they were based in Singapore which was supportive, but a NY trust might have inspired more confidence) and deep integration with the crypto ecosystem ended up favoring others. Nonetheless, Digix validated that tokens can effectively represent gold and inspired later projects. It also left an important lesson: **community and incentive alignment matter** (the DigixDAO experiment was one of the earliest attempts at decentralized governance of a tokenization project, and its mixed results taught future projects to carefully design token economics).

3.9.5 Kinesis – Tokenized Gold and Silver as Currency (UAE Connection)

Overview: Kinesis is an ambitious project that launched around 2018, aiming to make gold and silver-backed digital currencies for global use. It issues **KAU** (gold token, 1 KAU = 1 gram gold) and **KAG** (silver token, 1 KAG = 1 ounce silver). What sets Kinesis apart is its focus on building an entire monetary system (with exchanges, debit cards, and yield incentives) and its unique yield-sharing model to encourage adoption.

Technology: The Kinesis system runs on a custom blockchain forked from Stellar, which provides fast transactions and the ability to enforce KYC on accounts. Users buy gold or silver via the Kinesis Mint (which sources physical bullion and issues KAU/KAG). The blockchain tracks all KAU and KAG, and every token is 100% allocated to physical metal in one of several vaults worldwide (in partnership with vaulting company Allocated Bullion Exchange). Vaults are located in cities like London, Dubai, Zurich, Sydney, etc., to provide geographic diversification.

Custody & Ownership Structure: Importantly, Kinesis set up a legal structure where the users of KAU/KAG are the direct owners of the underlying metal. Kinesis (the company) is just managing it as a custodian. They even created an independent vault receipt holding entity as a contingency – so if Kinesis were to go bankrupt, user ownership of gold is protected and procedures are in place for them to claim their metal. This structure was appealing from a compliance standpoint – it reduces the risk that the tokens could be considered a liability of the company (thus more like title to specific allocated metal, which in many jurisdictions is not a security but a warehouse receipt).

Yields: Kinesis introduced a fee on transactions (0.45%) and a system to redistribute the majority of that fee to users as "yields". For example, a holder yield rewards users for simply holding KAU/KAG long-term (paid from a pool of collected fees), and a velocity yield rewards users who frequently use the tokens in transactions. There's also a yield for minters (initial buyers from the mint) and for referrers. This was to simulate how a central bank might pay interest, but here the interest is funded by transaction fees in the ecosystem, not by lending the gold (the gold itself remains inert). This model was somewhat complex but aimed at making gold and silver **yield-bearing**, something traditionally not possible (since gold bullion usually has storage cost, not yield).

Adoption: Kinesis built an exchange (Kinesis Money) where KAU and KAG trade against fiat and crypto, and they launched a debit card in certain regions to allow spending of KAU/KAG. They found niche adoption in Indonesia – notably, they partnered with PT Pos (the Indonesian post office network) to offer gold savings in KAU to locals, aligning with Indonesia's cultural affinity for gold savings. They also targeted the Middle East; since the system is **Shariah-compliant** by design (full allocation, no interest except the fee sharing which was approved by Islamic finance advisors as it's a share of revenue, not usury), they attempted to capture Gulf investors and mints. In fact, one of Kinesis's vault partners is in Dubai (with Gold Silver Central and others facilitating).

As of 2025, Kinesis claims a user base of tens of thousands and vaulted assets worth over $100M in metals (from public info). The market cap of KAU in 2023 was listed around $117 million, a respectable sum, though smaller than PAXG or XAUt.

UAE Connection: The UAE likely finds Kinesis interesting because it aligns with Dubai's vision to be a gold trading hub with modern tech, and it's **Shariah-compliant** which suits many investors in the region. While not as high-profile locally as DMCC's project, Kinesis did have regional marketing and possibly regional office representation.

Challenges: Running a whole monetary system is a big ask. Kinesis had to deal with not just issuing tokens but also providing liquidity, user education, and convincing people to spend gold as money (which historically is challenging – gold is often hoarded, not spent). The yields help, but the system's success hinges on volume of transactions to generate those yields. Also, being on a custom chain means interoperability with wider crypto (Ethereum DeFi, etc.) is limited though they provide bridging of KAU to ERC-20 (there were plans to have KAU on Ethereum or Binance chain for liquidity, possibly via wrapped tokens or a future multi-chain move).

Outcome: Kinesis is still operational and is one of the more innovative models. It shows a non-custodial approach (users hold tokens in their own wallets), combined with a business model to encourage usage. Technologically, it proved that even on a Stellar fork, you can run a complex global system with audits (they publish vault audit reports quarterly). It hasn't "failed" like some earlier projects, but it remains to be seen if it will hit the mainstream. It definitely has a community of precious metal enthusiasts who prefer it over trusting a single issuer like Paxos or Tether.

3.9.6 UAE Case Study: OneGram and UAE Gold Initiatives

The UAE has been forward-looking in embracing crypto assets, including commodity-backed tokens, to leverage its status as a gold trading hub.

