

Project DESFT
Build Trusted Digital Credential
for Inclusive Finance

Whitepaper

Jointly Incubated and Designed by
Solv Foundation and zCloak Network

Content

1. Abstract
2. Project Analysis
3. Project Background and Approach
4. Core Architecture
5. Use Case Analysis
6. Technical Advantages
7. Conclusion and Vision

1. Abstract

Project DESFT, designed and incubated jointly by Solv Foundation and zCloak Network, and developed by Ample FinTech, is a Distributed Trusted Digital Credential Network with a focus on cross-border trade and financial services. This initiative aligns with the open strategies of the Monetary Authority of Singapore (MAS) and the Bank of Ghana (BOG) in the field of inclusive FinTech.

Credentials act as a foundation of trust, covering an array of digital documents such as tickets, licenses, invoices, contracts, and official records. These documents are extensively utilized in everyday activities, commercial exchanges, and financial dealings as embodiments of trust. In compliance with international technical standards, Project DESFT has developed verifiable credentials that operate independently of any centralized platform. The project enables the issuance, attestation, storage, verification, and management of a wide range of digital credentials, encompassing digital IDs, invoices, licenses, contracts, and official paperwork. Through this initiative, the concept of "trust" is digitized, networked, and tokenized, harnessing the power of blockchain and cloud computing to forge a universally trusted network.

Just as Bitcoin provides a platform for peer-to-peer digital currency exchanges and Ethereum enables smart contract capabilities, Project DESFT positions itself as the cutting-edge network dedicated to facilitating Trusted Digital Credentials.

Key functions and features of Project DESFT include:

- A comprehensive one-stop solution to create, approve, attest, verify, present, circulate, and regulate trusted digital credentials.
- The use of cryptographic algorithms governs the entire flow of issuing, attesting, presenting, and verifying digital credentials. This approach removes the need for centralized platforms and trusted third parties, thereby guaranteeing full data sovereignty for users.

- Controllable transparency: In Project DESFT, a digital credential is represented in two ways – as a Verifiable Credential (VC) stored privately and as a Verifiable Credential Semi-Fungible Token (VCSFT) published on the blockchain. This selective disclosure mechanism allows credential holders to control the transparency of their information, addressing a longstanding challenge in blockchain applications.
- Capability to represent all types of credentials, including but not limited to personal and enterprise IDs, badges, licenses, tickets, qualifications, bills, invoices, receipts, L/Cs, B/Ls, warehouse receipts, checks, promissory notes, bills of exchange, drafts, various contractual documents.
- Support of the Universal Trusted Credential (UTC) standard proposed by the United Nations Development Programme (UNDP), aiding SMEs in developing regions to efficiently conduct credit verification in international trade and access inclusive financial services.
- Support of regulatory technology, empowering regulators to modify the status of VCs and VCSFTs. This functionality includes actions like revoking, suspending, or issuing warnings regarding the validity of credentials, effectively fulfilling regulatory goals.
- Interoperability with popular digital asset standards like ERC-20/721/1155 plays a key role in programmable payment and digital asset management.
- The technical architecture is not only meticulously engineered for seamless integration with traditional systems but also adeptly aligned with swiftly advancing frontier technologies such as Artificial Intelligence (AI) and Zero-Knowledge Proofs (ZKP).

Project DESFT, framed within the context of international trade and financial services, is strategically designed to align with the practical demands of multiple nations' central banks, financial institutions, global trade, and economic development organizations, as well as import-export-trading companies.

It focuses on creating and integrating applications with Central Bank Digital Currencies (CBDCs) and programmable money systems, thus accelerating the adoption of digital credentials into a functional and active stage.

2. Problem Analysis

As the global supply chain reorganized, facilitating the participation of micro, small, and medium-sized enterprises (MSMEs) within this international framework has become a significant global challenge. In response, numerous governments and international organizations are advocating for the proactive deployment of advanced digital technologies. This initiative aims to bolster inclusive financial growth and assist MSMEs in developing areas to rapidly assimilate into the worldwide trade infrastructure.

Consider a scenario where an East Asian coffee importer aims to procure indigenous coffee beans from a West African country. Although such international trade is common and occurs in large volumes daily, it is inherently intricate, involving numerous processes and details. These stages encompass trade preparation, negotiation, contract execution, and fulfillment, which includes assessing supplier credit, inspecting the quality of goods, conducting quarantine checks, managing warehousing and logistics, processing payments, clearing goods through import customs, insuring cargo, and securing supply chain financing. Despite advancements in internet and financial technologies that have digitized many aspects of international trade, some elements remain mired in cumbersome manual or paper-based processes, creating significant bottlenecks in the trade workflow.

In the referenced coffee trade example, a new coffee bean supplier faces several crucial challenges.

