Transparent yet Private Digital Currency

WHITEPAPER

Authors:
J. Scott Nelson, CEO, Sweetbridge
Aleksandr Bulkin, Co-Founder, Coin Fund
Scott Carlson, CISO, Sweetbridge
Aaron Stanley, Strategic Communications, Sweetbridge

Table of Contents

Abstract

This paper describes the BRC protocol, a model for implementing, governing, regulating, and accounting for hybrid crypto-virtual currencies that are 100% asset-backed and designed for use in global commercial activity. The protocol specifies technical, organizational, and economic mechanisms used to issue such electronic currencies for a multitude of use cases and jurisdictions.

A unique combination of technology and cryptoeconomics make the currencies issued under the BRC protocol an improvement over both the traditional fiat currencies and the recently popularized cryptocurrencies. The BRC protocol extends the thinking in other stable currency designs to include regulatory reporting, AML (Anti-Money Laundering), accounting and legal enforcement.

The BRC protocol is designed first and foremost to serve the needs of regulators and those entities for which regulatory compliance is essential. It does this using advanced cryptography that protects the privacy of entities from anyone who does not have a right to access the information. At the same time, it provides solutions for the requirements that must be met in order for an instrument to be used as an effective means to store and transfer economic value in contexts such as commerce, global trade, cryptocurrency exchange infrastructure, regulatory oversight, taxation, accounting, and payments. These requirements concern the performance of underlying technology, economic behavior, data privacy and transparency, reliability, recourse, and a number of other regulatory concerns.

The hybrid on-chain/off-chain technology that implements the BRC protocol provides an unprecedented best-of-both-worlds capability for any currency based on the BRC protocol, striking a balance between important features that often stand in opposition to one another. While adopting the useful aspects of cryptocurrencies, BRC prioritizes important aspects of traditional money and payment systems, which are critical for broad adoption in commerce and acceptance by governments.

This paper does not cover the stability mechanisms used in the BRC protocols in depth as they are covered in other Sweetbridge whitepapers.[1]

[1] See Sweetbridge Whitepapers, https://sweetbridge.com/whitepaper

Introduction

The need for an optimal combination of legal oversight, regulatory compliance, value stability, data privacy, and optimal performance for cryptocurrencies is becoming increasingly apparent. The emergence of cryptocurrency-native exchanges and subsequent regulatory attention[1] toward their KYC and AML processes provide a strong case for a digital unit of account that can be used as a stable reserve currency, while providing reliable KYC and AML services at the fundamental technology level, rather than relying on every organization to roll out their own suboptimal and expensive compliance operations.

At the same time, blockchain offers significant improvements to finance in global commerce and trade by extending the notion of economic value with additional features that drive liquidity, performance, and trust between participants and their governments. In this context, the biggest barrier to adoption of blockchain innovation for payments and settlement is anonymity and lack of recourse, which were priorities for the initial design of cryptocurrencies, but aren't appropriate in the context of global commerce. Anonymity in wealth preservation has long been prized, but has never been useful, in legal commerce. In fact, increasing transparency relative to traditional financial systems is both possible and would constitute a significant advantage for the BRC protocol.

In traditional financial systems, a substantial amount of information is lost during financial transactions. This is a major reason for accounting inefficiencies, as it creates significant risk within the financial system. It is also routinely exploited by bad actors for money laundering and the financing of illegal activity. The BRC protocol enables a unit of account to contain and transmit additional data, permitting unprecedented innovations in commerce. Sweetbridge is harnessing this potential to create a new type of financial network that reduces information loss and the risks associated with it. This network not only enables the reliable, inexpensive, and fast transfer of value, but also increases trust in the value chains between individuals, organizations and their governments.

[1] Joshua Fruth, "'Crypto Cleansing:' strategies to fight digital currency money laundering and sanctions evasion," Reuters, Feb 13, 2018 https://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-cleansing-strategies-to-fight-digital-currency-money-laundering-and-sanctions-evasion-idUSKCN1FX29I
Romain Dillet, "SEC says cryptocurrency exchanges are an unregulated mess,"TechCrunch, Mar 7, 2018 https://techcrunch.com/2018/03/07/sec-says-cryptocurrency-exchanges-are-an-unregulated-mess/
Michaela Ross,Peer-to-Peer Crypto Exchanges Raise Regulatory Questions"Bloomberg BNA, Apr 25, 2018 https://www.bna.com/peertopeer-crypto-exchanges-n57982091554/
Megumi Fujikawa and Steven Russolillo,"Japan's Biggest Bitcoin Exchange Suspends New Business,"The Wall Street Journal, June 22, 2018 https://www.wsj.com/articles/japans-biggest-bitcoin-exchange-halts-new-business-1529655557
Ian Talley and Samuel Rubenfeld, "U.S. Targets Bitcoin Exchange, Alleging it Facilitated Crime," The Wall Street Journal, July 27, 2018 https://www.wsj.com/articles/u-s-targets-bitcoin-exchange-alleging-it-facilitated-crime-1501194444

Through blockchain and cryptographic protocols, it is now possible to create an informationally transparent currency that both protects privacy and enables regulators to reduce the risk of bad actors. Currencies based on the BRC protocol are designed to be used as a substitute for cash while still being influenced by the monetary policy of nation states. The BRC protocol will increase liquidity, reduce friction, and lower risk within the system as a whole and to each entity that utilizes it.

The BRC protocol authored by Sweetbridge defines a model for implementing a transparent and value-stable currency specifically designed for commerce while keeping in mind the needs of individuals, organizations, and governments. The BRC protocol design rests on four pillars: technological, economic, organizational, and legal/regulatory. It is based on the premise that usable decentralization can be achieved by creating a number of centralized entities that operate under a common protocol and are each, individually, both replaceable and autonomous. This is represented in Figure 1, where the technological, economic, organizational and regulatory aspects are presented as elements of the protocol that unite the network of such entities.

