DSC^3 - Digital Symmetric Core Currency Cryptography

DSC^3 technology enables central banks to create and issue a safe, secure and non-counterfeitable Central Bank Digital Currency (CBDC) as a digital bearer instrument, which meets the scale, interoperability, instant settlement and other operational and policy requirements for use as legal tender alongside notes and coins.

Introduction

DSC^3 is a central bank security technology for operationalizing CBDC. At its core, DSC^3 utilizes symmetric key cryptography along with layers of digital security to ensure that the resultant cryptographic objects, i.e. digital bearer instruments in the form of a cryptogram, are protected from counterfeiting. It supports centralized, decentralized, and hybrid architectures. DSC^3 is highly scalable, capable of supporting high volume retail CBDC usage in even the largest economies. It is energy efficient and environmentally 'green.' It requires minimal energy for creation, distribution and processing of transactions.

Key Characteristics of the DSC^3 Technology

Bearer Instrument

DSC^3 allows CBDC to be issued as a true bearer instrument, like notes and coins, which settles instantly and with finality. There is no subsequent backend settlement, RTGS transfer, consensus or ledger reconciliation needed. DSC^3 technology allows central banks to issue a digital form of M0, a digital object (or bearer instrument), comprised of layers of security that prevent it from being modified or counterfeited. This instrument can then be put into circulation through commercial banks, payment services and electronic wallet providers. It can be stored by these private sector participants and passed from one wallet to another to settle transactions. The instrument itself is independent from the digital wallets and payment systems that store or transact with it.

As it is another form of M0, the digital instrument is, by law, legal tender and universally accepted. This is supported by the DSC^3 technology which decouples the instrument from the wallets and payment systems. This is analogous to notes and coins being stored in physical wallets or safes. While they are moved from one holder to another, they themselves remain unique central bank security instruments. A true digital bearer instrument, as created by DSC^3

technology, is a unique security instrument regardless of the organization providing the electronic wallet or participating in a transaction, thus, allowing it to be universally accepted.

Three Optional Architectures

DSC^3 supports different CBDC architectures, to allow central banks flexibility to meet their specific policy, regulatory and market requirements.

Centralized Architecture

The creation, issuance, and distribution of CBDC are all managed by the central bank. The central bank fully operates CBDC in this model. The public interacts with the central bank directly. The central bank manages KYC, provides the user interface, user authentication and support. DSC^3 supports this model adding security and offline capabilities available with a bearer instrument.

Decentralized Architecture

The central bank creates CBDC using the DSC^3 technology for wholesale use. The private sector partners provide retail payment services using money backed by the intermediary. When payments transact between intermediaries, it is subsequently settled in the wholesale CBDC using the DSC^3 technology.

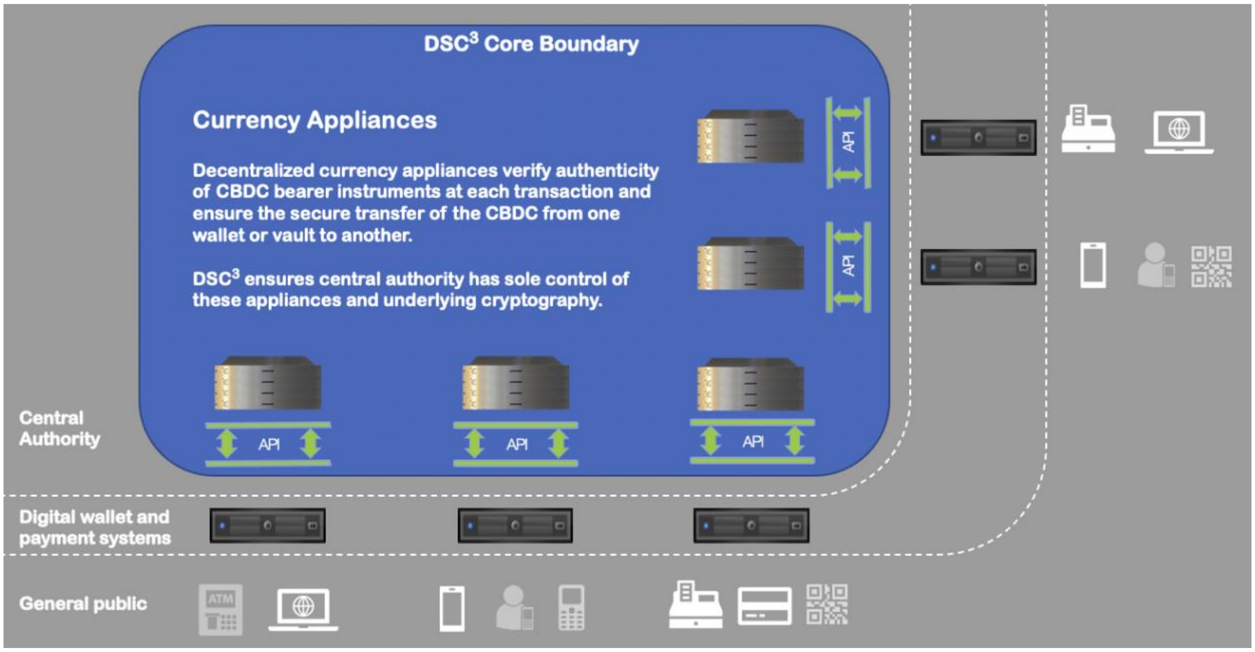
Hybrid (Two-tier) Architecture via a Public-Private Partnership