How can the supplier demonstrate its qualifications and build credibility with international clients and financial institutions to secure orders? How can the supplier obtain local financial support for cargo insurance and trade financing? How can the supplier effectively navigate the credit system to streamline payment processes? Currently, these aspects largely rely on manual procedures, which are not only time-consuming but also costly.

Consequently, many small and micro-scale suppliers find themselves systematically marginalized from the global trade ecosystem due to these inefficiencies and high costs.

It becomes evident that the core issue at hand is not technology, but rather trust. The process of international trade navigates through several trust boundaries, necessitating an array of credentials and documents to serve as carriers of trust among diverse participants. These credentials and documents need to be issued swiftly and with ease, while ensuring they are tamper-proof, verifiable, and cost-effective.

Despite advancements in technology, mainstream internet infrastructure and centralized digital economies still face challenges in effectively supporting digital credentials. The Internet, originally designed for sharing information, inherently lacks mechanisms for establishing trust and verifying identities. To address this, major Internet companies like Amazon, Meta, and Alibaba have each built vast, centralized digital platforms. Within these ecosystems, they aim to solve trust issues by creating their own account systems, data governance structures, and trust models. However, this centralization requires users to place their digital rights, including their digital identity, data sovereignty, and privacy, in the hands of these central authorities.

As long as all participants have confidence in the central platform, credentials and documents can be managed within a centralized database.

This centralized framework, however, is not sustainable for many businesses involved in international trade and finance, and it fails to meet the expectations of government agencies and regulatory authorities.

Firstly, the centralized model leads to a loss of data sovereignty and privacy for participants. Data is a critical component of contemporary production, intertwined with corporate governance, trade secrets, and the fundamental assets of government entities, as well as individual privacy. The relinquishment of control over this data and the erosion of privacy cannot be accepted by many stakeholders, as it poses significant risks to their operational integrity and competitive advantage.

Secondly, the efficiency of centralized platforms depends on all participants using the same platform. When it comes to inter-platform interactions, there are considerable inefficiencies and complexities. Each platform seeks to gather data from others while protecting its own, creating significant barriers to data exchange and collaboration across different platforms. This often results in a fragmented landscape where the full potential of digital ecosystems cannot be realized due to these interoperability challenges.

Thirdly, the power dynamics within this centralized model are heavily imbalanced, with platforms having the ability to extensively monitor and restrict users, while users have little to no oversight or control over the platform's operations.

This disparity can lead to the potential misuse of power, such as unauthorized data harvesting, storage, analysis, targeted advertising, price discrimination, and monetization of user data—practices that users are often oblivious to and consequently unable to challenge. This lack of transparency and control undermines user autonomy and can erode trust in the digital ecosystem.

Fourthly, the centralized model presents considerable security risks. Individuals and organizations must generate, remember, and manage numerous usernames and passwords. Research indicates that an average enterprise user has to handle 191 passwords, with 70% questioning their effectiveness in protecting online accounts.

This vulnerability has opened the door to widespread cybercrime, as malicious actors can often bypass security protocols, resulting in theft, fraud, and extortion. By 2021, the financial repercussions of cybercrime had soared to an alarming \$6 trillion globally.

Lastly, the complexity and opacity of centralized systems pose significant challenges for regulation. Government and regulatory bodies struggle to perform proactive oversight or respond quickly to violations within these systems. Regulators are frequently forced into a reactive stance, attempting to enforce accountability after infractions have taken place. By this stage, the harm to users' data sovereignty and privacy is often irreversible, demonstrating the need for systems that allow for more transparent and timely regulatory intervention.

These challenges extend beyond international trade and affect various sectors, including financial technology, e-commerce, social media, and office applications operating under the current internet architecture. All these areas are hindered by the centralized trust models that dominate today's digital interactions.

This reliance on central authorities for trust has become a significant barrier to the advancement and diversification of the digital economy.

The advent of Bitcoin in 2008 kindled hopes from global internet and digital economy experts that blockchain technology would revamp the internet's layer of trust. The optimism intensified with Ethereum's debut in 2015, given blockchain's notable strengths in data management, which include:

- multi-party maintenance
- cryptographic consistency
- tamper-resistance
- non-repudiation

These attributes facilitated Bitcoin's development of a decentralized peer-to-peer digital currency and Ethereum's creation of decentralized smart contracts, both conceptually acting as carriers of trust. Consequently, blockchain was anticipated to rapidly establish itself as a fundamental layer of trust and value for the internet, remedying its trust deficit.