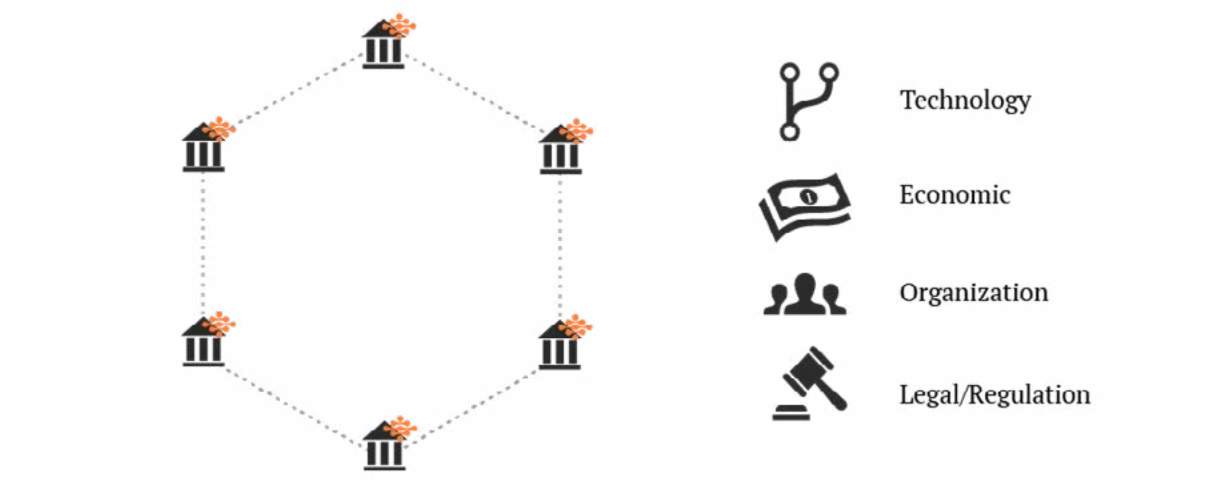


Figure 1: BRC Protocol Design

From the **technology** standpoint, BRC will be adopting a hybrid on-chain/off-chain model in order to combine the strong finality of blockchain settlement under consensus with the high speed and privacy of transactions in the interim. This hybrid model will enable seamless integration into the Sweetbridge ecosystem of both existing crypto assets and digital ownership models representing real-life assets such as receivables, commodities and real estate.

From the **economic** standpoint, BRC will operate as a fully collateralized value-stable currency and adhere to strict accounting standards that govern assets classified as cash equivalents. Sweetbridge-licensed entities will provide liquidity and collateralization mechanisms necessary for such classification. The BRC protocol allows the value trapped in any asset to be converted into a new asset class that can be treated as a cash equivalent. This process can be used with any asset that has a market for price discovery and is accomplished without selling the valued asset.

From the **organizational** standpoint, Sweetbridge will be establishing a network of Sweetbridge-licensed entities that will be required to adhere to strict standards of transparency, auditability, data privacy, and regulatory compliance. These entities will be tasked with implementing the highest standard of KYC/AML operations within their home jurisdiction as well as with issuing and overseeing the BRC treasury according to the overall protocol.

From the **legal and regulatory** standpoint, the BRC protocol uses the Sweetbridge accounting protocol to provide regulators with transparency and recourse mechanisms necessary to eliminate bad actors and monitor activity as required within their specific jurisdiction, while preserving the individual privacy of users and ensuring that due legal process is followed at all times.

This approach holistically answers the needs of global commercial activity, as well as responds to regulatory concerns. It provides a model that is better suited for trade than either the traditional fiat currencies or the pure on-chain cryptocurrencies. It ensures the privacy of information while allowing governments access to information when they have a right to know. Additionally, by establishing a network of independent entities, Sweetbridge is launching a network that is resilient to manipulation either through wealth or through political influence. The components of the approach are detailed in the subsequent sections.

Technological Approach

The protocol that underlies BRC uses the Sweetbridge accounting protocol to transfer value. This protocol is peer-to-peer, making it as decentralized as possible, while at the same time it preserves the features necessary to utilize the currency in a variety of situations where a fully decentralized cryptocurrency cannot be adopted. This approach makes BRC a hybrid between a cryptocurrency and a more traditional virtual currency that can be accounted and transmitted via centralized payment networks.

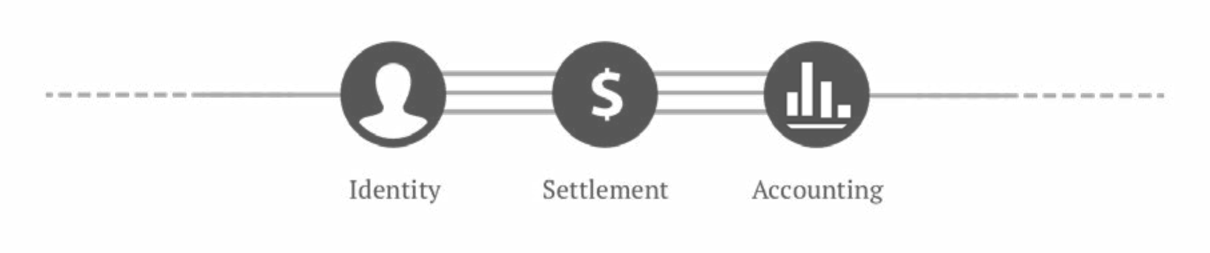


Figure 2: BRC Protocol Technology

The protocol is a combination of a fully decentralized blockchain used for the eventual settlement of value and for recording ownership of real-world assets; an identity protocol that ensures that the legal identity of transacting parties can be discovered for the purposes of commercial litigation or legal enforcement; and a blockchain-agnostic accounting protocol that permits integration of BRC into traditional payment systems and enables near-instantaneous transmission of payments.

It is important to recognize that BRC can be seen neither as a cryptocurrency nor as a private virtual currency[1], but rather is something that has the properties of both, depending on the context. The reader familiar with advances in the space of decentralized payments may compare the off-chain components of the protocol with state channels of Ethereum[2] and Lightning Network of Bitcoin[3]. The advantage that the BRC protocol brings to such decentralized solutions is that rather than being represented as a simple payment, the off-chain transaction data contains detailed accounting records, which allows for rich recourse, auditability, and monitoring needed by both regulators and risk managers.

[1] See Andrew Tar, "Digital Currencies vs. Cryptocurrencies, Explained," CoinTelegraph, Dec 13 2017 https://cointelegraph.com/explained/digital-currencies-vs-cryptocurrencies-explained

[2] See Antonio Madeira, "What are State Channels," CryptoCompare, 20 May 2018 https://www.cryptocompare.com/coins/guides/what-are-state-channels/.

[3] See Noelle Acheson, "What is the Lightning Network," CoinDesk, nd https://www.coindesk.com/information/what-is-the-lightning-network/.

Figure 3: Sweetbridge LOU

In order to preserve privacy, these transaction records are cryptographically signed and stored off-chain by Sweetbridge-licensed local entities know as an LOU (e.g. Local Operating Unit[1]), as well as the trade counterparties, who may at any time request on-chain settlement. The identity component of the protocol allows legal recourse to take place whenever one of the parties in the network misbehaves. The opportunity for legal recourse reduces the need for on-chain settlement, which is expensive and slow. The design of the peer-to-peer communication channel as a shared accounting ledger requires signatures from all counterparties in transactions, and makes it both difficult and futile to generate conflicting records (a case of an off-chain double spend).

[1] Similar to the GLEIF (Global Legal Entity Identifier Foundation) term for an organization authorized to issue LEIs to legal entities participating in financial transactions is referred to as a Local Operating Unit (LOU). LOUs supply registration, renewal and other services, and act as the primary interface with legal entities for LEIs. A LOU may issue LEIs to legal entities in any jurisdiction for which it is accredited.

