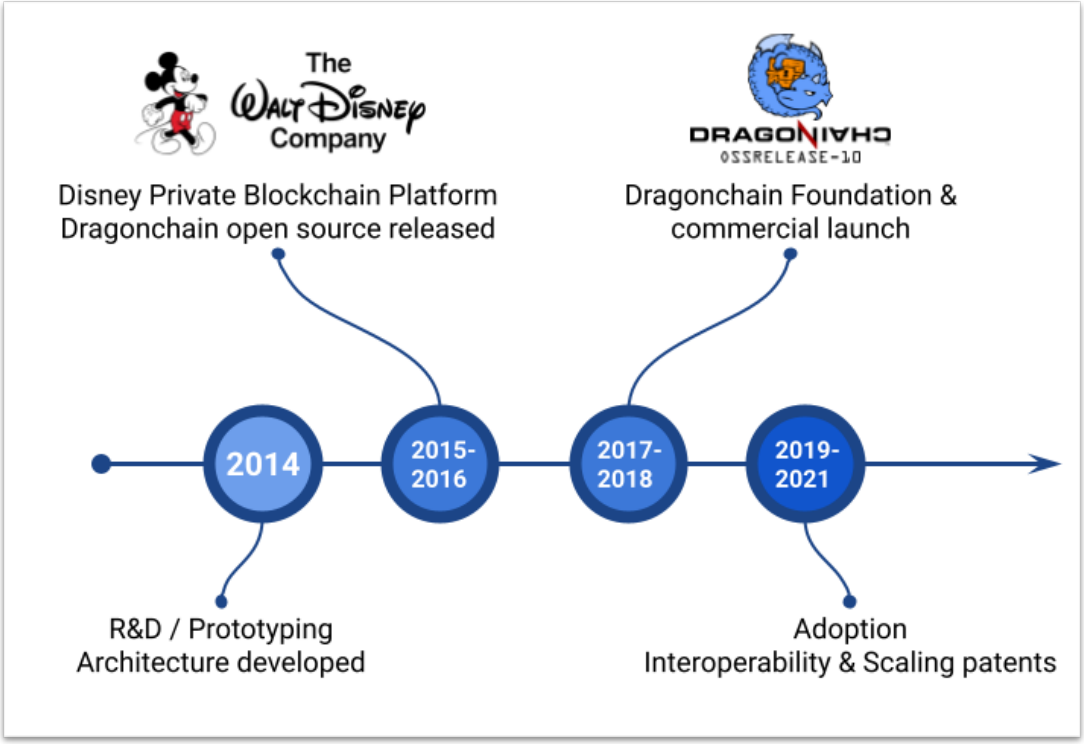
The Dragon Company
15731 NE 8TH ST #7058
Bellevue, WA 98008
dragonchain.com
info@dragonchain.com

Answering the Global CBDC Challenge

A Position Paper from Dragonchain

Date: December 7, 2021
Version: 001

Dragonchain History



The Dragonchain platform was originally created by our team at The Walt Disney Company in 2014. The system focused on solving business problems at an Enterprise scale. In 2016 we released a list of use cases that were explored at Disney to the W3C Blockchain Community Group. Also in 2016, Disney released the platform under an open source license. The original team from Disney commercialized the platform in 2017.

Dragonchain is a hybrid blockchain software development platform, offering secure and fast deployment of blockchain powered business solutions written in any programming language, interoperable with any external blockchain, legacy system, or application. The platform can be hosted in any cloud or on-premises environment.

Dragonchain's architecture considers interoperability and integration as key features. From inception, we had a goal to increase adoption via integration with real business use cases and traditional systems. Dragonchain and its customers have demonstrated extraordinary usability features in many applications, where users do not need to know that the system is backed by a live blockchain.

Proposal

Dragonchain's proposal for the Singapore Central Bank Digital Currency Challenge includes a flexible and Enterprise business focused model for creating and deploying a digital currency providing novel security measures and flexibility for current and future requirements, including unanticipated future requirements.

Dragonchain uniquely offers a CBDC platform with unmatched overall cost efficiency. Our proposal includes, not just physical cost savings by reducing intermediaries, but faster settlement times with near real-time proof versus several days as seen with the current system. Additionally, our system includes an over 90% reduction in energy usage compared to the worldwide non-cash payment system. This all-encompassing cost efficiency is the responsibility of all of us to lead the population towards a more sustainable future.

We will describe here the model from various perspectives. At the end of this document, we address each problem statement.

Blockchain and Architecture

We propose the use of a hybrid and interoperable blockchain architecture which at once protects sensitive information and metadata and leverages multiple public blockchains to prove data integrity.

