Whitepaper

Document Version 2.0
May 2018

CONTENTS

1

Executive Summary

We live in a world of open, connected, global, free communication and information sharing.

1.1 The CENTRE Vision

The open internet -- a global, distributed network of computers that share common open software protocols -- has enabled billions of humans to connect and share information instantly, securely and with zero consumer cost. The implications for the world have been profound, and are still unfolding.

The invention of cryptographic assets and blockchain-based computing and data sharing have ushered in the next major era of the open internet.

Just as HTTPS, SMTP and SIP allowed for free information sharing and communications, crypto assets and blockchain technology will allow humans to exchange value and transact with one another in the same way: instantly, globally, securely and at low cost. An open internet of value exchange can transform and integrate the world more deeply, eventually eliminating artificial economic borders and enabling a more efficient and inclusive global marketplace that connects every person on the planet. The future of the global economy is open, shared, inclusive, far more evenly distributed, and powerful not only for a few chosen gatekeepers, but for all who will connect.

CENTRE was born out of a desire to realize this vision.

CENTRE consists of price-stable crypto assets, network protocols, and business rules which were implemented in early form over the past several years by Circle, where the existing technology supports significant active daily transaction volume. CENTRE plans to create a network scheme to manage the creation, redemption, and flow of these assets under a new organization independent and separate from Circle.

In addition to governing and auditing network membership, CENTRE plans to provide technology to address price volatility and transaction scalability challenges on top of existing public blockchain infrastructure. Specifically, CENTRE plans to provide:

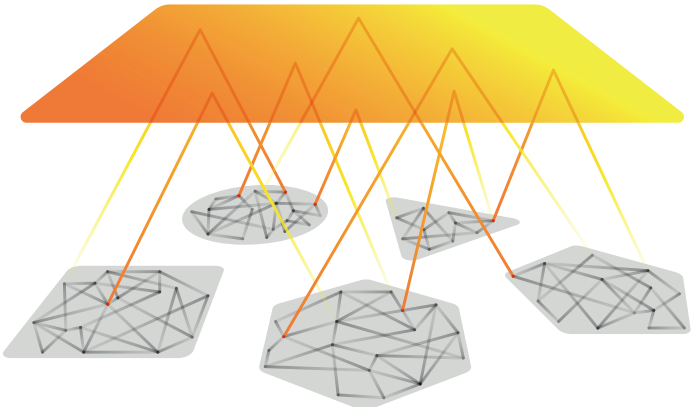
- A mechanism for issuing members to mint and burn/redeem asset-backed fiat tokens, or "stablecoins," to address price volatility;
- Protocols to enable global stablecoin transaction interoperability on public blockchains using state channels for increased throughput and scalability;
- Network membership rules and smart contracts to govern, audit, and manage the licensed network participants that mint, transact, and redeem stablecoins.

While Circle will become a licensed member of the CENTRE network, the network scheme and crypto asset technology will evolve under a new independent entity, an organization which will govern and further develop the CENTRE protocols separately from Circle.

This document describes CENTRE, the problems it is designed to solve, how it is designed to operate, and how it should be managed. To clarify vocabulary, a glossary of key terms is provided as an appendix.

1.2 Global Payment Use Cases

Over the past half-decade, mobile-based digital wallets have emerged all around the world. These applications allow people to make person-to-person and person-to-merchant payments using their mobile phones. These mobile wallets have proliferated in every country, where they are provided by a mixture of banks, mobile carriers, and technology companies. Each purports to make consumer payments more seamless. Yet nearly all of these exist as thin shims of software built on top of the legacy banking and card network payment system. Each one is siloed and proprietary. They live in walled gardens, to borrow from the internet 1.0 era of online services. While we can freely exchange information and content, and freely communicate in open and global ways, money and payments remain locked in the old closed world silos.



CENTRE is designed to provide a solution and new incentives for connecting the world's disparate digital wallets: a network scheme for fiat token stablecoins that will allow money to flow between wallets the same way information moves between web browsers and servers, email between mail services, text messages between SMS providers. CENTRE answers the question "I can instantly text someone who uses a different mobile carrier than I do, and I don't pay money to email someone who uses a different email service than I do, so why can't I use Alipay to pay someone who uses Square, to pay someone who uses Paytm in India, to pay someone who uses Facebook Messenger -- instantly, for free, anywhere in the world?"

Sharing content is free for consumers globally and is interoperable and not locked into specific software

programs or devices; so it will be with value, as money becomes another form of internet content.

Businesses and organizations, either directly by supporting CENTRE-endorsed stablecoins or indirectly by working with merchant acquirers, will be able to support direct payments from compatible digital wallets. Just as an individual can use her web browser to browse the content of a business website, she will similarly be able to use any wallet she chooses to make payments to people and businesses who use other compliant wallets anywhere in any currency instantly and safely.

CENTRE provides solutions for wallets to exchange value using the same or different currencies. A payment from one wallet holding tokenized US Dollars can be sent to another holding Korean Won, with seamless and instant currency exchange. Of course, payments can also be made between wallets in the same currency -- for example, a person using Venmo could pay another person using Square Cash or Circle.[1] CENTRE protocols aim to manage exchange rate rules and contracts across different stablecoin tokens both within and across currencies.

1.3 Crypto Exchange Use Cases

In addition to transactional use cases involving global payments, stablecoins issued by CENTRE network members also aim to address key use cases involving crypto asset exchange risk.

Crypto asset exchanges are online marketplaces in which buyers and sellers come together to trade crypto assets such as bitcoin, ethereum, and others. These crypto assets fluctuate in price according to the market. Tokenized fiat money, such as tokenized US dollars, does not fluctuate in value, but rather remains price-pegged to the value of its underlying backing asset (in this example, the value of one tokenized US dollar is always intended to be priced at one US fiat dollar).

This makes price-stable tokens useful for providing fiat connectivity and for hedging risk on crypto exchanges, particularly on those exchanges that do not provide traditional fiat on- and off-ramps -- so long as the price truly is stable, and so long as there are compliant protections around the minting and redemption of such tokens. A hypothetical investor may choose to protect himself from bitcoin's fluctuating value by trading his bitcoin for US dollar tokens on a supporting exchange, and be certain that the value of those US dollar tokens will not fluctuate.