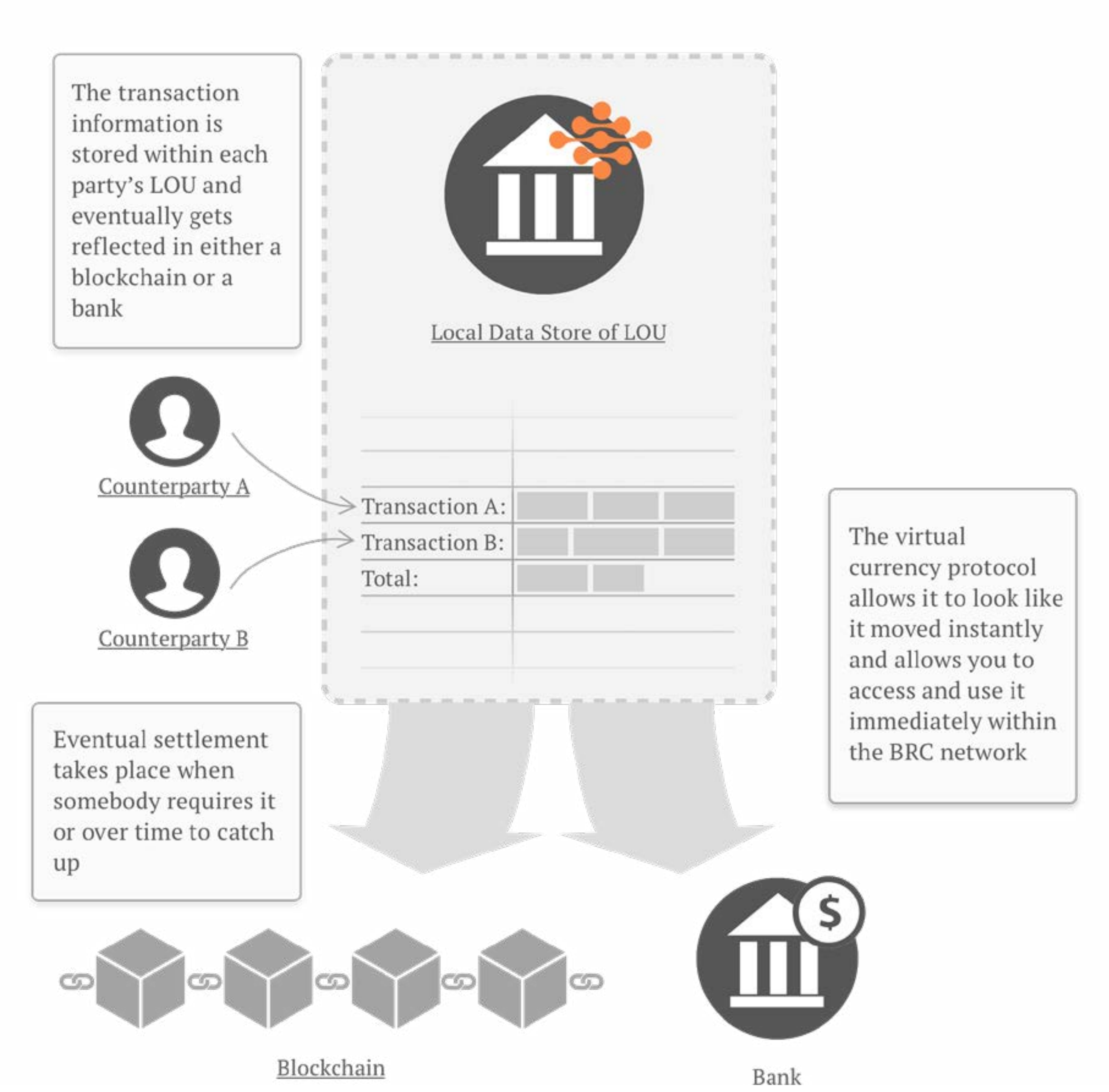

The transaction information is stored within each party's LOU and eventually gets reflected in either a blockchain or a bank
Local Data Store of LOU
Counterparty A
Counterparty B
Transaction A:
Transaction B:
Total:
The virtual currency protocol allows it to look like it moved instantly and allows you to access and use it immediately within the BRC network
Eventual settlement takes place when somebody requires it or over time to catch up
Blockchain
Bank

Figure 4: Eventual settlement

Associating detailed accounting records with off-chain transactions enriches the overall dataset with information required for purposes such as real-time tax accounting, AML monitoring, and real-time risk management between counterparties. At the same time, storing this information encrypted and off-chain allows for preservation of privacy of every individual participant, while ensuring that the details may be discovered through a due legal process.

Additionally, this model permits traditional payment processors, such as banks, Paypal or AliPay, to integrate BRC into their systems as if it were a virtual currency. In such cases, the off-chain accounting data for relevant transactions would be centrally managed by the payment providers and governed by the existing legal frameworks that control e-payments today. The on-chain settlement of transactions would be required infrequently, and when/if required, it would function as a background task that does not demand the user's attention. The speed and cost of payments that is achievable by this mechanism is comparable with those carried out by traditional banks, when funds are transferred between accounts that belong to the same organization.

Much of global commerce actively relies on legal recourse for protection against bad actors. While cryptocurrencies do not allow recourse, the architecture underlying BRC restores the ability of properly authorized parties to enforce economic obligations by counterparties in commercial settings. The rules associated with the off-chain accounting records include situations in which a transaction may be generated against a network member's account in the course of a criminal enforcement or an arbitration proceeding. The process is subject to strict rules and is dependent upon the agreements and laws governing every specific jurisdiction.

Additionally, this model provides a mechanism to protect Sweetbridge network members from exotic situations arising from the way blockchain consensus operates. Namely, if a branch of an underlying blockchain containing a settlement transaction were to be reverted, hard-forked, or pruned for any reason, the off-chain records can still be committed to the new active branch, ensuring that a valid BRC transaction is never lost.

PERFORMANCE

To be used for high-volume commercial transactions, a payment system must be able to support at least one million transactions per second to be a viable replacement for credit card networks or banking networks in use today. In addition, the time to process a single transaction at peak volume can't be more than three seconds and should ideally be under one second from any location in the world.

Current blockchain-based settlement processes that rely on consensus protocols to prevent double spending don't provide these levels of performance. The design of the BRC protocol enables an almost unlimited level of transaction throughput because it is a peer-to-peer protocol that mostly operates off-chain. The speed of the transaction is controlled by the performance of the servers operated by the LOUs. There is no limit for the number of LOUs in the network, so performance can be increased by subdividing the LOUs. To promote this behavior, the fees received per transaction by a LOU are decreased as the transactions it processes exceed optimal levels. Because the new LOUs are able to make more money per transaction, a continual forking and creation of new LOUs as existing entities grow larger is thus incentivized. This incentive structure fosters the creation of new LOUs as existing ones grow larger.

The speed of a single transaction is controlled by the performance of the LOUs that manage the member accounts. LOUs can share servers or have multiple dedicated servers. To encourage investing in performance improvements, the protocol charges an escalating penalty on transactions when performance is more than a second. This encourages investments in LOUs to provide performance improvements.

DATA PRIVACY

The BRC protocol maintains all publicly stored information using one-time identifiers that uniquely refer to the participants' accounts without revealing their identity. Furthermore, transactions are settled to the public blockchain in aggregate, hiding all of the participants' confidential details. Instead of storing the details in a publicly observable data store, the sensitive data is held inside the repository maintained by the Sweetbridge LOUs. These repositories link the private information to the on-chain hash codes as appropriate.