OneGram (OGC): Launched in 2017 by a Dubai-based company, OneGram was an attempt to create a **Shariah-compliant** cryptocurrency backed by gold. They conducted an ICO, reportedly raising a substantial amount (target was $500M), with each token initially representing a gram of gold in a Dubai vault. OneGram obtained a fatwa from Al Maali Consulting declaring it Shariah compliant. The idea was that as the network grew and was used for payments, a transaction fee charged in OGC would be used to buy more gold, thus continually increasing the gold backing per coin – a novel approach to rewarding early adopters with effectively increasing intrinsic value.

Technologically, OneGram was less transparent than newer projects; it's unclear if it ran on a private blockchain or an existing one (some reports suggest it was on Stellar or a fork of it). OGC traded on a small exchange (perhaps their own) but did not gain widespread traction. By 2019, OneGram faded from news, and its website eventually went offline. In retrospect, it likely suffered from the general ICO bust and the difficulty of bootstrapping a payment coin's usage. Its lofty raise target may not have been fully reached, and without continuous development or exchange adoption, it quietly stalled. OneGram's lesson was that **tying a token to gold isn't enough**; the project needs either strong technical execution or integration into financial systems. It did, however, spark the conversation on Islamic finance and crypto commodities – a legacy that projects like XAUt and Kinesis have also considered (ensuring their structures comply with Islamic principles).

Emirati Gold Tokens via DMCC and Others: The most notable recent UAE initiative is the DMCC Tradeflow-Comtech Gold token (CGO) we discussed earlier. To recap key points:

- 1 CGO = 1 gram of 99.99% gold.
- Each token corresponds to physical bars (1kg bars) stored in DMCC-approved vaults in Dubai.
- Each bar is registered as a DMCC Tradeflow warrant, giving a legal guarantee and tracking of ownership.
- Issued on the XDC blockchain for efficiency.
- Shariah-compliant, aimed at democratizing gold investment (smallest unit 1g).
- Launched in late 2022, demonstrating the UAE's commitment to leverage blockchain for commodities trade.

This project is ongoing and showcases UAE innovation: combining a government-backed trade platform (Tradeflow) with blockchain to increase transparency and ease of trading. It essentially digitizes the existing gold trade processes in UAE free zones.

Another development: **UAE's Regulators** – VARA has included asset-backed tokens in its regulatory framework under the term "Virtual Assets". ADGM's guidance from 2018 (and updated) explicitly mentions commodity tokens and how they may fit as either derivatives or spot depending on structure. In 2024, the Emirates Securities and Commodities Authority (ESCA) was reportedly working on rules for crypto commodities. Dubai's rapid move to regulate crypto in 2022-2023 likely means any gold token targeted at retail would need VARA approval.

Abu Dhabi Gold-backed Token: There were news of a company in Abu Dhabi planning a gold-backed stablecoin, possibly under the ADGM regime, but details are scant. It wouldn't be surprising, as ADGM was host to several crypto firms.

Private Sector: Some UAE-based jewelers or gold dealers have flirted with tokenization. For instance, Regal RA DMCC in 2017 got a license to trade cryptocurrencies and hinted at offering tokenized gold. Also, international firms like **Auruspartnered** with a Dubai vault (IBV Gold) around 2020 to allow minting of AurusGOLD tokens with UAE-stored gold. Aurus's multi-dealer model meant a user could buy an AWG token backed by gold from a Dubai supplier or a Spanish supplier interchangeably. This kind of partnership brings global token projects into the UAE ecosystem.

Summary of UAE stance: The UAE's case studies reflect a **proactive approach**:

- Encouraging innovation (OneGram in 2017 when few dared).
- Public sector involvement (DMCC in 2022 linking to trade infrastructure).
- Regulatory clarity (with VARA and ADGM frameworks).
- Integration with Islamic finance principles (most projects got Shariah certification).
- Aim to boost gold trade (tokenization seen as a way to increase liquidity and attract investors to UAE vaults, as they can trade 24/7 globally).

Going forward, UAE could become a hub for tokenized commodity trading, given its strong commodity sector and crypto-friendly policies. Projects like CGO could scale up, and perhaps we'll see DGCX (Dubai Gold & Commodities Exchange) or others launch tokenized gold futures or spot tokens on licensed exchanges.

3.10 Scalability, Interoperability, and Auditability in Practice

(This section is a brief reflection tying together the technical aspects demonstrated by the case studies, reinforcing how current implementations handle or struggle with these aspects.)

From the case studies, we glean how various projects approached scalability:

- PAXG and XAUF stick to major chains (Ethereum/Tron) and scale via centralized exchanges rather than on-chain transfers – a pragmatic approach that leverages existing infrastructure.
- Kinesis built a scalable custom chain (thousands of transactions per second) to support microtransactions in gold, showcasing a path for high throughput.
- Comtech Gold on XDC chose a chain with low fees, anticipating high retail volume in 1g tokens.

Interoperability:

- Tether bridged Ethereum and Tron communities.
- VNX Gold bridging multiple chains shows a push for interoperability, ensuring no matter which blockchain platform an investor uses, they can hold the gold token there.
- DMCC's token bridging trade finance (warrants) with blockchain is interoperability between systems.
- No project yet allows **seamless atomic swaps** of gold tokens between different blockchains without going through an exchange or custodian, indicating room for cross-chain protocols to mature.

