BRICS
CHAIN

The BRICS Chain White Paper v1.0

BRICS Chain

“BRICS on The Blockchain”

Table of Contents

Abstract

A digital token backed by BRICS currency provides individuals and organizations with a robust and decentralized method of exchanging value while using a familiar accounting unit. The innovation of blockchains is an auditable and cryptographically secured global ledger. Asset backed token issuers and other market participants can take advantage of blockchain technology, along with embedded consensus systems, to transact in familiar, less volatile currencies and assets. In order to maintain accountability and to ensure stability in exchange price, we propose a method to maintain a one to one reserve ratio between a cryptocurrency token, called $BRICS, and its fassociated real world asset, BRICS currency. This method uses the blockchain, Proof of Reserves, and other audit methods to prove that issued tokens are fully backed and reserved at all times.

Introduction

BRICS is an acronym for five leading emerging economies: Brazil, Russia, India, China, and South Africa. The first four were initially grouped as "BRIC" (or "the BRICs") in 2001 by Goldman Sachs economist Jim O'Neill, who coined the term to describe fast-growing economies that would collectively dominate the global economy by 2050; South Africa was added in 2010.

The BRICS have a combined area of 39,746,220 km2 (15,346,100 sq mi) and an estimated total population of about 3.21 billion, or about 26.7% of the world's land surface and 41.5% of the global population. Brazil, Russia, India, and China are among the world's ten largest countries by population, area, and GDP, and the latter three are widely considered to be current or emerging superpowers. All five states are members of the G20, with a combined nominal GDP of US$26.6 trillion (about 26.2% of the gross world product), a total GDP (PPP) of around US$51.99 trillion (32.1% of global GDP PPP), and an estimated US$4.46 trillion in combined foreign reserves (as of 2018).[1]

The last few years have been very critical for the BRICS nations as they have expanded, gained more recognition and allies. They also brought forth the idea of a BRICS currency backed by Gold, 26% Oil, 40% Corn, 46% Wheat, 3.21B People, and 5+ Powerful Nations. This currency will be used as a medium for financial transactions. Eventhought this is a good idea, it does not still solve FIAT money problem because the BRICS Currency will just be like any other FIAT currency existing.

Introducing BRICS Chain which in 1 phrase describes itself as “BRICS on The Blockchain”. We believe the Bitcoin blockchain is a better technology for transacting, storing, and accounting for these assets. There exists a vast array of crypto-assets in the world which people freely choose as a store of value, a transactional medium, or an investment.

Cryptocurrencies(Bitcoin) was created as “an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.”[2]. Bitcoin, Ethereum, etc created a new class of digital currency, a decentralized digital currency or cryptocurrency.

Some of the primary advantages of cryptocurrencies are: low transaction costs, international borderless transferability and convertibility, trustless ownership and exchange, pseudo anonymity, real time transparency, and immunity from legacy banking system problems [3].

Common explanations for the current limited mainstream use of cryptocurrencies include: volatile price swings, inadequate mass market understanding of the technology, and insufficient ease of use for non technical users.

The idea for asset pegged cryptocurrencies was initially popularized in the Bitcoin community by the Mastercoin white paper authored by J.R. Willett in January 2012[4]. Today, we're starting to see these ideas built with the likes of BitAssets, Ripple, Omni, Nxt, NuShares/Bits, Tether and others.

This means that the BRICS Chain is going to be pegged to the BRICS fiat currency and all exchanges and wallets which will allow you to hold BRICS Chain currency will provide a similar service in that users can avoid the volatility (or other traits) of a particular cryptocurrency by selling them for BRICS Chain, gold, or another asset.

Further, almost all types of existing financial institutions, payment providers, etc, which allow you to hold fiat value (or other assets) subsequently provide a similar service. In this white paper we focus on applications wherein the value of BRICS Chain is stored and transmitted with software that is open source, cryptographically secure, and uses distributed ledger technology, i.e. a true cryptocurrency.

While the goal of any successful cryptocurrency is to completely eliminate the requirement of trust, each of the aforementioned implementations either rely on a trusted third party or have other technical, market based, or process based drawbacks and limitations.