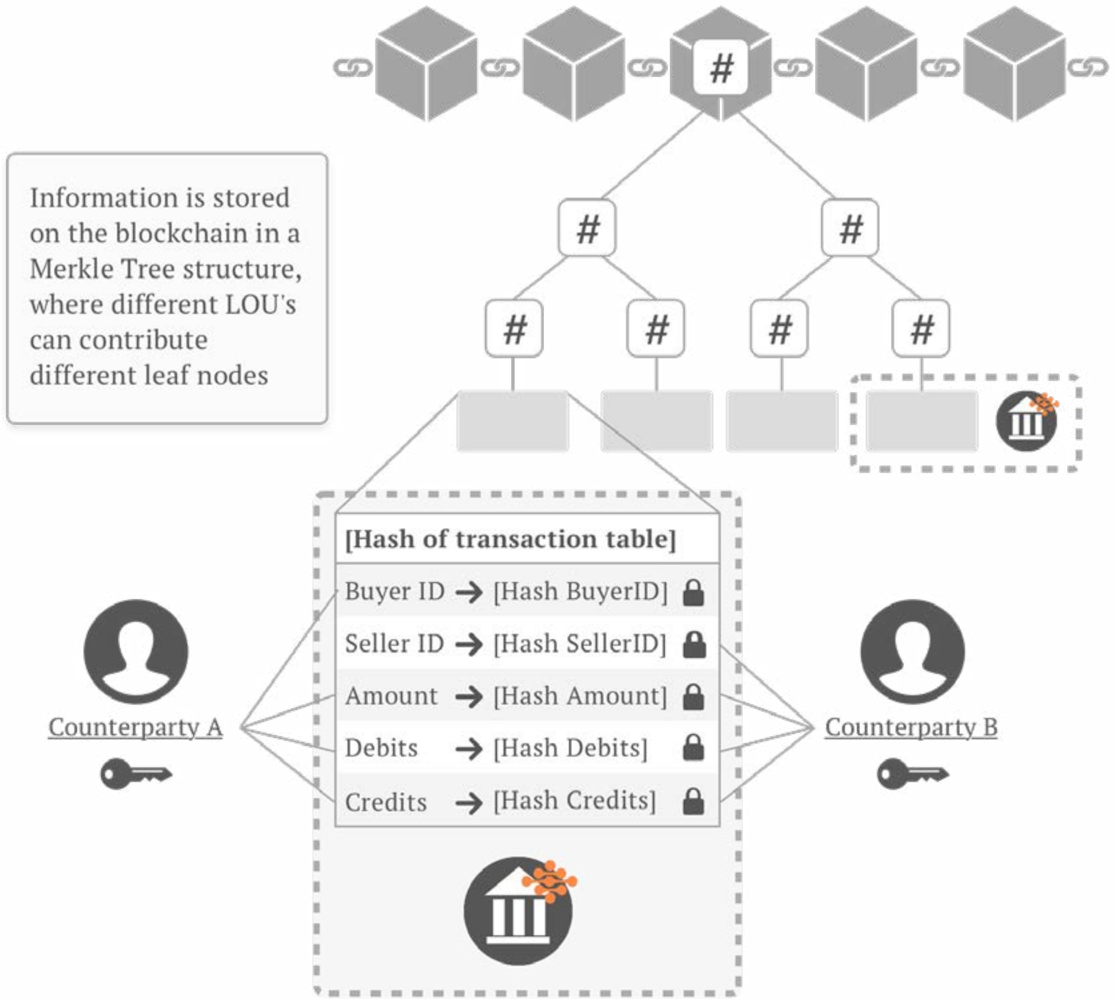

#
#
#
#
#
#
#
Information is stored on the blockchain in a Merkle Tree structure, where different LOU's can contribute different leaf nodes
[Hash of transaction table]
Buyer ID → [Hash BuyerID]
Seller ID → [Hash SellerID]
Amount → [Hash Amount]
Debits → [Hash Debits]
Credits → [Hash Credits]
Counterparty A
Counterparty B

Figure 5: Merkle tree hashed transaction table

The identity component of the BRC protocol stores private information of the member, or refers to external repositories (such as Sovrin Claims) in which the member has granted authorization to their sovereign identity. Private information and accounting details are encrypted with the member's private key. The information is also encrypted using a member specific jurisdiction key that allows the legal jurisdiction of the entity to access the information through due course of law. This ensures that the transparency is maintained, yet there are also privacy guarantees. The real identity can only be obtained and reported to authorities with a legal right to the information.

Regulatory Approach

The BRC protocol's regulatory approach aims to ease the burden of fulfilling regulatory and compliance obligations on the part of all participants, while protecting sensitive data from exposure both due to unauthorized access and unreasonable search and seizure. Additionally, this section describes the overall approach to data privacy, identity management, and location-specific data storage. Within its comprehensive structure, the BRC protocol also provides for the needs of individual participants for a sufficiently strong inter-entity trust mechanism, supported not only by technology, but also by reliable organizational and legal frameworks.

Such an approach is necessitated by the heightened governance, risk and compliance requirements currently faced by governments, corporations, and other commercial entities in the age of de-risking. Because of the various negative perceptions and activities with which cryptocurrencies have come to be associated, building proper compliance and risk controls into the protocol itself is a prerequisite to these types of institutions adopting any blockchain-enabled system at commercial scale.

An industry-developed solution to these problems must bake in transparency and visibility around the identities of the parties and assets involved in transactions, as well as RegTech mechanisms that facilitate consumer protections, tax and trade compliance and enforcement actions when necessary. While these issues have to date gone largely unaddressed, if not ignored altogether, by actors in the cryptocurrency industry, the BRC protocol seeks to empower both regulators and commercial entities by giving them the tools to better manage risk as technological change becomes more dynamic.

Properly addressing GRC concerns is also imperative for ensuring buy-in from large corporations that must manage these risks at board level. New payment and value transfer mechanisms that do not have governance and risk management procedures built in at the asset level will have difficulty becoming broadly accepted in commerce, particularly within heavily-regulated industries.

The framework described in this section draws on the capabilities of the BRC protocol's approach to cryptography and value accounting described in the Technological Approach section. The cryptographical model of data storage and access assures overall data privacy, while preserving the ability of regulators and payment processors to monitor transactions for suspicious activities, as detailed below.

REGULATORY REQUIREMENTS

Governments require transparency from financial organizations that provide means of value transfer. Consequently, there are ten requirements enforced by licensed organizations, the directors of which are legally accountable within their jurisdiction:

1. KYC (Know Your Customer) to identify that members are real, have a solid legal identification, and are in good standing;
2. CIP (Customer Identification Program) to ensure that the human behind the keyboard is the same as the customer during the sign-up process and during a transaction;
3. PEP (Politically Exposed Persons tracking) to identify situations in which bribes or improper financing of political activity may be involved;
4. AML (Anti-Money Laundering) to identify and report suspicious behaviors through active monitoring and reporting;
5. PIP (Payment Information Process) and CTR (Currency Transaction Report) or its equivalent internationally;
6. CP (Customer/Consumer Protection) to protect the customers' financial assets from loss or theft;
7. The ability to authorize parties such as employees or attorneys to act on behalf of a member;
8. Maker-checker process to require an approval by a designated additional party on certain transactions, such as those of high monetary value;
9. Recourse and indemnification to enforce a judgement in a legal context;
10. Transparency of identity for ownership proof, tax assignment, or criminal investi gation purposes.