Yet, after nearly a decade, it is evident that blockchain alone falls short of achieving this objective due to:

- Mainstream blockchains lack privacy protection for transaction data, rendering all transactions transparent. This poses a risk for businesses as competitors can easily gain insights into their operational specifics.
- The inability of blockchains to store large volumes of data efficiently, resulting in bloated systems with diminished performance.
- The oversimplification of blockchain accounts, lacking a comprehensive metadata mechanism, thus failing to address complex business requirements.
- The challenge of integrating pure blockchain structures with emergent technologies such as AI and big data.

Evidently, there is a need for a solution that transcends blockchain, one that diminishes dependency on centralized platforms and caters to the needs of enterprise users in terms of data sovereignty, privacy protection, system efficiency, and flexibility.

3. Project Background and Approach

Project DESFT aligns with the open strategies of the Monetary Authority of Singapore (MAS) and the Bank of Ghana (BOG) in the field of inclusive FinTech. It is designed and incubated jointly by Solv Foundation and zCloak Network, and developed and supported by Ample FinTech to build an advanced Trusted Digital Credential Network. It focuses on enabling micro, small and medium-sized enterprises (MSMEs) in developing countries like Ghana, to generate and manage digital credentials, thus providing verifiable qualifications and facilitating their integration into the international trade supply chain. This initiative not only assists in building credible trade histories to improve credit ratings but also eases the path to financial support.

Tailored for MSMEs in developing nations, Project DESFT is committed to tokenizing trusted digital credentials on the blockchain, thereby supporting MSME participation in international trade and granting access to efficient, accurate, and affordable financial services.

The technical objectives of the first phase include:

- Creating self-sovereign identity accounts for enterprises, supporting extensive business operations while securing the ownership of enterprise identity and data, and safeguarding corporate data privacy.
- Developing a suite of universally applicable, verifiable digital credential technologies, aligned with international standards, that are capable of representing diverse credentials in commercial trade and financial contexts.
- Supporting the Universal Trusted Credential (UTC) standard initiated by the United Nations Development Programme (UNDP), aiding MSMEs in creating and employing the necessary digital credentials for cross-border trade.
- Facilitating the principal regulatory functions proposed by authorities, thus enabling them to oversee the status of issued digital credentials.
- Integrating with Central Bank Digital Currencies (CBDC) to enhance the automation of cross-border trade procedures via programmable payment technologies.

To fulfill its goals and address previously mentioned challenges, Project DESFT introduces a groundbreaking concept utilizing the World Wide Web Consortium's (W3C) Verifiable Credential (VC) technology. This approach, which involves tokenizing VCs to be presented on blockchain, aims to strike a balance between data sovereignty, privacy protection, transparency, transferability, and regulatory compliance.

VCS, alongside their closely associated Decentralized Identifiers (DIDs), developed and endorsed through years of dedicated effort by digital identity and credential specialists under the W3C framework, are emerging as the fundamental protocols for self-sovereign identity and data.

VCS, designed in accordance with W3C standards, offer an optimal means of establishing trust in the digital economy, characterized by:

- Complete data sovereignty for holders
- Robust security against tampering, duplication, and theft
- Ease of verification
- Privacy-first with support for selective disclosure
- Status management enabling freezing, revoking, expiring, and modifying operations
- Almost negligible operational costs

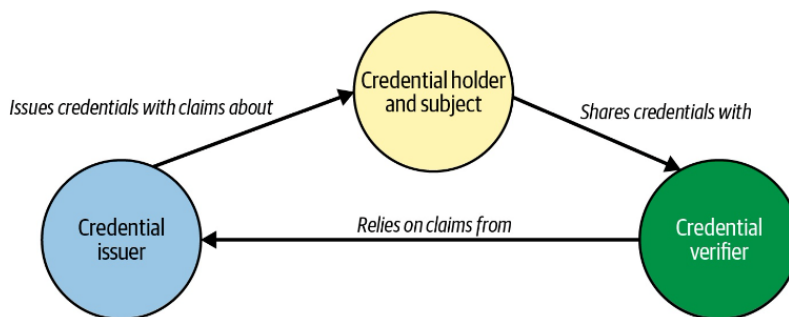


Figure 1. The Main Collaborative Parties of VC and Their Interrelationships

W3C's VCs are versatile, representing a broad range of credentials, including ID cards, business licenses, certificates, attestations, qualifications, invoices, receipts, admission tickets, membership cards, financial documents, proof of ownership, and contracts, among others. These credentials are crucial in international trade scenarios and can be developed using VC standards.

However, W3C's VC is a universal standard that doesn't inherently cater to specific technological architectures or scenarios. In numerous applications, VC alone proves insufficient. For instance, in international trade, regulatory bodies require real-time VC status updates, including the ability to freeze or revoke certain VCs, a feature not directly stipulated in the W3C standards. Additionally, the standards don't support the transfer and trading of VCs representing digital assets. Crucially, in trade contexts, critical credentials closely linked to payments are not addressed by the W3C standards.