Stablecoins also allow investment products (such as security and equity tokens) on crypto exchanges to be priced in fiat value rather than in cryptocurrency value. Tokens such as those designed to represent equity ownership, interest in funds, structured debt, loans, dividend rights, and other investment offerings benefit from stable price-pegging for both price and investment return.

Finally and most simply, many exchanges do not offer any direct on- and off-ramp connectivity for fiat bank accounts. On these exchanges,

[1] To the extent that real companies are used in examples contained in this document, it is for illustrative purposes only, and in no way indicates that such companies are participating or will participate in the CENTRE Network.

stablecoins pegged to fiat reserves can provide the needed integration for basic trading activity across multiple token types. Stablecoin gateways, created and maintained by licensed and compliant network members, become third-party fiat service providers for fiat connectivity to these exchanges.

CENTRE provides the smart contracts and the governance that enables issuing network members to mint such stablecoins for customers who may then use them to manage risk exposure on supporting crypto asset exchanges and to invest in tokens that represent investment products.

1.4 Addressing the Challenges of Crypto Assets and Public Blockchains

As underlying enablers of solutions to the aforementioned use cases, blockchain technology and crypto assets promise many benefits: a transparent distributed mechanism for managing trusted updates to shared data among parties who have varying degrees of trust between one another; and a transferable store of value that is not tied to the policy of an issuing sovereign, but rather value based on the processing power, work, stake, and markets that support it.

At the current time, however, existing public blockchain implementations and crypto assets struggle to fulfill the vision in part due to three significant challenges: price stability, transaction throughput, and risks due to the lack of independent governance over standards and network participants (particularly those members offering trade capability and fiat on- and off-ramps).

Firstly, price volatility: In order for global financial interoperability to function reliably and consistently, a price-stable medium of exchange and store of value is desired. Transacting in currencies which fluctuate with extreme volatility creates complexity and fragile settlement contracts, especially when compared to transacting in “tokenized fiat money” or fiat-pegged crypto assets.

CENTRE meets this challenge by providing a stablecoin framework involving “real world” asset reserves. Each stablecoin token corresponds to a real world asset that is reserved by an issuing CENTRE network member and verified and audited by CENTRE.

For example, a network member such as Circle might choose to provide a tokenized dollar and tokenized euro, and back such tokens with a reserved dollar and euro, with CENTRE auditing Circle to ensure compliance and solvency. In theory, another network member might tokenize another asset, such as gold, and similarly back that token with physical gold in reserve. Rules concerning limits, proofs, etc, would be enforced by CENTRE on each issuing network member.

A second challenge with current technology is blockchain transaction throughput. Current public blockchain implementations do not support high-volume performance, as every transaction is written to an underlying ledger and printing new blocks to such ledgers currently involves relatively high latency.

CENTRE addresses this challenge by providing a protocol for wallets to transact at higher velocity using state channels. The initial and final settlement states, such as account balances, of an interaction between two participating members is written to the relevant underlying blockchain, but intervening transactions are not written to the underlying chain and thus executed at the speed of the internet. This allows for payments in tokenized fiat currencies but with the speed, security, and auditability of blockchains.

A third challenge with existing implementations is the lack of independent governance over stablecoin providers. An issuing institution must be independently audited for solvency and security, otherwise the underlying asset cannot be independently verified, and the price stability becomes tenuous.

This issue has arisen with previous attempts at fiat-asset-backed stablecoins in production.

CENTRE addresses this issue through separation of the CENTRE organization from its issuing network members. CENTRE itself is not an issuing member or financial institution, but a network scheme manager and technology provider. CENTRE enforces compliance with network rules around membership and behavior in order to ensure stability, accountability, and consumer protection.

1.5 Service Providers: Compliance, Identity, Fraud, Risk

CENTRE plans to offer a service provider mechanism to support trust and identity decisions, rules for payment settlement and reversals, and the secure exchange of KYC/AML-related information to meet compliance obligations.

Providers of services for fraud detection, risk assessment, identity management, AML monitoring, and other services on the network will be able to implement the CENTRE Service Provider interface in order to participate in the network and earn fees for the services they provide to transacting network members.

For example, when different wallet providers connect to one another using CENTRE, it is important that these participating wallets meet applicable compliance and regulatory requirements, which include relevant KYC and AML obligations. CENTRE's service provider interface will allow providers to supply features that support KYC and AML information exchange while leveraging cryptography to secure PII and reduce the risk of PII leakage common to existing legacy payment networks.

1.6 Governance and the CENTRE Organization

CENTRE software implementation is expected to be managed by a new independent organization and entity created for this purpose. This organization aims to provide the support, governance, and ongoing R&D for the CENTRE open source software project.

The organization also expects to offer optional certification to improve trust in stablecoin-issuing members and wallet implementations, certify regulatory compliance of members, audit asset backing, and provide support and network operations to ensure continuous operation of network nodes.

The organization also aims to pursue business development and support programs to usher new members into the network and commit engineering and support resources to work on the underlying crypto infrastructure on which CENTRE is built.

Network governance is expected to include distributed consensus and voting mechanisms that leverage a forthcoming CENTRE-specific token, separate from fiat tokens, that is designed to facilitate such network decision-making.

2

Technology and Network

CENTRE enables crypto exchanges and wallets around the world to interoperate.

By exchanging price-stable tokenized value using a standard protocol across blockchains and fiat rails, and it enables those wallets to leverage services for compliance, identity, and risk management via well-defined interfaces for service providers which plug into the network. The technology provided by CENTRE supports tokenized fiat money through asset-backed stablecoins, and enables high transaction throughput by employing optional state channel implementations.

This section describes this technology in more detail.