The nature of these requirements, as well as the way the BRC protocol addresses them, is detailed in subsequent sections.

KNOW YOUR CUSTOMER (KYC) TRANSPARENCY REQUIREMENTS

Know Your Customer (KYC), Customer Identification Program (CIP) and Politically Exposed Persons (PEP) are increasingly required to prevent payment systems from being used by bad actors to launder money or finance illicit behavior. Any payment system used to transfer value in commerce must maintain records of the identity of the parties to ensure that the parties:

- Have identities confirmed by governmental identity documents,
- Are further reviewed if they have proven criminal backgrounds,
- Are not likely to be subject to bribes, and
- Are not likely to be associated with terrorist activities

The purpose of KYC is to ensure that actors involved in or likely to be involved in illicit activities are rejected by the payment system. BRC currencies can only be owned by Sweetbridge members that have passed KYC validation through licensed Sweetbridge financial services partners. BRC currencies cannot be transferred to anyone who does not have a Sweetbridge membership, and the only way to transfer value outside of the system is to go through a Sweetbridge licensed exchange, thus enabling full transaction assignment and completed KYC for all parties involved.

AML REQUIREMENTS

Governments have created both informational statements and regulations that will drive cryptocurrencies used in commerce to support transparency. The 4th Anti-Money Laundering Directive (4AMLD) in the European Union, and Article 4A of the Uniform Commercial Code in the US, are two such examples.

Corruption is estimated to cost $1.5–$2 trillion to the global economy[1]. A transparent cryptocurrency such as one based on the BRC protocol can reduce tax evasion in the shadow economy. The size of the shadow economy is difficult to estimate, but a recent estimate put the number at €454 billion in Europe alone[2].

Sweetbridge has carried out research into the financial regulations of major economies and found common patterns related to the use of money/cash within society.

Most regulatory jurisdictions aim to:

1. Understand how much income their citizens and companies earn;
2. Collect appropriate amount of taxes from entities operating within their jurisdiction;
3. Understand the volume of transactions affecting their economy;
4. Protect citizens from fraud by ensuring that they receive funds that are due in commercial activities;
5. Ensure that criminal activity or terrorism is not supported by payment systems; and
6. Minimize or eliminate corruption and illicit activity within their economy.

The AML monitoring and reporting systems required by governments will increasingly be applied and must be enhanced when cryptocurrencies are used. The Financial Action Task Force (FATF), formed to combat money laundering, has been seen by many nations as critical to recent progress in reducing illicit activity.[3]

[1] See David Lauder, "IMF: Global corruption costs trillions in bribes, lost growth," Reuters, May 11 2016, https://www.reuters.com/article/us-imf-corruption/imf-global-corruption-costs-trillions-in-bribes-lost-growth-idUSKCN0Y22B7

[2] See Vanessa Houlder, "Europe's shadow economy costs €454bn in 'lost' taxes," Financial Times, September 24 2015, https://www.ft.com/content/9c30cc14-5e1c-11e5-a28b-50226830d644

[3] See Joshua Fruth, "'Crypto-cleansing:' strategies to fight digital currency money laundering and sanctions evasion," Reuters, February 2018, https://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-cleansing-strategies-to-fight-digital-currency-money-laundering-and-sanctions-evasion-idUSKCN1FX29I

Cryptocurrency systems and exchanges will increasingly be required to look for and report on suspicious activities. This can already be seen today in the increasing difficulty of moving funds out of cryptocurrencies into fiat.[1] [2]

When it comes to existing cryptocurrencies, the only way to enforce AML standards is through exchanges. Regulators can only exert control over exchanges within the borders of their jurisdiction. The effectiveness of AML rules therefore suffers because of the use on non-regulated exchanges and trading activities outside of each government's jurisdiction.

The BRC protocol not only replaces the need for governments to rely on the service provider for AML, it eases the burden on those participating in the exchange that desire to proactively comply with regulation, because intrinsic to the transparency is full tracking of all assets as they move through the ecosystem.

THE BRC REGULATORY SOLUTION

The hybrid on-chain/off-chain technology underlying BRC delivers the best-of-both worlds features, combining privacy with the ability of regulators and arbitrators to provide legal recourse and regulatory oversight. Furthermore, it establishes standardized mechanisms for KYC and AML at the base technology level, rather than by requiring every member of the organization to implement their own solution. This is the key proposition that the BRC protocol brings to governments, banks, exchanges, and payment providers.

The transparency approach of BRC is designed to make monitoring for illicit activities easier. It is integrated with the Sweetbridge Accounting Protocol, which collects substantially more information about each transaction than any other payment system in use today. This enables a rigorous AML process, whichmakes using the Sweetbridge network for money laundering prohibitively expensive, especially when compared to existing banking systems, because there is a single source of information in which all parties and all assets are known, and every step in the process is tracked. This enables real-time direct monitoring for patterns present in potentially fraudulent transactions. Additionally, the Sweetbridge Accounting Protocol ensures that the physical, legal, and accounting states must match, making auditing trivial and ensuring that money laundering activity is arduous and ineffectual.

By providing regulators and other interested parties limited access to the identity and transaction data within the network, the BRC protocol goes beyond KYC/AML. It provides a level of detail around transactions that exceeds the information available in banking settlement systems or credit card networks; but unlike these systems, it provides an increased level of user privacy. The government or law enforcement agencies can only access the information through the

[1] See Rodney Greene, Liquidity or Leakage: Plumbing Problems with Cryptocurrencies, Long Finance, March 2018, http://www.longfinance.net/DF/Liquidity_Or_Leakage.pdf

[2] See Dancing With the Devil: 'Cashing Out' Cryptos Into Fiat Not So Easy, Dec 2017, Bitcoin.com, https://news.bitcoin.com/dancing-with-the-devil-cashing-out-cryptos-into-fiat-not-so-easy/

due process of law through the Sweetbridge licensed entities that issue membership to users.

To address the key governmental concerns of transparency and recourse, as well as to account for the individual monetary policies of each nation state, the accounting and identity data is kept in data-stores that are encrypted using a special encryption key for an entity within its legal jurisdiction. The private key is not known to anyone but rather is distributed across different LOUs in the Sweetbridge network (see Figure 6). Gaining access to the data requires due process to compel multiple LOUs to provide appropriate cryptographic keys, ensuring that a single actor is unable to read the data illegally, while providing regulators with tools to monitor and investigate transactions within their geographical zone.

By offering an appropriate balance between privacy and transparency based on the hierarchical view of accounting data describing all commercial activity, BRC addresses these concerns, alleviating the adoption problems and regulatory concerns with existing cryptocurrency models.