Project DESFT introduces a novel approach called "VC Tokenization," which utilizes the W3C DID and VC standards. By incorporating ERC-3525 semi-fungible tokens, the system allows for the tokenization of selectively disclosed information from W3C-standard VCs onto the blockchain.

Consequently, digital credentials are represented in two distinct forms: as on-chain tokens, referred to as VCSFTs, and as off-chain VCs. The two are interlinked, with one-to-one binding through cryptographic mechanisms for distinct functions. Off-chain VCs are primarily used for issuing, disclosing, and verifying identity and qualifications in contexts where privacy preservation is paramount. Meanwhile, VCSFTs enable on-chain functionalities such as timestamping, managing the regulatory status of VCs, and seamless interoperability with blockchain smart contracts. This integration paves the way for programmable payments and the development of innovative DeFi products.

Notably, VCSFTs, managed by on-chain smart contracts, can interoperate with digital currencies, including cryptocurrencies and CBDCs, to streamline complex cross-border trade payment processes including fund delivery, margin management, tax payments, and more. This integration also extends the smart contracts' programmability and automatic execution capabilities to other intricate scenarios, such as contract signing, notarization, and execution.

Project DESFT thus creates a unique digital identity and credential solution, synergizing the strengths of blockchain tokens and VCs to more effectively cater to a variety of application scenarios.

4. Core Architecture

As discussed earlier, VCs based on W3C standards exhibit some limitations, such as challenges in representing timestamps, indexing, and showcasing transaction data. However, blockchain's features of immutability, traceability, public accessibility, and real-time updates can effectively complement these limitations in VCs. Addressing this, DESFT introduces an innovative concept of tokenizing VCs on-chain, thereby harmonizing off-chain VCs with on-chain VCSFTs to adeptly manage intricate application scenarios.

In the domain of digital tokens, the most commonly known types are ERC-20 (fungible tokens) and ERC-721 (non-fungible tokens). To meet the unique needs and application scenarios of DESFT, ERC-3525 (semi-fungible tokens) has been chosen as the optimal token standard for representing Verifiable Credentials on the blockchain.

Ratified in September 2022, ERC-3525 is an Ethereum EIP (Ethereum Improvement Proposal) that sets the technical standards for semi-fungible tokens. These tokens combine the unique metadata representation capabilities of ERC-721 non-fungible tokens with the divisibility and mergeability features of ERC-20 fungible tokens. This hybrid functionality is what grants them the semi-fungible classification.

In practical applications, ERC-3525 is primarily used to create programmable digital vouchers, exhibiting several notable characteristics.:

- **Visualizable:** ERC-3525, akin to ERC-721 NFTs, supports extensive metadata, thereby facilitating dynamic information display, particularly apt for voucher representation.

- **Containment:** An ERC-3525 token has the capacity to encapsulate and manage a diverse range of digital assets. The logic governing the acceptance and management of these assets can be customized programmatically. This characteristic provides ERC-3525 with a distinct advantage for representing financial vouchers.
- **Divisible and Combinable:** Unique in their entirety, ERC-3525 tokens can be segmented into uniform portions, which are capable of independent circulation and recombination, maintaining consistency in information and synchrony in status.
- **Programmable:** ERC-3525 tokens are entirely programmable, ranging from their external appearance, internal state, to asset management protocols. Moreover, their interface is compatible with ERC-721, adhering to Ethereum's general token interaction standards, thus facilitating seamless integration with other smart contracts.

Project DESFT leverages the advantages of ERC-3525 by tokenizing VC into VCSFTs and linking them with their corresponding original VCs. This creates a dual-structure system known as a "VC-VCSFT Pair." The VCSFT token displays information on the blockchain publicly, whereas the off-chain information is securely encrypted and privately maintained by enterprises in the form of a VC.

The VC-VCSFT dual structure is a cornerstone in understanding the technological innovation of Project DESFT. Verifiable Credentials (VCs) are off-chain documents managed according to W3C standards. Holders, attesters, and verifiers interact with VCs using cryptographic methods and digital signatures, creating a robust framework for managing digital credentials. Tokenizing VCs into VCSFTs on the blockchain is justified by several compelling reasons:

- The blockchain serves as a "bulletin board," enabling the holder to selectively disclose parts of the VC. By minting publicly disclosable information into a VCSFT and publishing it on-chain, all public users can witness the information, which enhances the trust in the digital credentials.
- VCSFTs provide a natural timestamp for their associated VCs, lending additional credibility to the credentials.