2.1 Stablecoin Minting and Redemption Sequences

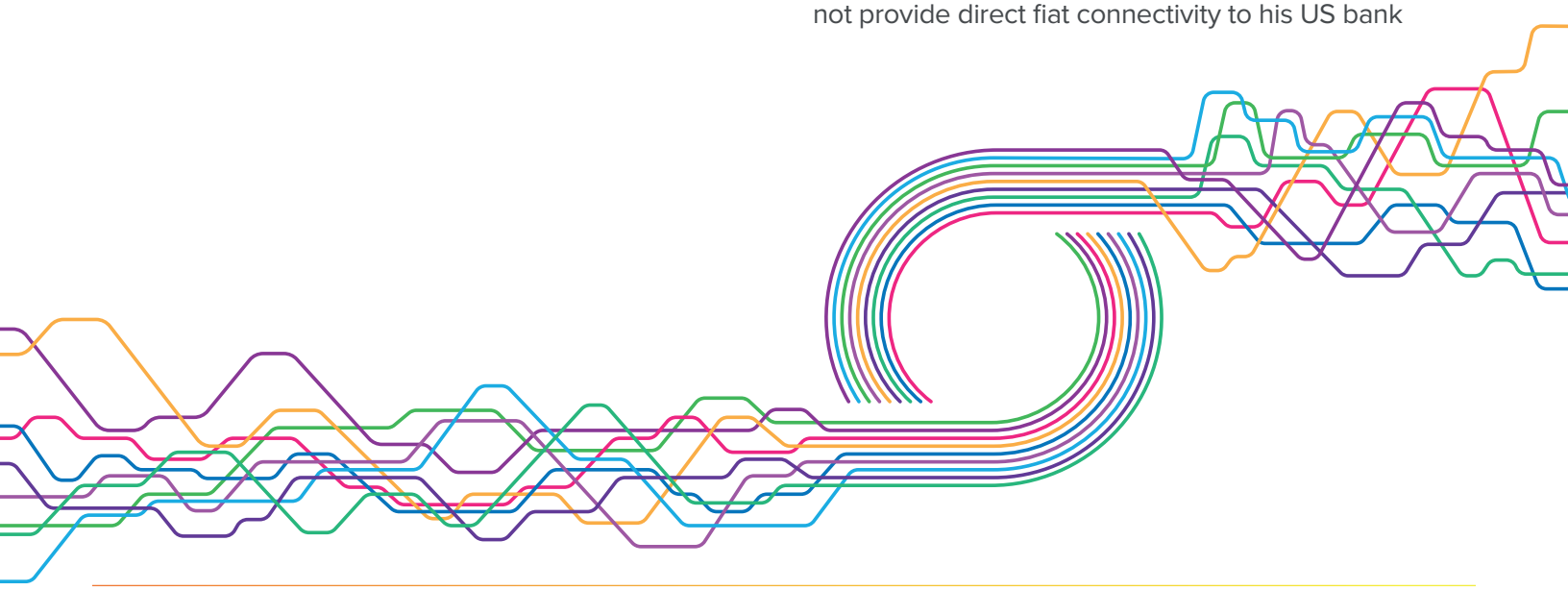
CENTRE contracts manage the minting and the redemption/burning of stablecoins, which can be used for both the exchange and wallet interoperability use cases.

Customers who on-board through a stablecoin on-ramp, such as a web application created and maintained by a licensed CENTRE token-issuing member, can transfer fiat funds into that CENTRE issuer's account. The issuer then executes a series of commands with the CENTRE network to verify, mint, and validate fiat tokens pegged to the value of those deposited funds. The customer can then transfer those tokens elsewhere in order to use them.

Redemption follows the reverse sequence: fiat tokens are burned when a customer visits an off-ramp such as a web application maintained by a licensed CENTRE issuing member. Upon successful verification and validation, funds from underlying fiat reserves would be transferred to the customer's external bank.

Consider this example:

David is a trader on crypto exchanges, and he would like to purchase crypto assets on exchanges that do not provide direct fiat connectivity to his US bank



account, and he would also like to hedge his risk exposure to the volatility of crypto assets on those exchanges by maintaining some of his holdings in the form of US dollar tokens that do not fluctuate in value.

David visits a web application created and maintained by Circle (David could also visit a web application of any other token-issuing member of CENTRE, but in this example he chooses Circle). David signs up for a customer account, which requires satisfaction of KYC requirements, and then begins the deposit process in order to turn his fiat dollars into tokenized US dollars. The deposit process requires David to transfer US dollars from his bank account into the Circle account. David has a limit on the amount of funds he may transfer (and thus the number of US dollar tokens he may acquire) in a given time period.

Once David's transfer settles, Circle interacts with the CENTRE network to execute the process required to transmit US dollar tokens to David. These tokens may be taken from existing reserves from Circle's buffer of pre-funded fiat assets to increase the speed of the process; if no such reserves are available, then Circle uses the CENTRE protocols to mint new tokens. David then receives the tokens, and the value of those tokens directly corresponds to the value of the funds he deposited into the system.

David may transfer the US dollar tokens to an address in a wallet or on an exchange so that he may use them to support his trading activity. CENTRE maintains a blacklist of forbidden addresses in order to protect David and other network participants from known bad actors and to support regulatory compliance.

When David -- or one of David's counterparties who may have acquired some of the US dollar tokens -- wishes to redeem the tokens and withdraw the underlying fiat dollars, then the process is executed in reverse: David returns to the issuing web application (Circle in this example), deposits the tokens into a wallet address made available to his account on that web application, and Circle executes a transfer of underlying dollar reserves into David's registered bank account.

The tokens are withdrawn from circulation, and either placed in reserve to service future requests, or else burned/destroyed if the value of those tokens surpasses the prefunded fiat buffer maintained by Circle. This process is subject to authentication and authorization, verification, validation, and compliance similarly to the deposit sequence.

Note that access to stablecoins need not be in a dedicated web application as in this example, but could also occur in a wallet, exchange, banking portal, or other product created by a licensed, compliant, token-issuing member of the CENTRE network.

2.2 Wallet-to-Wallet Transaction Sequence

CENTRE can facilitate compliant, reliable, safe, high-speed transfers between individuals who use different wallet apps in shared as well as different currencies without requiring private business development negotiations or using private networks.