IDENTITY

Identity management is one of the most important components of any information system used in trade and commerce. It provides information about parties one engages with, and implicitly establishes a framework for trust, recourse, dispute resolution, risk management, and legal enforcement.

The Sweetbridge KYC/CIP protocols are integrated with and extend the Sovrin protocol[1]. They use the credentialing and validation aspects of the Sovrin protocol to issue and revoke legal entity IDs within the Sweetbridge network as verifiable claims. These identity credentials can be shared with trading partners, governmental agencies and others to prove the tax identity of a party in a commercial activity. The identity system can also provide validation of authority and spending limits for individuals acting on behalf of an organization or another individual when digitally signing transactions or agreements. Identity claims from other Sovrin members could represent governments, banks, or other issuers of identity, which immediately allows onboarding and verification of members, all transacting in BRC-based currencies.

LOCATION OF DATA

The global nature of an economy means that a member in one region can transact with a member in any other region using the BRC currency. Where the data is stored for the member and individual transactions is important due to data localization and processing requirements ratified by national governments.

[1] See Sovrin: A Protocol and Token for Self-Sovereign Identity and Digital Trust, Jan 2018, https://sovrin.org/library/sovrin-protocol-and-token-white-paper/

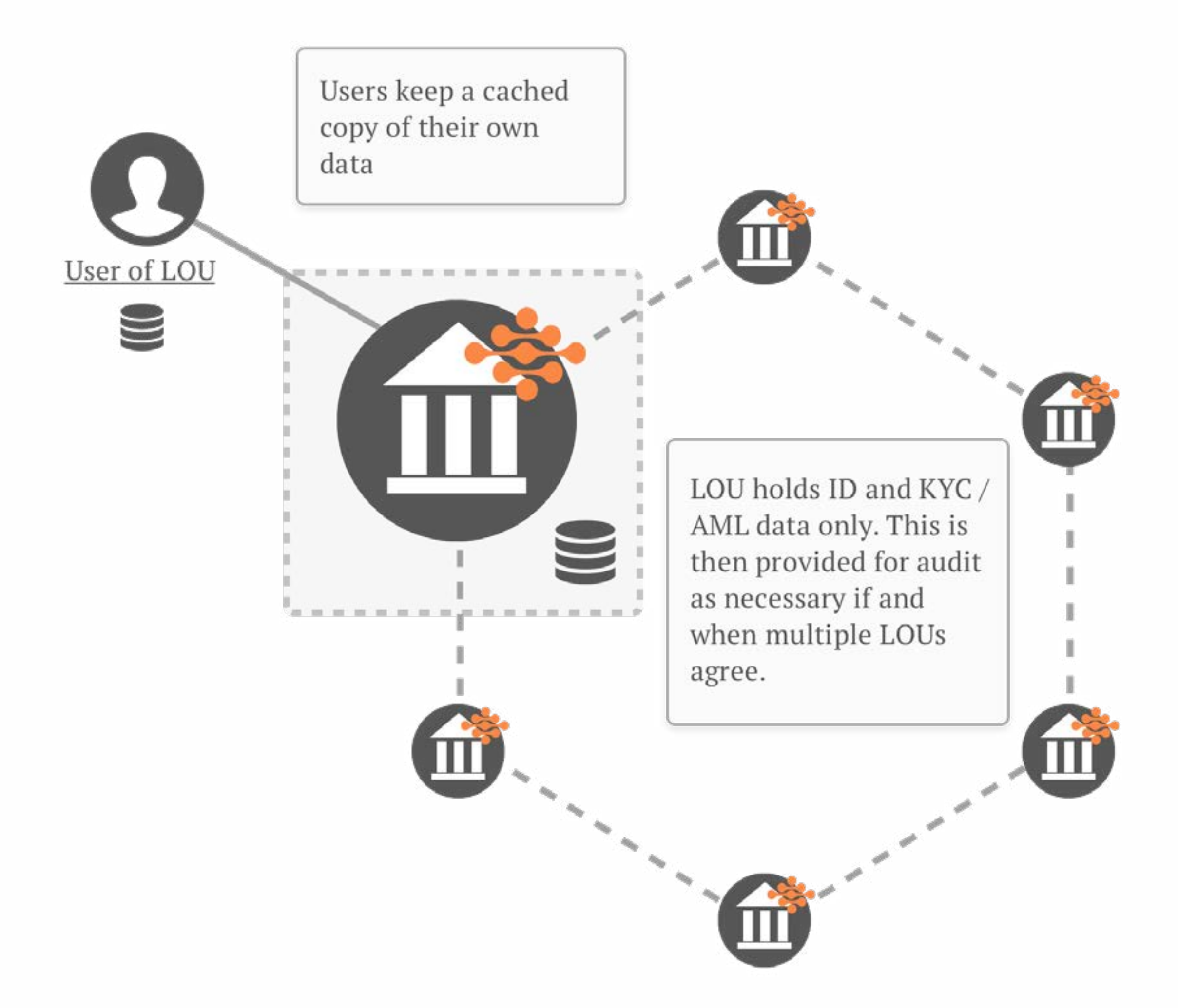

Users keep a cached copy of their own data
User of LOU
LOU holds ID and KYC / AML data only. This is then provided for audit as necessary if and when multiple LOUs agree.

Figure 6: Storage of data

Member data is controlled by each user and is verified by a distributed set of Sweetbridge-licensed LOUs. An encrypted copy of the data is maintained by each node and is stored within physical data centers or cloud providers in compliance with the the regional legal requirements expected of that entity. In some cases, there are requirements for private member data to not be transportable outside the region other than the specific cases to which members explicitly agree. In the model developed for BRC, the following steps have been taken to fulfill these requirements:

- Private data for citizens must be primarily stored within their assigned region. For instance, if I am a private citizen of the EU, my personal data must be physically stored within the EU. Where countries have such requirements for data storage, the data will be stored in the appropriate locations as mandated.
- The entire ecosystem can process a transaction from any member entity, as long as strong encryption guards the data, and is not compromised as part of the process.

- The Sweetbridge data on the public stores does not contain any personal or transaction data of any of its members that is not encrypted.
- If a country has a data localization requirement, a standard approach is taken including: (a) a country-specific encryption key, (b) at least one node within the country for localized storage of the data, (c) means to decrypt the data when required by local government that does not infringe on any other data within the network.
- As transactions are appropriately encrypted and anonymized, when a Sweetbridge entity processes a transaction, due care is taken to never directly refer to the individual member records except to retrieve and display them for authorized viewers. The act of transmitting data over the internet and displaying it to the member does not constitute storage.
- As an affiliate entity is bound to an LOU within a jurisdiction, there exists a method to identify the responsible LOU based on the hash of the member's tax identity. This is kept as an economy-wide lookup table.
- Where applicable, Sweetbridge operates in countries that are signatories to the Strasbourg Convention. These countries are the jurisdictions that provide "adequate protection" of the rights and interests of data subjects.[1]
- Sign-up, data processing, and data storage language presented to the members is clear and outlines when we use, share, and how we store data, following the requirements of GDPR.[2]