- VCSFTs function as indices for their corresponding VCs, facilitating access to the original VC with the holder's consent.
- As asset representations, VCSFTs embody digital credentials of ownership, usage rights, or other entitlements, with the blockchain acting as the infrastructure for their circulation and transactions.
- On-chain VCSFTs indicate the public status of the entire credential. For example, if a regulatory authority needs to suspend a digital credential, updating the status of the on-chain VCSFT effectively suspends the whole credential, including the off-chain VC.
- VCSFTs, as defined by ERC-3525, are programmable and naturally compatible with digital currencies and assets. This "activates" static digital credentials for new applications in payments, asset management, trading, and attestations. For instance, VCSFTs can act as payment receipts, allowing for the direct transfer of digital currency to the receipt, which integrates payment and voucher processes and significantly improves efficiency.

A complete usage of Project DESFT's "VC-VCSFT Pair" involves:

- Enterprises, as Claimers, create VC Claims on the DESFT platform that includes their entity's basic information.
- Regulators attest VC Claims off-chain and transform minimally necessary information into on-chain VCSFTs in accordance with the ERC-3525 standard.
- Enterprises maintain full data sovereignty with off-chain VCs, with the option to selectively disclose information to the public via on-chain VCSFTs.
- Service providers, including financial institutions that serve as Verifiers, have the ability to confirm enterprise information through a secure, end-to-end encrypted messaging channel. They can also verify the completeness, authenticity, and validity of the VC information supplied by the enterprise by examining its digital signature and the corresponding on-chain VCSFT.

- In cases of legal violations, regulators have the right to warn, suspend, revoke, temporarily or permanently invalidate the on-chain VCSFTs, among other actions. When a VCSFT is invalidated, its status is visible on-chain to everyone. Therefore, even if the enterprise still holds the off-chain VC, the corresponding on-chain VCSFT's invalidation prevents them from obtaining valid services, achieving real-time monitoring and management of VC status.

While DESFT's application scheme is nearing completion, there remains concerns in its system registration and login aspects. Traditional centralized databases use stored usernames and passwords for verification and login, posing significant risks of data leakage and legal issues regarding data export in international activities.

To address this, Project DESFT innovatively introduces IDSFT as an enterprise account credential for system registration and login. IDSFT, also inherently an on-chain ERC-3525 token, encompasses vital enterprise information, decentralized identifiers (DID), and other essential data. IDSFT's self-custody by enterprises mitigates risks associated with centralized database leaks, and as it serves as an enterprise's own "identity card," ensuring full data sovereignty, and effectively avoiding legal issues related to data export in DESFT.

Credential	IDSFT	VCSFT	VC
Storage	On-chain	On-chain	Off-chain
Data Standard	ERC-3525	ERC-3525	W3C VC Standard
Scenarios	Enterprise ID Register and Login	Publish Enterprise Info Verify Enterprise Status Verify VC's Validity	Present verified enterprise info without issuing complicated certificates
Ownership	Enterprise	Authorized Parties	Enterprise
Transparency	Public	Public	Private

Table 1. Comparison of the Three Types of Credentials in Project DESFT

DESFT approaches an ideal equilibrium by safeguarding enterprise data privacy, ensuring data reliability, and meeting regulatory requirements.

	On-chain VCSFT	Off-chain VC
Claimer/SME	Selective Disclosure	Full Access
Attester	Mint and View	Only Authorized
Verifier	Only View	Only Authorized
Supervisor/Regulator	Change status and revoke	Only Authorized
Public	Only View	Cannot Access

Table 2. Overview of Different Parties' Access to the "VC-VCSFT Pair"

As illustrated in Table 2, DESFT skillfully controls data access for all stakeholders while simultaneously safeguarding the data ownership rights of regulatory authorities and enterprises.

In "VC-VCSFT Pairs," VCSFT, the publicly visible on-chain element, is crucial for verifying VC's validity. Project DESFT has defined five distinct statuses for VCSFTs to reflect various states of the credentials:

- **Effective:** The normal state for a qualified VC once attested and tokenized. When VCSFT is in this state, it indicates that the VC is valid and can be fully trusted by third parties.
- **Warned:** An abnormal state. When regulatory authorities deem a VC potentially risky, they change its VCSFT status to Warned. The VCSFT status can revert to Effective once the warning is revoked.
- **Suspended:** An abnormal state for high-risk VCs. Regulators change the VCSFT status to Suspended, pausing its use until facts are clarified. In this state, third parties no longer accept the VC.

- **Expired:** VCs have an expiration date at issuance, synchronized to VCSFTs during tokenization. Regardless of the previous three states, VCSFTs automatically expire upon the date, thus invalidating the VC.
- **Revoked:** An extreme situation. When regulators find a non-expired VC violates laws or regulations, they can directly change the VCSFT status to Revoked, rendering the VC void.