Consider this hypothetical example which crosses apps as well as currencies:

Mobile wallets Paytm in India and Vipps in the Nordics could participate in the CENTRE network and allow their customers to transfer rupees and kronor even though the wallets themselves do not integrate with one another directly and even though they do not share common fiat currencies.

Behind the scenes, the Paytm wallet in this example could use CENTRE to issue price-stable INR tokens and publish exchange rates between that tokenized rupee and other tokenized fiat currencies. Similarly, Vipps could issue price stable kronor NOK tokens and publish an exchange rate between that stablecoin and other fiat tokens, such as a kronor-to-rupee exchange rate.

Alice is a customer of Vipps in Norway, and wishes to send money from her Vipps wallet to Bob in India, who uses Paytm as his wallet. When Alice begins her transaction, Vipps refers to its exchange rate between the kronor and rupee stablecoin tokens; if Alice accepts this rate, then the transaction will proceed. If Vipps had not had an exchange rate between these coins but Paytm did, then Vipps could also have surfaced that exchange rate instead, and sent kronor to Paytm, which in turn would have converted it to rupees using that exchange rate.

Next, Vipps and Paytm may perform any required identity checks, compliance requests, or risk assessments as part of the transaction approval process. These operations may optionally call on service providers who provide such offerings to the CENTRE network in exchange for fees paid in tokens.

For example, to continue the sequence in the Vipps-Paytm narrative: Vipps may have configured its CENTRE node to execute its own internal identity checks, while Paytm may have configured its node to use a third party service which provides an identity verification service. Paytm and the company agreed to a price for this service, and Paytm can pay that price on a per API call basis by utilizing state channels and stablecoin token balances. Other service providers such as those involving fraud detection or other risk assessment may similarly be plugged into the sequence.

If any of the checks fail in this example, Paytm or Vipps can abort the transaction before transferring any value.

If the checks all pass, then the value can be transferred atomically through the use of chained state channels.

To complete this example: Vipps would then update Alice's app balance to deduct the appropriate kronor, and Bob would see his Paytm rupee balance increased correspondingly. Vipps and Paytm settle asynchronously for a batch of their customers when the state channel is closed.

2.3 Merchant Payment Sequence

CENTRE also facilitates compliant, reliable, safe, high-speed transfers between an individual who uses a consumer wallet app and a merchant who uses a point of sale app. The consumer wallet and the merchant point of sale software interact using the CENTRE standard. This is analogous to a web browser accessing a remote website using the HTTP protocol without resorting to use of a closed private network.

Consider the following cross-currency example:

Carol has a WeChat wallet holding a Chinese RMB stablecoin balance. She is traveling in the United States and wishes to buy a sandwich from Dave, who is a merchant who uses a Square mobile point of sale app that accepts US dollar payments.

In this example, Dave's Square point of sale app does not accept RMB or WeChat payments, and WeChat has no direct integration with Square. However, the payment could work seamlessly between WeChat and Square, without a custom private integration between them, if Square and WeChat supported the CENTRE standard protocols.

In this example, WeChat and Square could facilitate a payment between their apps for Carol and Dave by agreeing upon an exchange rate between the RMB and USD tokens that each accepts for settlement. WeChat's CENTRE node could surface an exchange rate from RMB tokens to USD tokens, and execute a purchase of USD tokens using RMB tokens for Carol. The transfer would then involve sending the USD tokens to Square. As in the person-to-person

sequence above, the same service providers (for compliance, risk, identity, etc.) may also be called upon as part of the transaction approval logic.

Naturally, no exchange between stablecoin tokens would be required if the node owners (WeChat and Square in this hypothetical example) agreed upon another token for settlement. For example, if Square accepted RMB stablecoin tokens directly, then that token could be used for the same transaction, and the amount of RMB transferred would be dictated by Square's RMB-USD exchange rate rather than WeChat's.

More simply, consider this same-currency wallet interoperability example:

Charlie has a mobile wallet app which holds a balance in US dollars. He is in line behind Carol at Dave's sandwich shop and when it is his turn, Charlie uses his mobile wallet to pay into Dave's Square point of sale app.

Even though Charlie and Dave have apps by competing companies, these apps can interoperate because both support transfers of US dollar tokens. Using CENTRE, the apps achieve interoperability and can seamlessly facilitate a payment based on supporting a common open protocol.

2.4 Crypto Asset Cross-Blockchain Sequence

CENTRE also plans to enable transactions across blockchains and crypto assets, and can connect such crypto assets to fiat-based accounts and wallets.

For example:

Frank holds a bitcoin balance in Ledger, a hardware-based wallet. If his wallet supports CENTRE, he can open a state channel with other CENTRE nodes for the purpose of routing bitcoin-based transactions and transfers. For example, if the Poloniex crypto exchange supported CENTRE, then Frank could maintain a state channel with Poloniex.

If Frank wishes to use his bitcoin wallet to send money to Charlie, who as in the example above maintains a US dollar balance in his mobile wallet, then Frank can use his bitcoin wallet to do so since both Frank's and Charlie's wallets interoperate via CENTRE, even though Frank does not hold any US dollar tokens.

Frank's connection is to Poloniex, which in this example maintains a CENTRE node that supports US dollar stablecoin tokens and BTC. Charlie's mobile wallet supports US dollar stablecoin tokens, but not BTC. The Poloniex node publishes its exchange rate between BTC and US dollar tokens (i.e., the current US dollar value of bitcoin). That rate is displayed to Frank, and if he accepts, the transaction can proceed.

Then, as in earlier examples, token-consuming service providers may enter the sequence to offer compliance, fraud, identity, risk, or other services to Frank or Charlie as required by the products they are using.

The transaction in this example executes through state channels so Frank can be sure that Charlie received the transfer even though it crosses blockchains from bitcoin to US dollar tokens (on the ethereum chain).

2.5 Existing Technology

CENTRE plans to bootstrap development of its implementation by utilizing intellectual property contributions as well as perpetual licensing, as appropriate, from Circle, where an early form of these kinds of protocols is in production today.