In our solution, BRICS pegged cryptocurrencies are called "$BRICS". All $BRICS will initially be issued on an EVM-compatible blockchain and so they exist as a cryptocurrency token. Each $BRICS unit issued into circulation is backed in a one to one ratio (i.e. one $BRICS is one BRICS) by the corresponding fiat currency unit. $BRICS may be redeemable/exchangeable for the underlying fiat currency pursuant to BRICS Chain Limited's terms of service or, if the holder prefers, the equivalent spot value in the respective EVM network coin. Once a $BRICS has been issued, it can be transferred, stored, spent, etc just like Bitcoins or any other cryptocurrency.

The fiat currency on reserve has gained the properties of a cryptocurrency and its price is permanently synced to the price of the fiat currency. Our implementation has the following advantages over other fiat pegged cryptocurrencies:

- $BRICS exist on stable EVM blockchains, later it's own network rather than a less developed/tested "altcoin" blockchain nor within closed source software running on centralized, private databases.
- $BRICS can be used just like any other cryptocurrency, i.e. in a p2p, pseudo anonymous, decentralized, cryptographically secure environment.
- $BRICS can be integrated with merchants, exchanges, and wallets just as easily as any other cryptocurrencies can be integrated.
- $BRICS inherit the properties of the EVM Network protocol which include: a decentralized exchange; browser based, open source, wallet encryption; blockchain based transparency, accountability, multi party security and reporting functions.
- BRICS Chain employs a simple but effective approach for conducting Proof of Reserves which significantly reduces our counterparty risk as the custodian of the reserve assets.
- $BRICS issuance or redemption will not face any pricing or liquidity constraints. Users can buy or sell as many $BRICS as they want, quickly, and with very low fees.
- $BRICS will not face any market risks such as Black Swan events, liquidity crunches, etc as reserves are maintained in a one to one ratio rather than relying on market forces.
- $BRICS one to one backing implementation is easier for non technical users to understand as opposed to collateralization techniques or derivative strategies.

At any given time the balance of fiat currency held in our reserves will be equal to (or greater than) the number of $BRICS in circulation. This simple configuration most easily supports a reliable Proof of Reserves process; a process which is fundamental to maintaining the price parity between $BRICS in circulation and the underlying fiat currency held in reserves. In this paper we provide evidence that shows exchange and wallet audits (in their current state) are very unreliable (i.e. flaws in Proof of Solvency[6] methods) and instead propose that exchanges and wallets outsource the custody of user funds to us via $BRICS.

Users can purchase $BRICS from https://wallet.bricschain.io (our web wallet) or from supported exchanges who support $BRICS as a deposit and withdrawal method. Users can also transact and store $BRICS on any EVM Network Blockchain ofcourse using bridges to migrate from one network to another. Other exchanges, wallets, and merchants are encouraged to reach out to us about integrating $BRICS as a surrogate for traditional fiat payment methods.

We recognize that our implementation isn't perfectly decentralized since BRICS Chain must act as a centralized custodian of reserve assets (albeit $BRICS in circulation exist as a decentralized digital currency). However, we believe this implementation sets the foundation for building future innovations that will eliminate these weaknesses, create a robust platform for new products and services, and support the growth and utility of the blockchain technology over the long run.

Some of these innovations include:

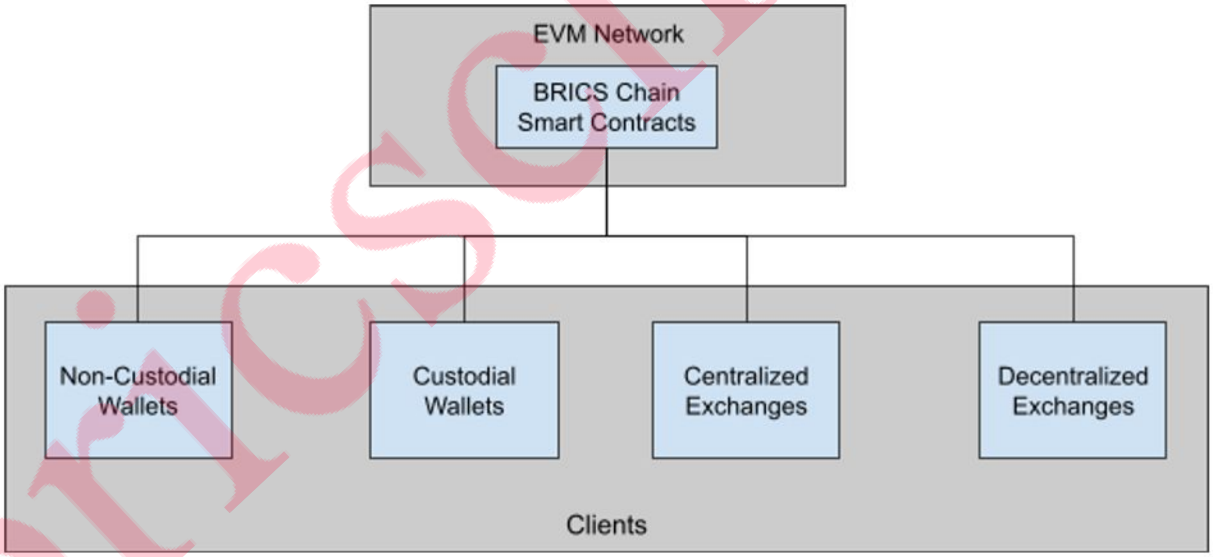
- Mobile payment facilitation between users and other parties, including other users and merchants , and Instant or near instant fiat value transfer between decentralized parties (such as multiple exchanges).
- Multi signature capabilities to further improve the general security process, Proof of Reserves, and enable new features.

Technology Stack and Processes

Each $BRICS issued into circulation will be backed in a one to one ratio with the equivalent amount of corresponding fiat currency held in reserves by BRICS Chain. As the custodian of the backing asset we are acting as a trusted third party responsible for that asset.

This risk is mitigated by a simple implementation that collectively reduces the complexity of conducting both fiat and crypto audits while increasing the security, provability, and transparency of these audits.