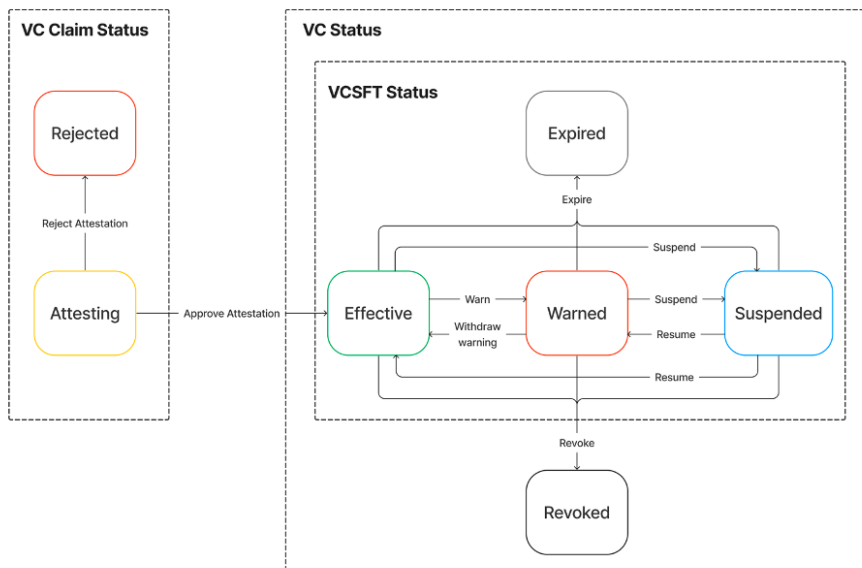


Figure 2. Diagram of the Status Transition of VC, VC Claim, and VCSFT

The corresponding VC remains a VC Claim until receiving an Attestation. Typically, it's in either Rejected (unattested) or Attesting (under review) status. In these states, VC Claims cannot be tokenized, thus preventing the misuse of VCSFTs.


5. Use Case Analysis

In traditional international trade, MSMEs frequently grapple with challenges stemming from insufficient documentation and intricate certification processes. Take Alice Beans, a small African business specializing in coffee beans, which receives a substantial order from East Asia. Prior to formal trading, Alice Beans must furnish a host of credentials and quality certifications.

In this situation, Project DESFT plays a crucial role, offering Alice Beans a streamlined digital certification process that bolsters trust and transparency for all involved parties.

First, Alice Beans establishes a digital identity on the Project DESFT platform, known as IDSFT, which becomes their authenticated digital identity credential.