The protocols, APIs, and business rules defining interactions between network participants represent a level of abstraction above any particular implementation of those rules. Existing web content protocols illustrate this relationship: HTTP defines a vocabulary for requesting an HTML page, but does not require any specific technical implementation, operating system, or programming language for that

vocabulary. Similarly, the CENTRE protocols define a vocabulary and business rules but do not require a specific distributed ledger, language, runtime, or operating system for implementing those rules.

The initial implementation of the CENTRE protocol exists at Circle, where it was built over the past several years and has supported significant transaction volume in production across multiple fiat and crypto currencies. CENTRE plans to implement the protocols on top of Ethereum as a series of smart contracts and ERC20 tokens. CENTRE plans to leverage the existing implementation to accelerate development of a new implementation of the protocol.

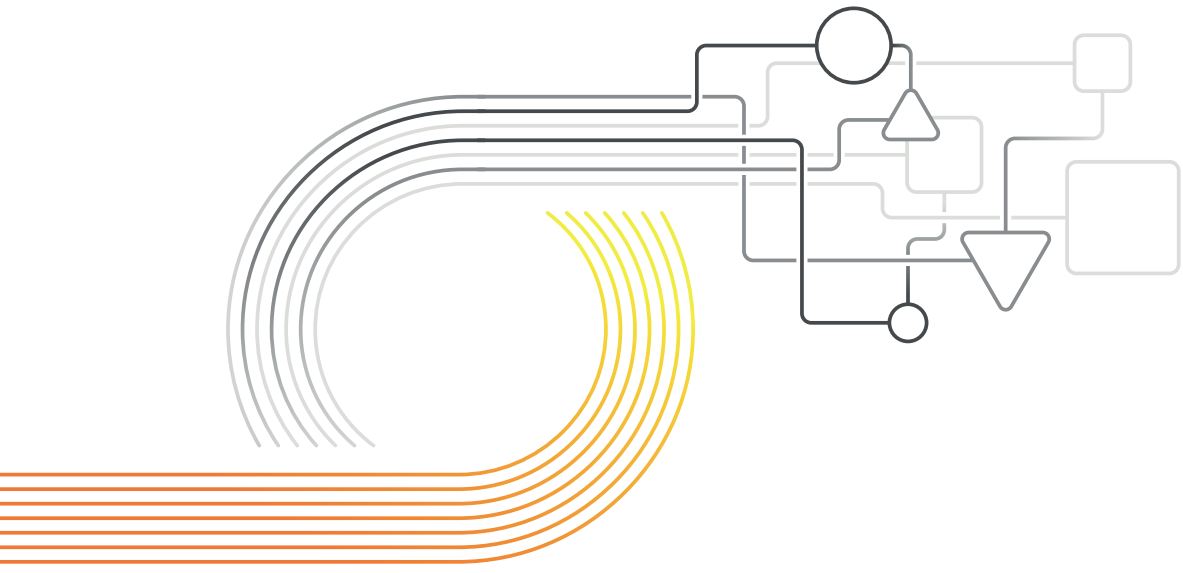
2.6 CENTRE Nodes

CENTRE intends to evolve the existing protocol implementation from Circle into a new software package that defines a CENTRE "node." Initially, a node is expected to consist of (1) a collection of smart contracts deployed on Ethereum, and (2) code that knows how to interact with Ethereum and those smart contracts. The smart contracts include fiat token contracts (implemented as ERC20 tokens), and state channel contracts as an option for quickly transfering value on the network.

Wallet account providers, financial institutions, software companies and other participants will begin to join the network by hosting one or more CENTRE nodes.

A node is intended to provide a network participant the ability to:

- Issue new fiat tokens, such as tokens to represent US dollars, Euros, RMB, or other currency that a node owner can settle;
- Configure which fiat tokens to accept, or delegate the decision to a third party;
- Publish rates for exchanging fiat tokens;
- Configure trust levels as rules dictating which other node owners and network participants to trust, or to delegate the decision to a third party such as a payment network;
- Exchange metadata about a transaction before any value is transferred and deny/approve transactions based on the metadata;
- Ensure that value transfers execute atomically and quickly through the use of state channels.



While the initial CENTRE node implementation (unlike the original Circle implementation of the protocols) is intended to operate on Ethereum, the use of state channels allows the network to be implemented on multiple blockchains and perform atomic transfers across blockchains. Thus in the future, participants would not necessarily be limited to Ethereum and new blockchains could be added to the network.

2.7 Technology Implementation Notes

2.7.1 STABLECOIN DESIGN

Four general approaches exist for a price-stable token strategy:

- Fiat-collateralized: Fiat assets in reserves collateralize tokens and thus provide price stability by pegging token value to reserved fiat value;
- Crypto-collateralized: Crypto assets in reserves collateralize tokens and provide price stability pegged to the value of those reserved crypto assets;
- Algorithmic non-collateralized: Software economic models aim to provide price stability without relying on underlying collateralized assets;
- Hybrid: A blend of the three basic approaches above.

CENTRE aims to provide the first: a fiat-collateralized approach. One unit of tokenized fiat currency is backed by one unit of reserved fiat. More so than the other approaches to stablecoin development, the fiat-collateralized approach requires meeting firm traditional regulatory requirements, requires issuing members to have strong auditable reserve capability for traditional backing assets (such as fiat banking relationships), and provides less decentralization -- and it is also currently the most robust approach in terms of price stability.

CENTRE addresses the centralization tradeoff by envisioning a network of multiple token-issuing members, thus providing multiple reserves and liquidity sources for network users rather than presenting a single collateralization gateway point of failure. This approach is distributed, though it does not purport to be -- or aim to be -- entirely decentralized.

Further, CENTRE itself enforces membership requirements related to audits/solvency, licensing and compliance, and capitalization thresholds and limits. This eliminates reliance on any one issuing member to provide these controls. CENTRE, as a technology provider and network scheme, provides such governance and is incentivized to maintain compliance and solvency from all its licensed issuing members.