Technology Stack

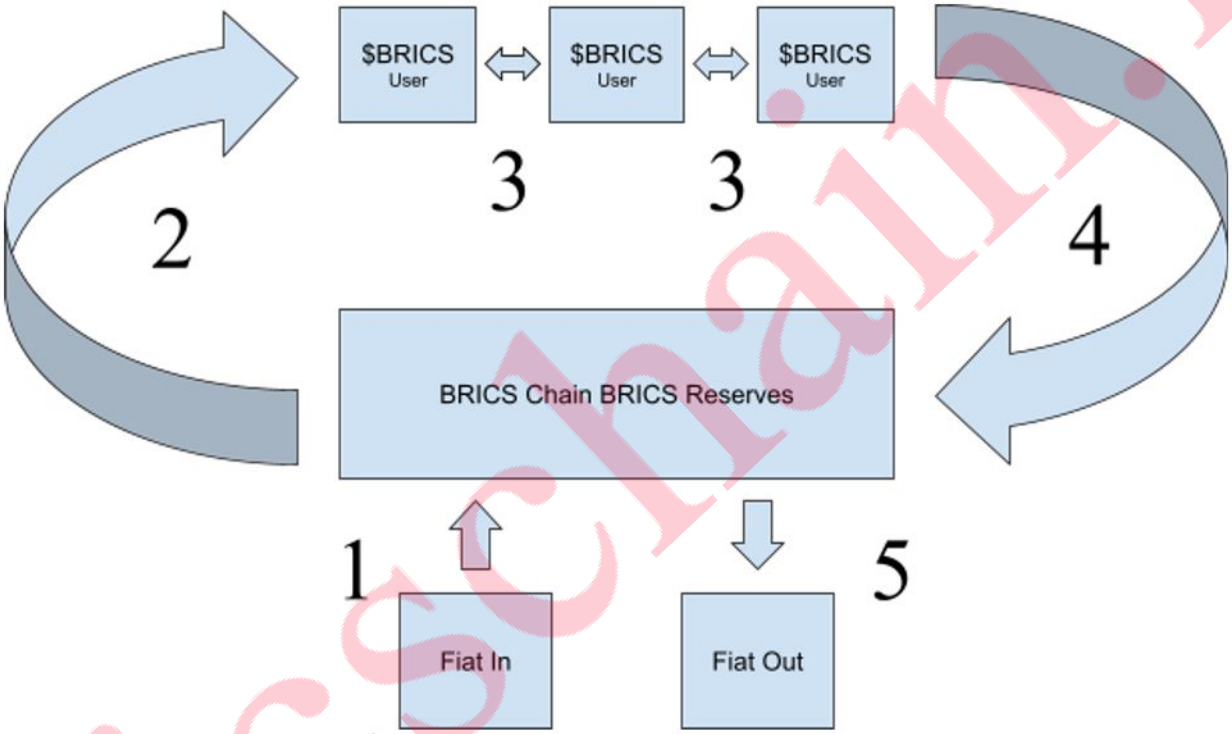


Here is a review of each layer;

- **The EVM Network Blockchain**: Serves as the blockchain hosting the BRICS Chain smart contracts.
- **BRICS Chain Smart Contracts**: The set of smart contract applications running all the operations of The BRICS Chain, $BRICS, NFT, DeFI, DePETRO, etc.
- **Clients**: These are users who own custodial wallets and non-custodial wallets, both centralized exchanges and decentralized exchanges who interact with the BRICS Chain Smart Contracts.

Flow of Funds Process

There are five steps in the lifecycle of a $BRICS, best understood via a diagram.



- **Step 1**: User deposits fiat currency into BRICS Chain Reserves via web wallet https://wallet.bricschain.io
- **Step 2**: BRICS Chain generates and credits the user's $BRICS account. $BRICS enter circulation. Amount of fiat currency deposited by user = amount of $BRICS issued to user (i.e. 10k BRICS deposited = 10k $BRICS issued).
- **Step 3:** Users transact with $BRICS. The user can transfer, exchange, and store $BRICS via a p2p, open source, pseudo anonymous, EVM based network.
- **Step 4**: The user deposits $BRICS with BRICS Chain for redemption into fiat currency.
- **Step 5**: BRICS Chain destroys the $BRICS and sends fiat currency to the user's bank account.

Users can obtain $BRICS outside of the afore mentioned process via an exchange or another individual. Once a $BRICS enters circulation it can be traded freely between any business or individual.

For example: Users can purchase $BRICS from the web wallet, with more exchanges to follow soon. The main concept to be conveyed by the Flow of Funds diagram is that BRICS Chain is the only party who can issue $BRICS into circulation (create them) or take them out of circulation (destroy them). This is the main process by which the system solvency is maintained.

Proof of Reserves Process

Proof of Solvency, Proof of Reserves, Real Time Transparency, and other similar phrases have been growing and resonating across the cryptocurrency industry.

Exchange and wallets audits, in their current form, are very unreliable. Insolvency has occurred numerous times in the cryptocurrency ecosystem, either via hacks, mismanagement, or outright fraud. Users must be diligent with their exchange selection and vigilant in their use of exchanges. Even then, a savvy user will not be able to fully eliminate the risks. Further, there are exchange users like traders and businesses who must keep non trivial fiat balances in exchanges at all times. In financial language, this is known as the "counterparty risk" of storing value with a third party.

We believe it's safe to conclude that exchange and wallet audits in their current form are not very reliable. These processes do not guarantee users that a custodian or exchange is solvent. Although there have been great contributions to improving the exchange audit processes, like the Merkle tree approach[6], major flaws still remain.

BRICS Chain's Proof of Reserves configuration is novel because it simplifies the process of proving that the total number of $BRICS in circulation (liabilities) are always fully backed by an equal amount of fiat currency held in reserve (assets). In our configuration, each $BRICS in circulation represents 1 BRICS held in our reserves (i.e. a one to one ratio) which means the system is fully reserved when the sum of all $BRICS in existence (at any point in time) is exactly equal to the balance of BRICS held in our reserve. Since $BRICS live on the blockchain, the provability and accounting of $BRICS at any given point in time is trivial.