Auditability:

- All successful projects embraced transparency: PAXG and XAUT publish bar details, PMGT piggybacked off GoldPass audits, Kinesis publishes audit reports.
- On-chain monitoring by third parties (Chainlink PoR for Paxos) is an emerging norm.
- Even when projects closed (Digix, PMGT), the audit trail helped unwind responsibly.
- A point of improvement is to see more real-time public audit feeds (beyond Paxos) and maybe even **zero-knowledge proofs** that could confirm reserves without revealing sensitive info (an area being researched in 2025).

In terms of compliance-by-design:

- Paxos and others have the ability to freeze (satisfying regulators that they can intervene in illicit cases).
- ERC-3643 tokens haven't been mainstream for gold yet, but likely will come into play for institutional platforms (e.g., a tokenized gold ETF might use it to enforce only authorized participants can hold it).
- The HSBC Gold token case shows a private DLT approach where compliance is inherently enforced by the closed nature (only HSBC KYC'd customers on the ledger). It's a different path than public chain tokens but achieves similar end of fractional gold access.

Finally, blockchain analytics is quietly working in the background. As large holders move gold tokens, we have visibility – for example, one can see if exchanges shift assets to cold storage or if whales accumulate. This kind of transparency sometimes even surpasses traditional gold market insights (where central banks and sovereigns operate opaquely).

Overall, the technology and architecture of tokenized gold and metals as of 2025 have **matured significantly** from the experimental days of 2017. We now have multiple robust implementations across jurisdictions. Each contributes to an evolving blueprint of best practices:

- **Robust smart contracts** (audited, with upgrade and freeze capabilities as needed).
- **Solid backing and custody** (allocated bullion, reputable vaults, insurance).
- **Clear compliance frameworks** (working within regulations or even enhancing compliance through code).

- **Integration with finance and DeFi** (ensuring these tokens are not in isolation but part of financial products and services).

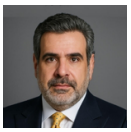
The next steps likely involve scaling these solutions to broader markets, enhancing interoperability (maybe a global standard so a gold token on Ethereum could be swapped with one on XDC or Tezos smoothly), and continuing to build trust through transparency (perhaps automated audits or even regulator nodes in networks).

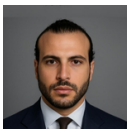
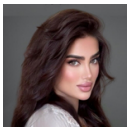
Conclusion: The marriage of precious metals with blockchain tech has given birth to a new asset class that retains the timeless value of gold and silver while gaining the speed and openness of crypto. Module 3 has delved into the technical and architectural backbone of this asset class, revealing a landscape of innovation that balances on-chain code and off-chain metal. With strong foundations now in place, tokenized metals are poised to play a significant role in portfolios, trading markets, and payment systems, all under the watchful eyes of code, regulators, and investors alike – a true melding of old-world asset security with new-world technology.

Hoot Professionals

Meet The Visionaries

Driving legal brilliance and innovation at the intersection of strategy, technology, and global investment insight. Where law meets code, capital, and clarity.

Name	Designation	Regions of Operation	
Ghassan Makki	Founder and Managing Partner - Financial Markets and Digital Assets	UAE, Sudan, Qatar, KSA, Bahrain	
Nicholas Kairis	Senior Partner - Financial Markets and Digital Assets	USA, Greece, Germany, Cyprus, UAE	
Fahad Al Howdari	Principal Advocate - Litigation	UAE	
Adil A. Babiker	Senior Partner - Insurance and Islamic Finance (Sovereign/Private)	Sudan, Saudi Arabia, USA, UAE, Qatar, Bahrain	

Name	Designation	Regions of Operation	
Abdullah Metwalli	Co-founder & Managing Legal Associate - Financial Markets & Digital Assets	UAE, United Kingdom, Australia	
Vladyslav Mozharov	Senior Advisor - High Value Real Estate Tokenization	Ukraine, Russia, Turkey, Italy, UAE	
Yuki Yoshizawa	Senior Investment Advisor - M&A and Medical Technology	Japan, UAE	
Luca Rubino	Senior Venture Capital Advisor - AI and Cybersecurity	USA, Italy, France, UAE	
Ibrahim Igbariye	Investment Advisor - Real Estate Tokenization	Israel, UAE	
Salwa Alhawamda	Business Setup and CSP Advisor - Fintech	Canada, UAE	
Farhan Ahmed	Barrister at Law - Arbitration and Disputes Resolution	United Kingdom, Singapore, UAE	

Name	Designation	Regions of Operation	
Kamal Touma	Partner CMO	UAE	
Wajeeha Zia	Legal Associate - Financial Markets and Digital Assets	Pakistan, UAE	
Moamen Mohamed	Legal Associate - Financial markets and Digital Assets	Egypt, UAE	

Contact Information

You can reach out to us at:

- Email: info@hootlegal.com
- Phone: +971 58 5592991
- Website: www.hootlegal.com