Dragonchain's patented approach to interoperability provides novel capabilities in the blockchain industry. Among them is measurable proof wherein every transaction is secured to multiple public blockchains. From this action, a measure of proof can be shown for every transaction on the order of millions of US Dollars daily. This measure indicates how much it would cost an attacker to fake transaction data.

> Dragonchain has operational interoperability with Ethereum, Bitcoin, Hyperledger, NEO, Binance, and more.

Supply and Governance

With our model, supply can be controlled of course, but we offer the ability to control supply with advanced governance and transparency features.

Governance features such as token smart contracts, processing versioning, and time-based supply change updates are possible, as well as any capability that can be implemented in software.

Currency Backing

The model we propose would permit any manner of backing including fiat currency, precious metals, or a combination of precious metals and cryptocurrencies. We have further ability to allow for true proof of reserves reporting to maintain value.

This model would allow flexibility in adjusting or modifying the backing components and algorithms or equations in mapping the backing of a CBDC token.

Usability and Speed

Use of the CBDC token is seamless and usable by non-technical users, similar to traditional modern banking payment network features, with the potential to provide advanced traceability with privacy controls and powerful KYC and AML features necessary to a modern banking system.

The hybrid architecture with centralized components provides payment resolution comparable to or exceeding the speed of modern payment systems with near real-time resolution. Inter-bank reconciliation can likewise be automated for quick and efficient processing.

Scalability

Our operational network *Dragon Net* has demonstrated that it can scale beyond the volume of the worldwide Visa payments platform for an extended period of time. Such scalability is necessary for any national digital currency.

Controlled Transparency

Any metadata, tagging, or actions that are necessary for the minting, management, distribution, or flagging of currency transfers or use can be selectively exposed to regulators, banks, or managers with complete proof of action, integrity, and timing.

Clear Communication

A CBDC based on a hybrid blockchain could end the days of potential misinterpretation of financial representative speeches about the state of the economy and planned monetary supply policy. Every word is listened to and parsed, affecting the markets. The ability to use a smart contract with timed exposure allows precise and fair communication to selected parties. An automatic and measurable proof of money supply or scarcity can also be a direct benefit.

Security

Dragonchain provides quantum-safe encryption and signing capabilities, using advanced lab-tested and patented quantum encryption technology. The platform also includes several advanced security features, including multiple levels of network consensus to prevent common blockchain-specific attacks.

Beyond the typical IT security features, the use of blockchain offers many alternatives and advanced capabilities in countering security threats. The Dragonchain team has developed numerous behavior systems algorithms to address security and counter user fraud. Many of these capabilities may interest the panel in pursuit of a well-designed CBDC.

Sustainability

Dragonchain itself is very energy efficient. Not only is our platform infrastructure (including managed nodes), by default, hosted in carbon-neutral facilities, but our verification platform, Dragon Net,

operates at just 0.02 Watts of energy per transaction. More powerful than this minute amount of energy is the security it affords businesses. Unique to Dragonchain is the creation of measurable proof for every individual business transaction based on approximately $4 billion USD worth of network energy per year while using only 0.02 W per transaction. With Dragonchain, CBDCs can use blockchain technology in an efficient and responsible way.

For detailed information on Dragonchain sustainability features please see the Dragonchain Network Energy Efficiency and Sustainability Report.

Use Cases & Concerns

What follows, we address all problem statements from the statements document.[1]

New Functionalities vs Inclusivity

Can a retail CBDC system be embedded with additional functionalities beyond a basic transfer of value without requiring users to use smartphones (or other expensive/complex hardware)? How might this improve the efficiency and effectiveness of Government-to-Person payment programmes in the context of an economy with low levels of digital penetration?

Yes. In the model proposed, additional functionalities, including complex workflows, may be embedded into the system in a very flexible manner, including for the implementation of currently unanticipated requirements. Any such functionality may be executed “behind the scenes” as desired, no matter the user interface pattern. The team has designed systems that would even allow for interchange or purchase without Internet connectivity or a smartphone.

Such capabilities would definitely be helpful in the deployment of the CBDC in an economy with low levels of digital adoption. With the model described, decentralized identity in combination with EMV/chip cards (or even low-tech ID cards) can be used in lieu of a smart device.

Security vs Accessibility

Can the design of a retail CBDC system be highly secure for users (e.g. one that prevents unauthorized uses and illicit transactions) without compromising the ease of use? Would such a system be able to cater to the varied needs of the elderly, minors, and those with disabilities?

Yes, the design is highly secure, allowing the authorities to leverage advanced blockchain capabilities, including the protection of business and user information. The data in our model would also be encrypted at rest and in transit with the most advanced quantum-safe encryption on the market.