In deploying CBDC in a hybrid model, central banks continue their role as sole providers of currency to the public. Central banks continue to create and issue currency, while relying on private sector participants, such as commercial banks and mobile money operators, to distribute it to the public in line with the current practice. In this architecture, intermediaries provide the user interaction, authentication, support and KYC, but transactions are enacted in CBDC backed by the central bank.

The DSC^3 technology was specifically designed to leverage existing, and future, payment rails built by private sector participants. DSC^3 de-couples the wallets and payments from the instruments. As such, existing digital wallet and payment systems are able to store and transact in CBDC instruments while retaining their user interfaces and functionalities. The user experience remains the same, and user authentication, support and KYC continue to be the responsibility of the private sector service providers. The central bank is not required to create new payment systems, drive adoption by the public, or be responsible for customer-facing interfaces and support. The private sector will support this approach over approaches that contemplate replacing these financial intermediaries with centralized CBDC systems.

Deployment Architectures

DSC^3 can be implemented as a centralized, decentralized or hybrid solution. The currency appliances can be centralized or decentralized to best meet country-specific operation and policy requirements.



Fully Secure

A true bearer instrument must contain layers of security to prevent counterfeiting. Furthermore, those security layers must be verified locally. Therefore, DSC³ provides layers of cryptography that can be verified in a decentralized manner.

DSC³ achieves this, in part, by creating a symmetric key cryptographic core specific to the central authority and then extends that core throughout the economy to purpose-built appliances. These appliances may be deployed at banks, payment services providers, in the cloud and optionally to appropriately-secured end-user devices, such as phones and smart cards. The appliances in the core secure transactions, and verify the authenticity, of the bearer instruments. The creation and subsequent extension of this core is a critical component of DSC³.

DSC³ also enables the secure distribution and transaction of CBDC within this core. The core remains under the control of the central bank.

Users access this core through authorized payment systems, e-wallet systems and apps provided by banks, mobile operators, fintech and optionally the central authority. These authorized systems interface with the core through a secure, standards-based API. This allows the private sector to innovate, bolstering user functionality and security, while at the same time ensuring the integrity of bearer instruments and their transactions through the central bank-protected core.

Only DSC^3 Technology Meets Central Banks' Operational and Policy Requirements

Avoiding Original Sin

DSC^3 was designed and created specifically for CBDC, in which the central bank provides the trust. This allowed the technology to be built without the inefficiencies, risks and challenges inherent in the original sin of a distributed trust approach, such as blockchain/DLT.

By contrast to DSC^3, blockchain/DLT was created for Bitcoin to eliminate reliance on central banks. Blockchain/DLT attempts to replace trust in a central authority with trust through a community of replicated ledgers and chains of signed transaction records that are later authenticated through a consensus process. These precepts make blockchain/DLT inefficient. While DLT providers have sought various workarounds, the original sin of distributed trust and consensus makes these systems inherently ill-suited for CBDC.

	DSC^3 - Digital Symmetric Core Currency Cryptography	**DLT** - Distributed Ledger Technology/ Blockchain
Technology Origination	Created to enable central banks to issue digital currency	Created to eliminate reliance on central authority (e.g. Bitcoin)
Architecture	Digital bearer instrument; value based	Ledger entries, distributed and replicated
Deployment	Leverages existing financial systems	Replaces existing financial systems
Settlement	Instant and final	Probabilistic convergent
Offline use	Bearer instrument can be stored and transacted offline	Online only
Security	Central bank-controlled symmetric cryptography core with layered security protected in hardware	Participant-managed asymmetric keys, only stored in software
Privacy/ Anonymity	Fully supports the policy choice	Dependent on implementation
Interoper-abilty	Interoperable with all digital wallet and payment systems	Closed system
Scalability	Highly scalable; '000s transactions per second	Limited to a few transactions per second
Efficiency	Minimal energy consumption (standard computational requirements)	Exorbitant energy and power requirements, which can exponentially increase with usage

Providing Final and Instant Settlement

A bearer instrument by definition settles instantly. When the instrument is passed to an individual or organization, they are then the bearer of that instrument. There is no subsequent backend bank settlement, RTGS transfer, consensus settlement or ledger reconciliation needed. A digital bearer instrument, as enabled by DSC³, therefore also settles instantly with finality.

RTGS Role in Wholesale, not Retail, CBDC

RTGS is not involved in retail CBDC transactions. However, for CBDC issuance and for wholesale CBDC, RTGS accounts can be automatically updated through the RTGS integration.

Benefitting from Continuing Private Sector Innovation

DSC³ allows the central bank to continue the public-private partnership. By doing so, the central bank leverages digital wallet and payment systems already being used by the public and paves the way for future innovations by the private sector.