Conversely, the corresponding total amount of BRICS held in our reserves is proved by publishing the bank balance and undergoing periodic audits by professionals. Find this implementation further detailed below:

- BRICS Chain issues all $BRICS via an EVM Network protocol as smart contracts. Smart contracts run on the blockchain and therefore all issued, redeemed, and existing $BRICS,

including transactional history, are publicly auditable via the tools provided at the respective EVM Networks scan page.
- Each $BRICS token will only exist on one network at any given time. This means the amount of $BRICS in circulation is the sum of $BRICS on all networks issued by BRICS Chain.
- BRICS Chain which will receive and send fiat currency to users who purchase/redeem $BRICS directly with us.
- Each $BRICS issued will be backed by the equivalent amount of currency unit (one $BRICS equals one BRICS). By combining the above crypto and fiat accounting processes, we conclude the "Solvency Equation" for the $BRICS System.

For clarity, we'd like to acknowledge that the $BRICS System is different than the https://wallet.bricschain.io web wallet in terms of Proof of Reserves. In this paper, we mostly focus on Proof of Reserves for the $BRICS System; i.e. all $BRICS in circulation at any point in time.

The https://wallet.bricschain.io wallet is a consumer facing web wallet operating on closed source code and centralized servers. Conducting a Proof of Reserves for this wallet is fundamentally different than what we've outlined for the $BRICS System. We're planning the deployment of a PoR based transparency solution for the https://wallet.bricschain.io wallet. We believe it will be the most advanced PoR system in existence today. It overcomes almost all of the challenges outlined in the appendix on this topic. Mind you, users can always secure $BRICS through managing the private keys themselves through a non-custodial wallet and handle trades on a decentralized exchange.

Implementation of Weakness

We understand that our implementation doesn't immediately create a fully trustless cryptocurrency system. Mainly because users must trust BRICS Chain and our corresponding legacy banking institution to be the custodian of the reserve assets. However, almost all exchanges and wallets (assuming they hold BRICS/fiats) are subject to the same weaknesses. Users of these services are already subject to these risks. Here is a summary of the weaknesses in our approach:

- We could go bankrupt.
- Our bank could go insolvent.
- Our bank could freeze or confiscate the funds.
- We could abscond with the reserve funds.

- Re-centralized of risk to a single point of failure.

Observe that almost all digital currency exchanges and wallets (assuming they hold BRICS/fiat) already face many of these challenges. Therefore, users of these services are already subject to these risks. Below we describe how each of these concerns are being addressed.

We could go bankrupt

In this case, the business entity BRICS Chain would go bankrupt but client funds would be safe, and subsequently, all $BRICS will remain redeemable. Most security breaches on the financial businesses have targeted cryptocurrencies rather than bank accounts. Since all $BRICS exist on the blockchain they can be stored by individuals directly through securing their own private keys.

Our bank could go insolvent

This is a risk faced by all users of the legacy financial system and by all exchange operators. BRICS Chain currently has accounts with banks, whom are aware and confident that BRICS Chain business model is acceptable. Additional banking partners are being established in other jurisdictions to further mitigate this concern.

Our bank could freeze or confiscate the funds

Our banks are aware of the nature of cryptocurrencies and are accepting of cryptocurrency businesses. They also provide banking services to some of the largest exchanges globally. The KYC/AML processes we follow are also used by the other digital currency exchanges they currently bank. They have assured us we are in full compliance. These banks also abide to laws of the country in which they reside or belong to.

We could abscond with the reserve assets

The corporate charter is public as well as the business owners names, locations, and reputations. Ownership of the account is legally bound to the corporate charter. Any transfers in or out of the bank account will have the associated traces and are bound by rigid internal policies.