Using decentralized identity capabilities, the system would have visibility into all currency movements and can even control the level of public transparency for most or all transactions on the system. This gives enormous power to prevent unauthorized uses and illicit transactions on the

[1] Use cases and concerns sourced from Singapore Central Bank Digital Currency Challenge Problem Statements document <<link>>

system. Normally implemented in business systems, full KYC and AML capabilities are available for direct integration into the CBDC system as well.

These capabilities would not hinder the ease of use for any user, including the elderly, minors, and those with disabilities. In fact, several measures are possible to aid use by such users such as lost wallet recovery, identity protection, accessibility user experience features, and more.

Availability vs Risk of Disputes

Can offline transactions be enabled in areas with no or limited internet connectivity? What safeguards against double-spending and counterfeiting can be embedded to minimize disputes related to offline payments?

Yes. In fact, the team designed a system at Disney with capabilities to continue operational function in the parks in the event that a user is without Internet access.

There are several strategies to counter dispute issues with offline payments. The system can allow configuration to allow a limited amount of offline payment by the user based on the latest balance(s). The system can provide the ability for existing chargebacks in the event of fraud by the user as well. If the user is without connectivity, but the vendor is connected, the system can provide the ability to accept payment between smart devices or between a smart device and a user payment card.

With regards to counterfeiting, in our model, every user or payer would have a digital identity that has decentralization features. This identity has multiple cryptographic signing keys which are tied to the identity. These signing keys prevent anyone from counterfeiting as the user will have known identity and some available system signed proof of prior balance, either on a local chain or the user device itself.

Recoverability vs Anonymity

In the event of theft, damage or loss of a wallet, card or instrument, can a retail CBDC system adequately trace transactions, limit the loss or support the recovery of lost funds without compromising user identity?

Yes, using our proprietary decentralized digital identity platform, Dragonchain's model offers the ability for a "grandma safe" interface to identity and currency recovery. We prefer to not use typical cryptocurrency wallet nomenclature, instead ultimately mapping tokens or currency to a user ID. This allows some of the features of "account" based pools for a user to organize their holdings, but without the risk of key or device loss. These features even include user interfaces much more natural and friendly to the normal, non-technical user than even modern banking interfaces.

Widespread Frictionless Use vs Control

Are there technological features that can be incorporated into a retail CBDC solution to minimise the risk of significant and abrupt outflows from bank deposits to the CBDC, while ensuring that the use of the CBDC is as seamless as possible?

Absolutely. With the hybrid blockchain platform, any transfer can be selectively minimized based upon the established definition of the category, classification, or time-related criteria. This capability happens fully behind the scenes on the blockchain network and will not impair the use of the CBDC in any way.

Personal Data Protection vs System Integrity

Can the retail CBDC solution protect personal and consumer transactions data, while allowing for monitoring, detection and prevention of illicit activities on the network (e.g. money laundering /terrorism financing, fraud, scams and corruption)?

The hybrid architecture of our model for CBDC is instrumental to our ability to answer this question. Our model protects the personal and private information of the user by breaking it down into atomic elements or identity “factors” which can be exposed selectively at will by the user to businesses or other users when necessary or desired. This information can also be exposed to authorities in the case of specific operations or payments, with no risk of public exposure. When certain operations are flagged for potential fraud or improper use, more extensive identity information may be required by the payment network to complete the transaction. All of this information can be tied to the user identity as well if desired.

It should be noted that, unlike a typical blockchain or cryptocurrency, our model uses a hybrid blockchain architecture that exposes no information at all about any transaction unless the system owner (in this case the CBDC authority) wishes that information be exposed. Further, any such disclosure may be to only selected authorities or other users.

This model is capable of compliance with GDPR, CCPA, or any other privacy regulation, and may also allow the system to prove compliance with those regulations.

Dragonchain offers KYC, AML, and anti-fraud system components that can be integrated into the CBDC model to meet requirements.

Expanding Access to Financial Services vs Guarding against Data Monopolies

How can the design of a retail CBDC solution allow participating firms to harness payment data to enable the offering, customising, or improving the pricing of financial services (e.g. credit, insurance) to users, while avoiding the undesirable effects of data monopolies on consumer welfare over time? How might users retain control over use of their data?

Although there are several strategies that could meet this goal, the proposed CBDC model would contain all of the necessary fundamentals to establish an ecosystem that would allow the

monetization of data. Dragonchain has expertise in building data and information markets that can be tuned to a specific system and organization goals which produce value to the community and individual users.

Among them, we provide the ability to establish personal information protection (PIP) smart contracts. These identity-aware smart contracts allow a user to protect their data from any unauthorized access, allow emergency access or access under specific legal precedent. They can also serve as a basis for the monetization of identity obfuscated information for research or analytics purposes. PIP smart contracts can also provide value by notifying the user of access outside of a normal range or purpose.