Providing Offline Capability

Natural disasters, remote and rural access, and power and network outages drive the need for CBDC to operate, at least occasionally, in an offline manner. A DSC³-enabled bearer instrument can be stored and transacted offline. DSC³ accomplishes this by extending the central bank security and cryptography to offline devices so that they can verify the authenticity of the bearer instruments during transactions.

At the same time, there is concern that offline transactions can impede AML, CFT and anti-corruption efforts. Therefore, DSC³ technology also allows the central bank to establish value and volume limits for offline transactions.

Only a bearer instrument can be truly settled offline. Architectures such as DLT require subsequent settlement online.

Incorporating the Highest Security Standard

DSC³ is a central bank security technology for implementing CBDC. At its core, it utilizes symmetric key cryptography along with layers of digital security to ensure that the resultant cryptographic objects, i.e. digital bearer instruments in the form of a cryptogram, are protected from counterfeiting. Symmetric key cryptography has many advantages over the asymmetric key cryptography utilized in DLT, especially in currency applications. Symmetric keys are not susceptible to quantum computing attacks. The DSC³ technology establishes a symmetric core cryptography in a hermetically isolated environment at the central bank and then extends the core to currency-specific decentralized hardware security appliances through multichannel threshold cryptography key distribution. This core protects the integrity and authenticity of each CBDC instrument at each use and enables the central bank to issue CBDC as a true digital bearer instrument.

Preserving Anonymity and Privacy

Anonymity and privacy are important for CBDC to truly behave like paper money. Concurrently, CBDC should not be exploitable for money laundering, funding of terrorism and corruption. DSC^3 enables the identity information to be managed by private sector intermediaries, in decentralized and hybrid deployment architectures, without sharing that identity information with the central bank. Accordingly, DSC^3 technology provides the flexibility necessary to support the appropriate and necessary policy choices relative to anonymity and privacy. For example, it is possible to set thresholds based on policy to permit anonymity for small- and low-volume transactions, but with full visibility for the central bank into the largest and most frequent transactions.

Being Fully Interoperable

As DSC^3-enabled CBDC are common universal bearer instruments, they are interoperable with any and all e-wallet or payment systems including those provided by banks, mobile operators and optionally the central bank itself. Additionally, payment from one e-wallet or payment system to another is enabled by this common universal instrument.

Being Highly Scalable

DSC^3 technology makes decentralized transactions possible by securely extending the central bank cryptography to appliances in the field. Appliances are stacked vertically allowing for multiple load-balanced appliances in a single location that achieve thousands of transactions per second. Deploying these appliance stacks at multiple locations provides horizontal scalability. This combination of horizontal and vertical scaling means that the technology can achieve tens of thousands of transactions per second, enough to support the largest economies now and in the future.

Delivering Energy Efficiency

Because DSC^3 was designed specifically with a single central authority in mind, the technology allows for the creation of digital currency stock without mining, settlement without consensus, and a bearer instrument that does not grow in size and complexity with every use. As such it is a highly efficient and energy-friendly ‘green’ technology. When compared to blockchain/DLT solutions, this efficiency translates into hundreds of times greater performance at fractions of a percent of energy use.

Retail, Wholesale and Cross-Border CBDC
DSC³ enables central authorities to create CBDCs. For retail and wholesale use, the central bank is the issuing authority. For cross-border transactions, the issuing authority could also be a regional or multilateral organization, with central banks or sovereign states as members.

Summary

DSC^3 is the only technology that meets the operational and policy requirements of CBDCs. It enables central banks to create and issue a safe, secure and non-counterfeitable CBDC, which fulfills the scale, interoperability, instant settlement and other operational and policy requirements for use as legal tender alongside notes and coins.

About eCurrency

eCurrency was established for the sole purpose of enabling central banks to issue their existing currencies in digital form, thus improving economies and financial inclusion through reduced friction. With eCurrency as a partner, central banks can quickly issue and deploy a central bank digital currency (CBDC) alongside the paper notes and coins.

CBDC greatly reduces the cost of currency, eliminates liquidity risks inherent in payment systems today, enables competing payment platforms to transact in CBDC and to interoperate. A properly architected CBDC solution, as enabled by eCurrency, maintains privacy protections and the role of intermediaries, while also enabling real-time monitoring of the digital economy and enabling both remote currency transactions and local transactions without internet connections.

eCurrency offers both products and services to enable central banks. eCurrency is not a cryptocurrency company nor an issuer of any coins. The technology is built on the belief that currency can only be issued by the central banks. Thus, we provide the technology and services specifically to central banks and specifically for this purpose.

eCurrency's product offering is a CBDC platform built on its innovative DSC^3 technology. This white paper explains the DSC^3 technology.

eCurrency also offers consulting services to central banks wishing to understand what CBDC, possible use cases, benefits, potential pitfalls, legal consideration, and architecture and deployment technical options, as well as Central Banks wishing to build their own CBDC solution.

Please contact info@ecurrency.net for more information on product or service offerings.

https://www.ecurrency.net