The interaction between a token-issuing member and the CENTRE network is codified in a series of smart contracts created and maintained by CENTRE, along with a protocol and network policies to facilitate such interactions. CENTRE does not maintain fiat asset reserves itself, and CENTRE is a not a financial institution; likewise, issuing network members do not control the fiat token contracts, but rather leverage them as they interact with the CENTRE network. New issuing members must on-board into the CENTRE network, and new fiat tokens join the scheme through that process.

The contracts created and maintained by CENTRE are intended to be open source software, subject to ongoing global peer review as well as formal security review, and evolved through internal CENTRE engineering development as well as through collaboration with open source developers around the world.

2.7.2 STATE CHANNEL TRANSACTION MANAGEMENT

To transfer tokens at higher throughput rates, as an option in addition to direct usage of Ethereum, CENTRE transactions can utilize the state channel pattern. Using this option, nodes exchange balance information in the form of tokens transferred

in state channels. This section describes how state channels operate at a conceptual level.

State channels are a way for two or more participants to update shared state between them securely without executing transactions on a distributed ledger, except for creating and finalizing the state channel on the ledger. State channels are similar to payment channels, but state channels can manage multiple types of shared state in addition to payment data.

To create a state channel, the participants agree to an initial state and execute transactions on an underlying distributed ledger in order to lock in that state. Subsequent updates can be executed without executing any transactions on the ledger. Each update is simply a new state, and each participant cryptographically signs the new state if it is valid. When the participants wish to close the channel, they can each execute a transaction saying they agree to the final state.

For example, imagine Alice and Bob wish to create a state channel for payments. They each lock 100 US dollar tokens into a state channel contract on the ledger, for an initial state as follows:

```
{
   alice_balance: 100,
   bob_balance: 100,
   sequence: 0
}
```

Thereafter, Alice and Bob can perform updates by communicating between themselves: When Alice sends 50 euro tokens to Bob, she does so by generating a new state, cryptographically signing it, and sending it to Bob. If Bob agrees to the new state, he signs it and sends it back to Alice. The new state between them looks as follows:

```
{
   alice_balance: 50,
   bob_balance: 150,
   sequence: 1
}
```

If Bob then sends 25 tokens back to Alice, he generates a new state, signs it, sends it back to Alice, who signs it, producing another new state of:

```
{
   alice_balance: 75,
   bob_balance: 125,
   sequence: 2
}
```

When Alice and Bob wish to settle these payments, they do so by closing the channel. Alice executes a transaction reporting that she agrees to the final state; Bob agrees, so he also executes a transaction agreeing to the final state. Since they agreed, the state channel contract then sends the funds to each participant based on the final state it was given. In this example, Alice receives 75 euro tokens and Bob receives 125. The net change of 25 tokens from Alice to Bob is committed to the ledger. Any intermediate state changes will never be committed to the ledger.

When one party wishes to close a channel, the state channel contract does not close immediately on demand. Instead, a challenge period commences in which the other participants have a period of time to either:

- Agree, in which case the channel is closed and the changes are committed immediately;
- Dispute the final state by submitting a state signed by all parties with a higher sequence number; or
- Do nothing, which will constitute agreement once the challenge period expires.

Imagine the scenario in which Bob wished to "cheat" by broadcasting the earlier state which assigned him 150 tokens instead of 125 tokens. That state was also signed by both Bob and Alice, so it is in some sense valid.

In this example, if Alice disagrees with the final state that Bob submits, then she would have a chance to submit the later state (sequence 2), which was also signed by both parties; in this example, that would supersede Bob's final state. Bob could then either agree or do nothing. He would be unable to dispute since he does not have a later state signed by both parties. This means that no participant can prevent another participant from closing the channel, and no one should be able to close the channel except with the legitimate final state.

Further, the reputational impact of any party attempting to cheat the network is recorded and subsequently visible to other participants.

2.7.3 CHAINING STATE CHANNELS

State channels can be chained to enable payments to additional parties. If Alice wishes to pay Carol, and both Alice and Carol have a channel with Bob but not with each other directly, then the transfer from Alice to Carol can flow through Bob and then on to Carol without requiring Alice and Carol to open a direct channel. To chain state channels in this manner, the system must enforce assurance that when Alice pays Bob, that Bob will in turn pay Carol and that Bob cannot retain the funds himself.

This is accomplished through the use of a hashed time locked contract (HTLC), which makes executing the chained payment as secure as executing it through a normal direct state channel. A chain of states is established in which the funds will be released if and when the recipient can produce a secret. The final recipient is then given the secret, which they pass up the chain, and everybody in the chain can use the secret to claim the funds.

In this example, Alice gives Bob a new state that essentially states: "if you can produce the preimage that will produce this hash, then you can receive the funds." Bob then produces a similar state with Carol. Alice then gives Carol the preimage. Carol uses that preimage to retrieve the funds from Bob, and then Bob uses that to retrieve the funds from Alice. Since the HTLC is enforced by the state channel, if one party attempts to steal the funds then the other party can broadcast a transaction with the HTLC and the preimage, which will direct the funds to them.

2.7.4 NODE MODULES

Interaction between internal node subsystems occurs through well-defined modules and API interfaces to

make replacing or extending parts of a CENTRE node as easy as possible. Different network participants may wish to employ different internal technologies (such as a relational database, key management, PII storage, etc.), so it is critical that CENTRE has a pluggable means of supporting those requirements.

A preliminary, non-inclusive list of planned modules is as follows:

Distributed Ledger and Smart Contract Modules
A module and interface to manage and employ a distributed ledger and the necessary associated smart contracts. Initially CENTRE provides a module that implements a module and interface for Ethereum. This smart contract module includes: Code that understands how to talk to an Ethereum node, smart contracts for tokens and state channels to be deployed as needed, and code to interact with the included smart contracts to enable value transfers.

Routing Modules
A module to determine routing for negotiating transfers.

CENTRE Protocol Module
A module to implement APIs that CENTRE nodes use to communicate with one another.