PROTECTION FROM LOCALIZED SEIZURE OR NATION STATES

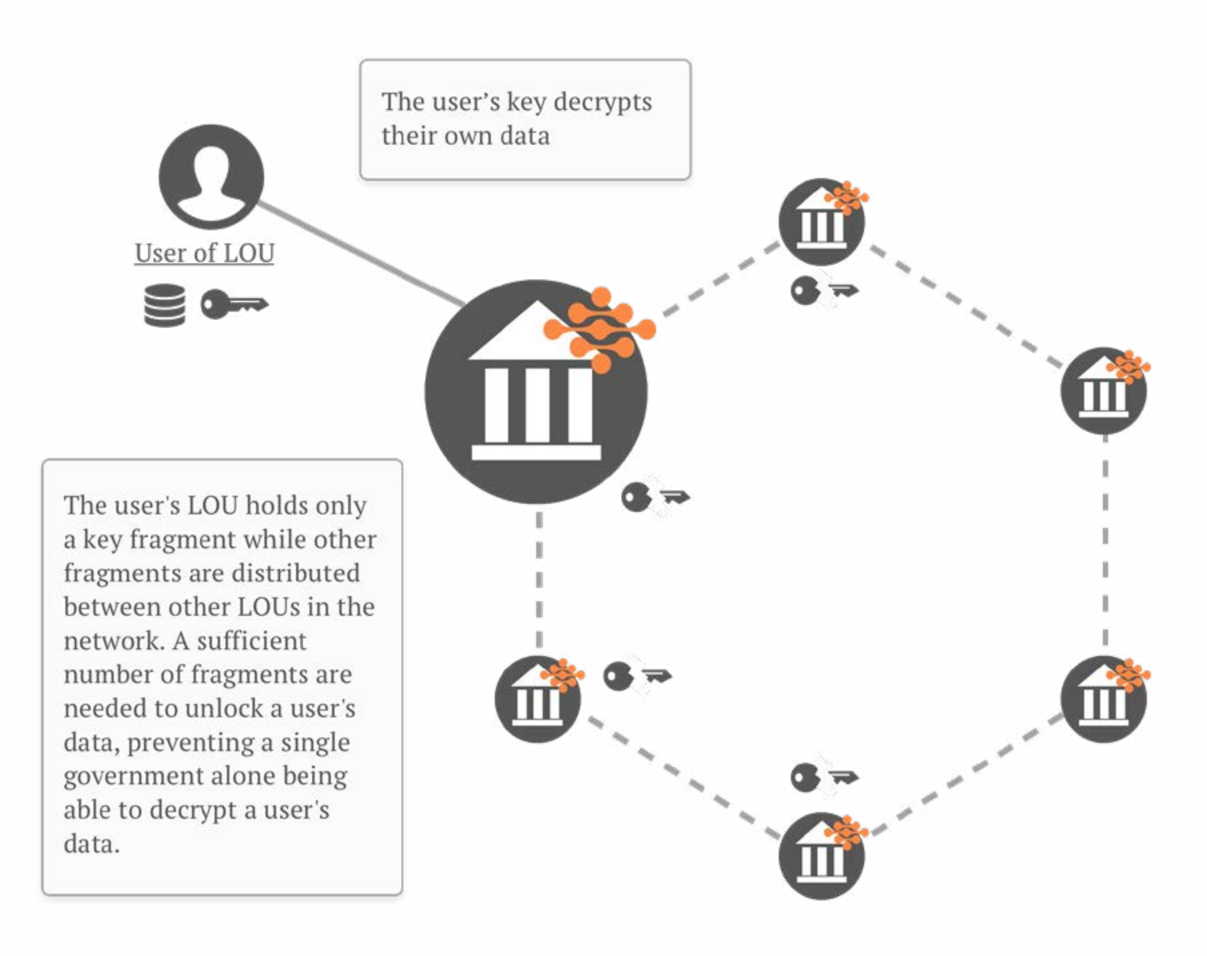
Data related to each country is encrypted with a key unique to the member's tax identity within that country. To provide for the ability for the government to enforce its right to access the data under due process, such key is also broken up and distributed between Sweetbridge LOUs. This ensures that the data can only be accessed by the jurisdiction in which it is legal to do so.

When data is stored within a certain country, it is possible that the nation could, without proper legal means, seize the data repositories of any LOUs located within that country. Due to the way in which keys are distributed, that government would not be able to decrypt its own country's data. This assures that due process is followed in all cases and prevents a power shift or coup d'état from gaining access to information for bad purposes such as ethnic cleansing.

[1] See "Council of Europe Privacy Convention," Electronic Privacy Information Center, nd, https://epic.org/privacy/intl/coeconvention/

[2] See Sweetbridge Privacy Policy, May 25, 2018, https://sweetbridge.com/privacy-policy

Only users can decrypt their transactions, documents, or identity information without permission from multiple LOUs holding parts of the member and LOU specific keys. This means that a legal request for information or a legal judgement must be submitted to a sufficient number of LOUs and that they must agree that the request or judgement is valid, in order to access information or process a financial adjustment.