Powered by Ample Fintech & zCloak
Created on 2023-10-30

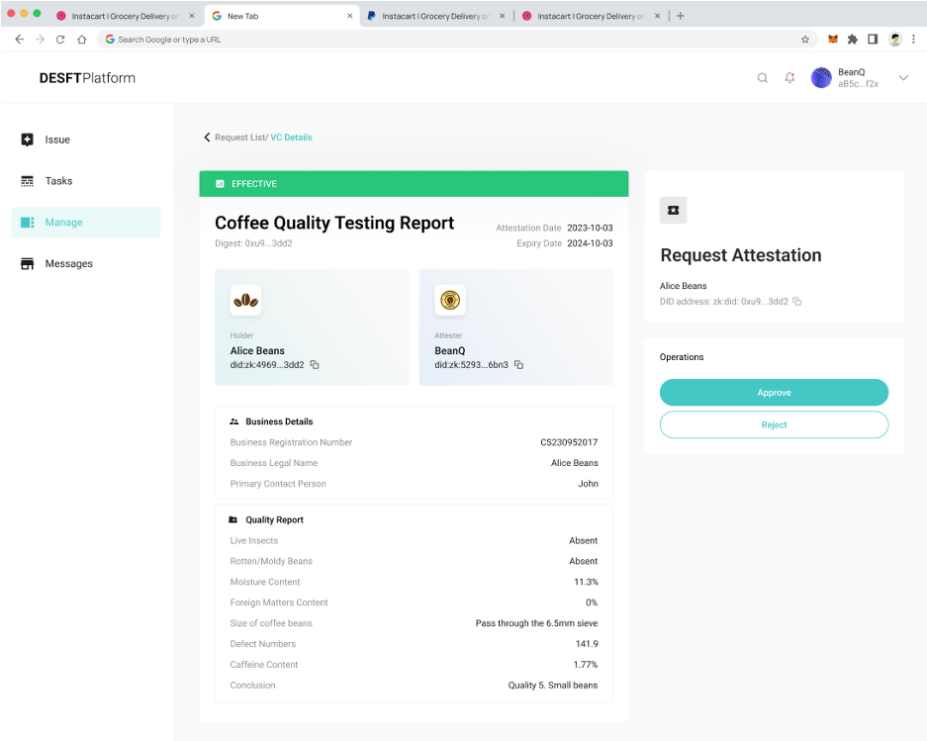


Alice Beans

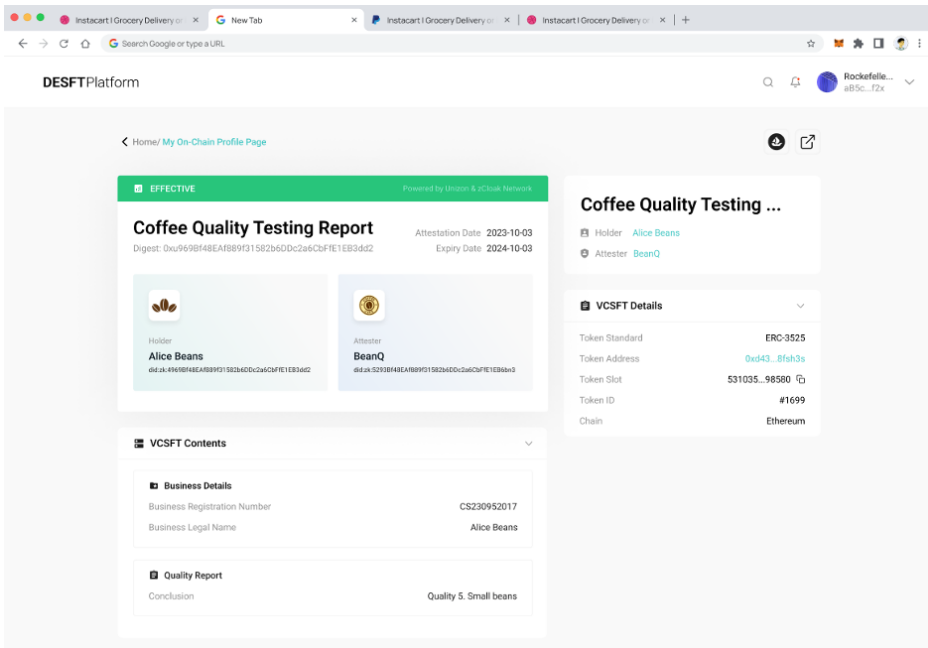
did:zk:4969Bf48EAf889f31582b6Dc2a6CbFfE1EB3dd2

Country of Registration	Ghana
Business Registration Number	S230952017
LEI Code	984500V05HDA8AAP8924
Website	Alicebeans.com

Then, Alice Beans prepares a digital quality statement, a Verifiable Credential Claim (VC Claim), and submits it to BeanQ, a coffee bean inspection agency. Upon BeanQ's inspection of quality standards, they endorse the claim, converting it into an official Verifiable Credential (VC).

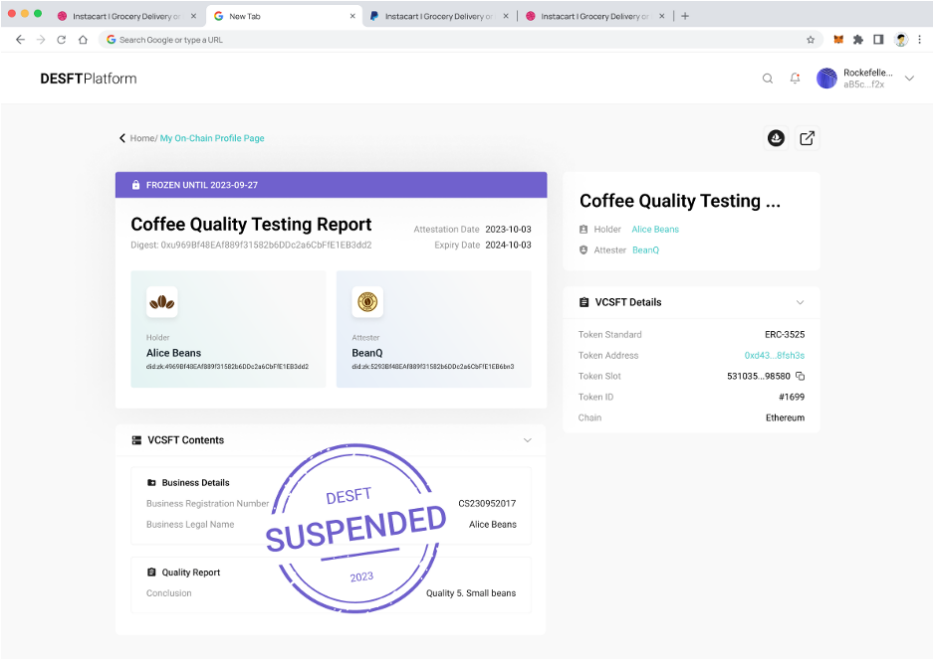


This marks just the beginning. Through Project DESFT, Alice Beans can not only generate a comprehensive VC but also selectively disclose specific information, creating an on-chain token called VCSFT. This mechanism of selective disclosure protects Alice Beans' proprietary information while allowing public access to their verified credentials.