CENTRE Management Module
A module implementing APIs that node owners employ to control and administer a CENTRE node. This includes support for initiating a value transfer, deploying a new token, and updating trust parameters for nodes and tokens, among other features.

Exchange Rate Module
A module to manage what rates a node offers when trading between assets.

Key Management Module
Modules to handle securely storing and retrieving cryptographic keys for signing transactions and executing state updates.

Identity, Risk, PII, Compliance, Authorization, and Service Modules
Extensible modules employed for identity and account management, KYC/AML compliance, secure storage, authentication and authorization, risk scoring, and other services.

3

The CENTRE Team and Organization

While initially a wholly owned subsidiary of Circle, it is proposed that CENTRE operations and team members are to be transferred to the CENTRE organization, a new entity which is to be created in the coming months. The CENTRE organization expects to operate independently, with entirely separate dedicated working capital, employees and technology development. Circle expects to act merely as a founding member and source of the original technology and IP, and as a production user of CENTRE, as further detailed below.

3.1 The CENTRE Organization

The CENTRE organization aims to satisfy four key objectives:

- Provide R&D capability, support and maintenance of the CENTRE open source software project. This includes managing the open source code repository and facilitating and supporting third party developer engagement, evangelism and code contributions.
- Provide the business development, governance and compliance functions for the CENTRE Network, including business development required to usher new nodes into the network for consumer wallets, merchants, payment acquirers, and others.
- Provide optional certification testing, trust authority services, compliance reviews, and due diligence programs to allow node owners to opt into proving, maintaining, and broadcasting high degrees of trust to satisfy legal obligations and to increase reputation and presence among other network participants.
- Contribute engineering and support services to the underlying distributed ledger infrastructure (such as Ethereum) on top of which CENTRE operates.

This vision sees CENTRE growing to become a significant global organization with business and operational professionals in all major markets around the world, a global compliance function that is working closely with digital wallets in every region, and a significant R&D function that continues to build and improve the CENTRE software protocols. Software contributors are expected to include a growing community of third party developers from CENTRE network members as well as independent developers around the world.

3.2 Circle Corporate Background

As the creators of the core CENTRE technology and IP, and as the network's founding member, Circle's broader background and leadership is critical to CENTRE's launch and initial development.

3.2.1 LEADERSHIP, INVESTORS, AND DIRECTORS

Circle's senior management team brings highly seasoned leaders with decades of success in leading companies in the Internet technology, online services and banking industries. Cofounders Jeremy Allaire and Sean Neville have built multiple global public companies with products and platforms that have helped to transform software development, web content, online media, and core Internet infrastructure.

Sean and Jeremy are joined by seasoned executives and a broad leadership team coming from companies including Goldman Sachs, Amazon, Square, Google, AirBnB, Expedia, eBay and Adobe, among others. A unique combination of top Internet technologists and operators familiar with the complexities and risks of global finance, the management team represents one of the most experienced and talented firms in the global Internet Finance industry.

Circle is backed by by leading venture and strategic investors including IDG Capital, one of the largest venture capital firms in China and early investor in Tencent, Baidu and CreditEase; Breyer Capital, founded by Jim Breyer, one of the leading VCs in the world and first investor in Facebook; General Catalyst Partners, major investors in Snap, Airbnb, Stripe, and Kayak. Strategic investors

include Goldman Sachs, CICC Alpha, Baidu, WanXiang, CreditEase and EverBright Bank.

Circle's board of directors includes, in addition to Jeremy and Sean, veteran venture investors Jim Breyer, Quan Zhou and David Orfao, who have helped to build some of the most significant consumer, Internet, and technology companies in the United States and China. Independent Director Raj Date brings decades of experience in consumer finance as a senior executive at Capital One and Deutsche Bank, and he was recruited by US Secretary of the Treasury Timothy Geithner and Senator Elizabeth Warren to spearhead a new regulatory agency for consumer financial protection. Independent Director M. Michele Burns is a leading global financial executive who was CFO of Delta Airlines, Mercer and Marsh McClennan, and has served on the board of directors of Walmart, Cisco, Goldman Sachs (where she chairs the risk committee) and Inbev. Independent director Alex Norstrom is a Spotify executive who oversees the Spotify subscription business unit and brings a strong background in growth and marketing in the consumer internet space.

3.2.2 CIRCLE PRODUCTS AS CATALYSTS FOR CENTRE ADOPTION

With billions of dollars in transaction volume, millions of customers, and a growing global footprint, Circle's products can be major catalysts for broader CENTRE Network adoption.

Circle currently operates four major product lines: Circle Pay, Circle Trade, Circle Invest, and Poloniex.

Circle Pay is a global social payment app that enables customers to make payments instantly and without fees, including instant payments that cross currencies and borders. Circle Pay combines open, cross-currency transactions with delightful social messaging behaviors -- conversations, media and payments.

Circle Pay was built from the ground up on blockchain technology and specifically on the technology behind CENTRE. The company envisions money and value transcending walled gardens to become more inclusive and globe-spanning, nearly instant, secure, and enabling new forms of growth and innovation for businesses and individuals. Charging a toll for payments will disappear, opening up enormous opportunities for global value exchange, including bringing several billion people into the global digital economy.

Circle Trade operates the company's crypto asset trading business, which today is one of the largest market makers and OTC liquidity providers in the world. Circle Trade directly trades over $2B per month in the marketplace, provides daily liquidity to large natural buyers and sellers of crypto, trades at high values (minimum of $500k USD), and acts as a liquidity provider and market maker on all mature crypto asset exchanges.

Circle Invest, first released in the US in spring of 2018, is a mobile app that surfaces Circle Trade's capabilities to retail consumers. Circle Invest simplifies crypto asset investment particularly for those new to the space. Circle Invest has zero commission fees, instant funds access, and a minimum of $1 USD. Circle Invest will grow its features and expand global market availability over the course of 2018.