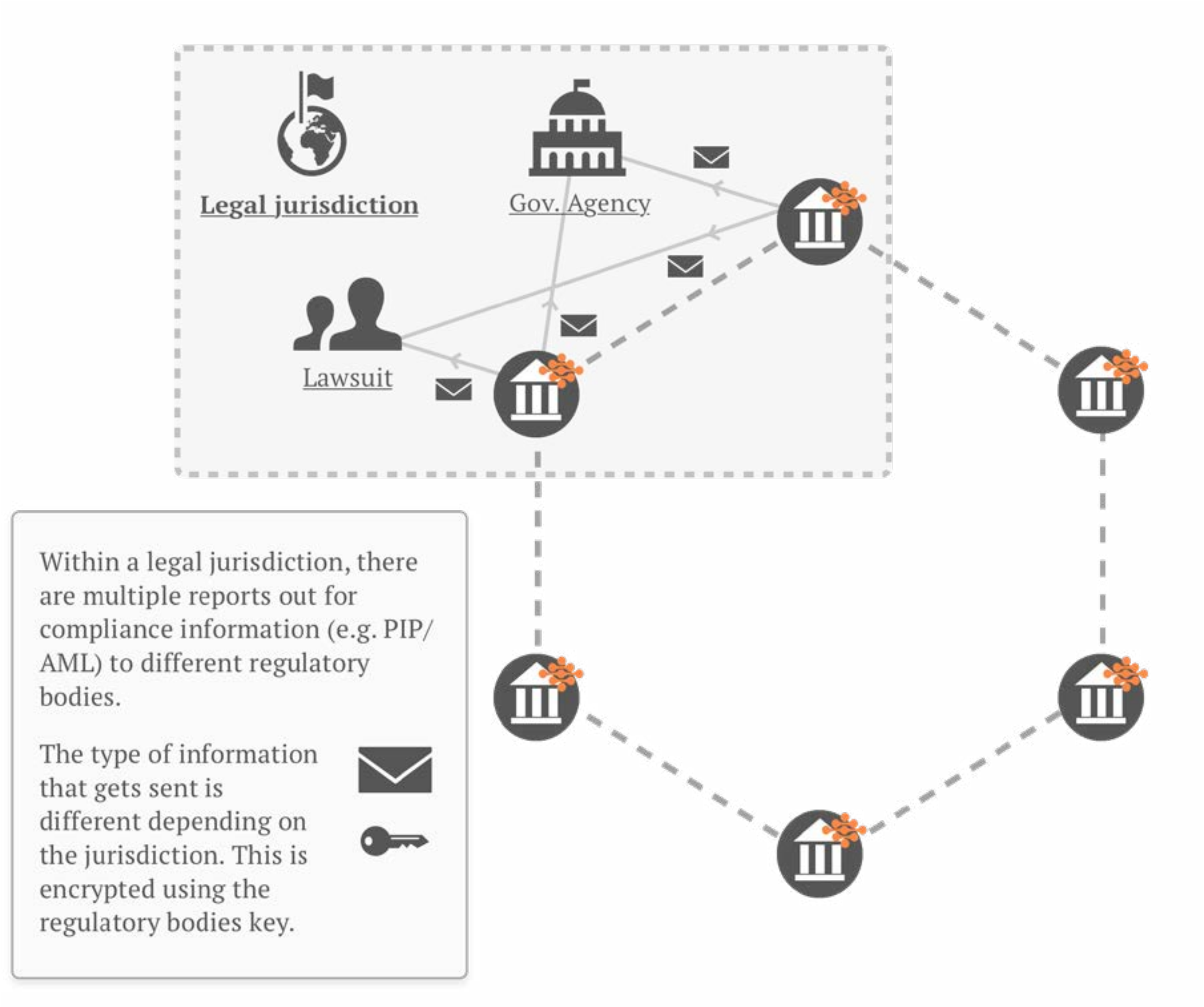
The user's key decrypts their own data

The user's LOU holds only a key fragment while other fragments are distributed between other LOUs in the network. A sufficient number of fragments are needed to unlock a user's data, preventing a single government alone being able to decrypt a user's data.

Figure 7: Distribution of keys

PUBLIC AUDITABILITY

When BRC currency is minted the collateral asset and its valuation must be publicly disclosed and auditable. The asset class must be periodically re-evaluated by an independent entity depending on the asset class and jurisdiction. When the asset is removed from the network, the BRC minted will be destroyed.



Within a legal jurisdiction, there are multiple reports out for compliance information (e.g. PIP/AML) to different regulatory bodies.

The type of information that gets sent is different depending on the jurisdiction. This is encrypted using the regulatory bodies key.

Figure 8: Reporting in a legal jurisdiction

Organizational approach

The BRC protocol is open source. It is developed and maintained by multiple organizations building on the initial work done by Sweetbridge for the benefit of the global community. Entities that want to be able to issue BRC-based currencies must obtain a Sweetbridge license and in many jurisdictions may need one or more government-issued licenses for money transmission and other bank or custodial licenses depending on the asset classes involved.

These entities are called LOUs and must maintain hardware-encrypted servers capable of implementing appropriate key management procedures. LOUs act as a line of defense against potential regulatory overreach or influence by other types of power brokers. Each request to decrypt private data by an LOU must be approved by a sufficient number of other LOUs before it can be carried out. The LOU data repositories also host the information required to satisfy regulatory reporting requirements or meet local storage of data requirements.

To maintain a Sweetbridge license, entities must submit to periodic and random audits that verify (1) that each node follows all regulatory requirements, (2) that asset-backing BRC currencies are real, (3) that appropriate contracts are in place, and (4) that all data storage requirements are met. To ensure that LOUs don't have an incentive to cheat, each one must maintain an economic stake consistent with their level of activity. Some or all of their stake can be seized by a vote of a sufficient number of LOUs when violations of the regulations are found.

By using a network of independent licensed entities, the BRC protocol solves the governmental need to have local organizations that can be held accountable, while still allowing the system to operate via a sufficiently decentralized network of independent actors.

Economic approach

The BRC protocol defines a mechanism for issuing and transacting in a number of hybrid electronic currencies. In order to seamlessly serve the economic needs of multiple jurisdictions, BRC currencies can be created in various flavors, each pegged to the fiat currency of some nation state. This aligns the BRC economy with the monetary policy of the nation states, while giving participants a way to eliminate currency exchange risks. The currencies within the BRC protocol can be pegged to any asset. For example, it is possible to issue a currency pegged to a globally recognized basket of value and thus establish a global cross-border currency to serve the needs of world trade and commerce.

BRC is intended to be sufficiently stable in value against its underlying asset (such as the local fiat currency) to meet the GAAP[1] and IFRS[2] accounting requirements of a cash equivalent, so that it can be held on a balance sheet as cash. As such, it must be convertible to fiat within five business days or less, using the exchange services provided by Sweetbridge and its affiliates. These currencies strive to become rated financial instruments by recognized rating agencies such as Fitch Rating, Moody's and Standard & Poor's.

[1] See Generally Accepted Accounting Practice in the UK, Institute of Chartered Accountants in England and Wales, nd, https://www.icaew.com/technical/financial-reporting/uk-gaap

[2] See International Financial Reporting Standards, https://www.ifrs.org/

Conclusion and Summary

It’s no secret that the frictionless value transfer ability that cryptocurrencies offer hold the potential to upend and transform all verticals of commerce. Yet, to date, these technologies have yet to penetrate supply chains and other areas of business-to-business commercial activity and have instead been relegated to the confines of peer-to-peer transfers and trading in crypto markets. This is primarily because a core feature of early-stage cryptocurrencies has been that of anonymity and pseudonomity, making currencies like bitcoin too precarious for risk-averse regulated entities. Thus, while this emphasis on anonymity is beneficial when one’s objective is wealth preservation, it becomes a severe impediment when the goal is to realize scaled adoption in real-world commerce.

Through blockchain and cryptographic protocols, it is now possible to create an informationally transparent currency that is faster, cheaper and more efficient than existing alternatives; protects user privacy and enables governments and regulators to safeguard citizens and mitigate risks posed by bad actors. Such a currency could be used as a substitute for cash yet still be subservient to the monetary policy of nation states. It would be a stable asset-backed currency that increases liquidity, reduces friction, and lowers risk within the system as a whole and to each entity using the currency.

Sweetbridge’s BRC protocol is designed to fill such a role by fulfilling all three requirements of a functioning currency (medium of exchange, store of value, unit of account) in addition to compliance requirements that, while not inherent to the nature of money, are demanded by modern governments and regulated financial systems. These include Know Your Customer processes, Anti-Money Laundering provisions and transparency of identity for proof of ownership, tax or criminal investigation purposes.

The BRC protocol is designed first and foremost to serve the needs of regulators and those entities for which regulatory compliance is essential. By using advanced cryptography that prohibits access to data by non-legally authorized parties, the protocol strikes a balance between the needs of users who demand privacy and regulators and law enforcement that require visibility in certain circumstances. At the same time, the protocol solves the practical requirements that are prerequisites to storing and transferring economic value in contexts such as commerce, global trade, cryptocurrency exchange infrastructure, regulatory oversight, taxation, accounting, and payments.