VCSFT enables tracking of the credential's origin. Particularly significant when VCSFT acts as a credential for asset rights, it utilizes blockchain and DeFi infrastructure to facilitate the secure and efficient transfer and trading of digital assets. Thus, VC and VCSFT not only endorse qualification credentials but also support data such as basic company information, licenses, certificates of conformity, orders, contracts, invoices, warehouse receipts, bills of lading, drafts, and more. This functionality allows businesses to readily prove their qualifications, credibility, and transaction history to prospective clients or financial institutions, facilitating their entry into international trade and financial services.

More importantly, should any concerns about Alice Beans' product quality emerge in the future, regulatory authorities can swiftly respond by adjusting or freezing the relevant VCSFTs, ensuring trade integrity and security.



Therefore, Project DESFT not only simplifies Alice Beans' entry into international trade but also establishes a reliable and efficient trading environment for all participants, positioning trust as a fundamental element of the digital economy.

6. Technical Advantages

Project DESFT unites the ERC-3525 semi-fungible token technology with W3C's VC and DID, pioneering the tokenization of VCs and DIDs on-chain. This innovation boasts several key technological strengths:

- Project DESFT establishes unique, privacy-preserving, secure digital identities for enterprises. Utilizing ERC-3525 to tokenize these identities into IDSFTs reduces password-related burdens and information leakage risks, paving the way for enterprise participation in the emerging decentralized digital economy.
- Project DESFT tackles a persistent issue in the FinTech industry: the excessive dependence on third-party centralized platforms. By addressing the concern of centralized platforms wielding too much power, it ensures user data sovereignty and fosters the growth of a collaborative, cross-border digital economy ecosystem.
- Project DESFT presents an innovative approach to digital credential tokenization. Utilizing the ERC-3525 standard, it converts enterprise digital identities into IDSFTs and digital assets into VCSFTs, both represented as on-chain, verifiable credentials. These credentials provide advanced functionalities, including dynamic visualization, real-time status updates, and efficient management of digital assets.

- Using the “VC-VCSFT Pair” structure, Project DESFT enables versatile credential representation with controllable transparency, balancing data privacy with visibility, and addressing both liquidity and regulability.
- Project DESFT integrates four pivotal functionalities—digital credential management, digital asset management, data asset oversight, and programmable payments—into a single system. This enhances the management of complex digital assets and transaction processes, especially in intricate international trade and finance scenarios.
- Project DESFT empowers regulators with rapid access to essential information, enhanced decision-making capabilities, and the ability to take enforcement actions by adjusting the status of VCSFTs. This advanced regulatory technology exceeds traditional approaches, providing more effective oversight and supervision.
- Project DESFT is committed to a user-friendly interface, providing professional, easily navigable interfaces for diverse stakeholders, including businesses, authorized attestors, and regulatory bodies.

7. Conclusion and Vision

In this whitepaper, we have identified the limitations and risks inherent in the centralized trust model commonly found in current global supply chains and financial systems. To overcome these challenges, we propose an innovative solution known as Project DESFT, which is a decentralized trust network that offers a range of features and benefits.:

- First and foremost, the initiative integrates the semi-fungible token technology of blockchain, ERC-3525, with Verifiable Credential technology. This combination greatly improves the flexibility and verifiability of the VC system. Through the tokenization of VCs into VCSFTs and their selective disclosure on the blockchain, the project effectively protects sensitive corporate information while also complying with legal disclosure obligations.
- Secondly, ERC-3525 offers an ideal framework for the tokenization of Verifiable Credentials. By leveraging ERC-3525, it becomes possible to track, split, and transfer a business's VCSFT on the blockchain, significantly enhancing the liquidity potential of digital assets. From a regulatory perspective, the system empowers authorities to alter or revoke the status of VCSFTs in response to legal or regulatory violations. This feature overcomes the constraints of traditional credential systems and underscores Project DESFT's flexibility and user-friendliness.
- Finally, the "VC-VCSFT Pair" structure within Project DESFT manages access rights for all stakeholders in relation to VCs and VCSFTs. This design achieves a harmonious balance between privacy, transparency, and regulatory compliance within the decentralized trust network.

Looking ahead, Project DESFT aims to incorporate Central Bank Digital Currency (CBDC) payments and digital asset management into its platform. Additionally, the project is exploring the use of zero-knowledge proofs and AI technologies to address increasingly complex application scenarios.

Contact us: erc3525@solv.finance