Poloniex is one of the world's largest crypto asset exchanges. Circle envisions Poloniex evolving into a robust multi-sided distributed marketplace that can host tokens which represent everything of value: physical goods, fundraising and equity, real estate, creative productions such as works of art,

music and literature, service leases and time-based rentals, credit, futures, and more. Circle believes that the contractual rules around exchange for anything and everything will become increasingly represented in distributed global software, rely on inconvertible distributed shared memory in the form of distributed ledgers, and benefit from the services of global multidimensional marketplaces.

3.2.3 REGULATORY AND LICENSING PORTFOLIO

The advent of cryptocurrency and blockchain technology represents the most significant technology breakthrough since the emergence of the commercial internet, and Circle has believed it is crucial to build strong relationships with governments who are seeking to understand the technology and ensure that markets can adopt it while also addressing key risks to society, the economy, and consumers. Because of this, Circle has focused on deep and high-quality engagement with regulators since its inception, and holds the broadest licensing of any crypto company in the world.

Circle is a registered Money Services Business (MSB) with the Financial Crimes Enforcement Network (FinCEN) of the US Treasury Department and holds money transmission (or equivalent) licenses in 48 US states and territories. Circle is the first and currently one of only four companies to have been granted a BitLicense from New York. Circle also holds an E-Money Issuer license from the Financial Conduct Authority in the UK. These licenses enable the company to offer fiat and crypto asset storage, currency exchange, and payment services in the United States, UK, and European Union.

3.2.4 TECHNOLOGY AND IP CONTRIBUTIONS

Circle is contributing core technology and IP to the CENTRE organization. This IP is the result of several years of technology development at Circle to support the consumer social payments and crypto asset trading businesses. Circle's pioneering work in building seamless consumer payment experiences and using fiat currency on top of underlying blockchain settlement and integration layers are core to CENTRE. Other technology innovations include systems and services for layering KYC and AML risk decisions into payment networks and transactions, and systems for providing instant liquidity and conversion between fiat and crypto assets.

3.3 Organizational Structure and Advisors

The CENTRE organization will be seeded with several key Circle employees who anticipate moving from Circle into CENTRE. This talent includes individuals in engineering, operations, business development, finance, and compliance.

The CENTRE organization will be supported by a strong board of advisors with deep experience in internet platforms, protocols and consumer products, enterprise development, open source software, and also deep expertise in cryptocurrency and blockchain technology.

4.0 The CENTRE Organization

The CENTRE working group expects to update this paper periodically during the course of technical peer review, legal and compliance review, finance and tax counsel, and during ongoing engineering progress.

Major updates are expected to be reported on the CENTRE web site: **http://centre.io.**

5.0 Glossary

Anti-Money Laundering rules (AML): A set of procedures, laws or regulations designed to stop the practice of generating income through illegal actions.

Application Programming Interface (API): A set of routines, protocols, and tools for building software applications. An API specifies how software components should interact. In general terms, it is a set of clearly defined methods of communication between various software components.

Bitcoin: A network in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds (when lowercase, the term also refers to the units of currency rather than the network).

CENTRE: A protocol for digital wallet interoperability across currencies and borders, across diverse software implementations, and across multiple blockchains, ledgers, and settlement rails.

CENTRE Network: The connected network of CENTRE nodes operated by participants such as wallet providers, service providers, and financial institutions.

Chained State Channels: A mechanism for allowing two state channels that are not connected directly to one another to connect securely indirectly using intermediary connections to other state channels.

Circle: Circle Internet Financial is the company which created the initial implementation of the protocol, and which will help bootstrap CENTRE development with IP contributions and licensing.

Crypto Asset: A cryptographic unit of data and software code which has value as a tradeable asset.

Ethereum: An open source, public, blockchain-based distributed computing platform featuring smart contract scripting functionality.

Hashed TimeLock Contract (HTLC): A class of smart contracts that require that the receiver of a payment either acknowledge receiving the payment prior to a deadline by generating cryptographic proof of payment or forfeit the ability to claim the payment, returning it to the payer.

IOU: A cryptographically-signed piece of data acknowledging a debt.

Implementation: A specific realization of a protocol or other software abstraction in the form of one particular incarnation in particular software code. Loosely speaking, a blueprint is to a house as a protocol specification is to an implementation.

Know Your Customer (KYC): Rules and processes in which a business identifies and verifies the identity of its clients. The term is also used to refer to the bank and anti-money laundering regulations which govern these activities.

Node: A software package which operates and manages network participation, including providing protocol and API implementations, on behalf of a network participant.

Payment Channel: Specific to Bitcoin, a Micropayment Channel or Payment Channel is a class of techniques designed to allow multiple transactions without committing all of those transactions to the blockchain. In a typical payment channel, only two transactions are added to the blockchain but an unlimited or nearly unlimited number of payments can be made between the participants. Payment Channels are a class of State Channels.

Protocol: A set of rules and guidelines for communication. Rules are defined for each step and process during communication between two or more nodes, and nodes must follow these rules to transmit data successfully. A single protocol may be realized in diverse implementations in varying programming languages and runtimes across diverse blockchains or other infrastructure.

Service Provider: A CENTRE network participant that provides services to the network to support financial transactions. In exchange for fees paid in tokens, service providers may offer compliance, KYC, identity, data storage, fraud detection, or other services of interest to other network participants.

Settlement: Delivery of an obligation in satisfaction of an IOU which may have been transacted between network members.

Smart Contract: Computer protocols intended to facilitate, verify, or enforce the negotiation or performance of an agreement.

Stablecoin: A term used to describe a crypto asset that is pegged to underlying reserved assets and/or managed by software algorithms in order to enforce price stability.

State Channel: A discussion channel between network participants capable of updating internal data (state) without requiring that every such data change be printed to an underlying blockchain. A superclass of Payment Channels.

Token: A smart contract that is employed to gain access to and use of the network, and which identifies the holder as a network participant, and which implicitly accrues value in proportion to the usefulness of the network it unlocks.

Transaction: In CENTRE, a transaction is a transfer of an IOU from one network participant to another.

Trust Level: A numeric indicator of a network participant's trust and certification level which is determined by that participant's licensing profile as well as its behavior over time.