Coexistence vs Integration Complexity

How can a retail CBDC solution allow financial institutions to distribute CBDCs to the end user in a manner that leverages existing national payment rails such as a country's payment systems, while keeping participation cost competitive at minimal disruption?

The distribution of our CBDC model can follow the pattern of any existing payment rail. As stated elsewhere, even existing payment cards could be integrated into the model. National or regional identity systems can also be leveraged and integrated into the system, mapping the model's decentralized digital identity system to the existing identities of citizens.

Decentralisation vs Accountability

How can a retail CBDC infrastructure be made more resilient to single points of failure? Can concentration risks be minimised through decentralisation? How can we develop a safe, stable and sustainable governance model for such decentralised infrastructure with clear lines of responsibility and accountability?

The CBDC system can be decentralized by the establishment of multiple nodes (effectively, multiple payment blockchains) synchronized to a single CBDC issuance blockchain. Likewise, the model would allow for decentralization of the identity blockchains as well. With this model, and the decentralization of identity information at the user level, the system is more resilient to attack and other natural technology issues.

An advanced governance model for managing the currency itself as well as components of the system infrastructure (e.g. trusted identity authorities, bank enrollment, user registration, vendor access, etc.). Any governance model defined in the real world can be implemented.

Extensibility vs Operational Resilience

Can a retail CBDC infrastructure be flexible yet robust, allowing for computationally intensive use of programmable functions and addition of new capabilities without incurring additional overheads in terms of cost, operational performance or introducing system vulnerabilities?

The Dragonchain platform was purpose-built to be flexible for advanced and complex business use. The architecture itself and its commercial implementation account for such requirements in

Enterprise systems. Every blockchain built on Dragonchain and every smart contract is independently scalable for this reason. Deployable to any cloud provider (e.g. Amazon AWS, Microsoft Azure, Google Cloud), smart contracts can be coded in any executable software programming language. This is highly effective in lowering development costs and lowering security risks, as an organization's existing engineering resources can re-use code or integrate existing IT services into the business logic.

In a scaling event in January 2020, Dragonchain demonstrated the execution of over **260 million** transactions in a 24 hour period on the operational network. This represented a constant volume **greater than the worldwide Visa payment network** for an extended period. During that time, every transaction was fully verified by thousands of interoperable blockchains on the network, as well as the Bitcoin and Ethereum blockchain networks. Even though this was a 6 orders of magnitude increase in traffic, no other blockchain on the Dragonchain network saw any congestion or increase in fees.

Privacy vs Performance

Can a retail CBDC infrastructure incorporate privacy preserving capabilities while remaining high performing, with fast response time, low latency and scalability to support large deployment?

The hybrid architecture of our model for CBDC is instrumental to our ability to answer this question. Our model protects the personal and private information of the user by breaking it down into atomic elements or identity "factors" which can be exposed selectively at will by the user to businesses or other users when necessary or desired. This information can also be exposed to authorities in the case of specific operations or payments, with no risk of public exposure. When certain operations are flagged for potential fraud or improper use, more extensive identity information may be required by the payment network to complete the transaction. All of this information can be tied to the user identity as well if desired.

It should be noted that, unlike a typical blockchain or cryptocurrency, our model uses a hybrid blockchain architecture that exposes no information at all about any transaction unless the system owner (in this case the CBDC authority) wishes that information be exposed. Further, any such disclosure may be to only selected authorities or other users. This model is capable of compliance with GDPR, CCPA, or any other privacy regulation, and may also allow the system to prove compliance with those regulations.

All of this occurs behind the scenes and does not affect response times, latency, or scalability because any processing that might be required to provide identity capabilities are independently scalable and deployable as necessary to aid in processing efficiencies.

See problem statement #10 for further detail about our operational scalability.

Interoperability vs Standardisation

How can interoperability be achieved across different instruments of digital money and across different technologies without a commonly accepted standard?

Dragonchain has a patent on interoperability between blockchains that leverages a RESTful approach for flexibility. This model allows multiple dimensions of interoperability:

1. Token or asset transfer between blockchains (or traditional banking systems)
2. Security - leveraging external blockchains for security
3. Utility - leveraging external blockchains for novel utility (future proof)
4. Tradition systems - leverage the functionality and data of traditional systems

These capabilities stem from our philosophy of “software first” blockchain, that is of a blockchain platform that considers any integration that of a “RESTful” API software integration. This allows the customer (in this case the CBDC authority) to create interoperability as needed very quickly and without complexity. There is no need for an “industry group” standardization initiative. There is no need to even expose sensitive or proprietary information or modeling.

The customer can implement needed capabilities immediately and have the flexibility to refactor as new patterns emerge. Existing code can even be integrated into smart contracts or Enterprise Smart Contract Orchestrations for advanced and flexible use.