Re-centralization of risk to a single point of failure

We have some ideas on how to overcome this and we'll be sharing them in upcoming blog and product updates. There are many ways to tackle this problem. For now, this initial implementation gets us on the right track to realize these innovations in following versions. By leveraging the platforms we have chosen, we have reduced the centralization risk to one singular responsibility: the creation and redemption of tokens. All other aspects of the system are decentralized.

Main Applications

In this section we'll summarize and discuss the main applications of $BRICS across the blockchain/cryptocurrency ecosystem and for other consumers globally. We break up the beneficiaries into three user groups: Exchanges, Individuals, and Merchants.

The main benefits, applicable to all groups:

- Properties of cryptocurrency bestowed upon other asset classes.
- Less volatile, familiar unit of account.
- World's assets migrate to the cryptocurrency blockchain.

For Exchanges

Exchange operators understand that accepting fiat deposits and withdrawals using legacy financial systems can be complicated, risky, slow, and expensive. Some of these issues include:

- Identifying the right payment providers for your exchange
  - Irreversible transactions, fraud protection, lowest fees, etc.
- Integrating the platform with banks who have no APIs.
- Liaising with these banks to coordinate compliance, security, and to build trust.
- Prohibitive costs for small value transfers.
- 3 7 days for international wire transfers to clear.
- Poor and unfavorable currency conversion fees.

By offering $BRICS, an exchange can relieve themselves of the above complications and gain additional benefits, such as:

- Accept crypto fiats as deposit/withdrawal/storage method rather than using a legacy bank or payment provider.
  - Allows users to move fiat in and out of exchange more freely, quickly, cheaply.
- Outsource fiat custodial risk to BRICS Chain just manage cryptos.
- Easily add other pegged fiat currencies as trading pairs to the platform.
- Secure customer assets purely through accepted crypto processes.
  - Multi signature security, cold and hot wallets, HD wallets, etc
  - Conduct audits easier and more securely in a purely crypto environment
- Anything one can do with cryptocurrencies as an exchange can be done with $BRICS.

Exchange users know how risky it can be to hold fiat currencies on an exchange. With the growing number of insolvency events it can be quite dangerous. As mentioned previously, we believe that using $BRICS exposes exchange users to less counterparty risk than continually holding fiat on exchanges. Additionally, there are other benefits to holding $BRICS, explained in the next section.

For Individuals

There are many types of individual cryptocurrency users in the world today, like;

- From traders looking to earn profits daily.
- Tto long term investors looking to store their cryptocurrency securely.
- To tech savvy shoppers looking to avoid credit card fees or maintain their privacy.
- To philosophical users looking to change the world.
- To those looking to remit payments globally more effectively.
- To those in third world countries looking for access to financial services for the first time.
- To developers looking to create new technologies.
- To all those who have found many uses for cryptocurrencies.

For each of these individuals, we believe $BRICS are useful in similar ways, like:

- Transact in BRICS/fiat value, pseudo anonymously, without any middlemen/intermediaries.
- Cold store BRICS/fiat value by securing one's own private keys.
- Avoid the risk of storing fiat on exchanges move crypto fiat in and out of exchanges easily.
- Avoid having to open a fiat bank account to store fiat value.
- Easily enhance applications that work with cryptocurrencies to also support $BRICS.
- Anything one can do with a cryptocurrency as an individual one can also do with $BRICS.

For Merchants

Merchants want to focus on their business, not on payments. The lack of global, inexpensive, ubiquitous payment solutions continue to plague merchants around the world both large and small. Merchants deserve more. Here are some of the ways $BRICS can help them:

- Price goods in BRICS/fiat value rather than other cryptocurrencies (no moving conversion rates/purchase windows).
- Avoid conversion from other cryptocurrencies to BRICS/fiat and associated fees and processes.
- Prevent chargebacks, reduce fees, and gain greater privacy.
- Provide novel services because of fiat crypto features.
    - Microtipping, gift cards, more.
- Anything one can do with other cryptocurrencies as a merchant one can also do with $BRICS.

Future Innovations

Multi Sig

Own Blockchain

Proof of Solvency Innovations

Improve Privacy

Conclusion

$BRICS constitutes the first EVM based fiat pegged cryptocurrencies in existence today. $BRICS is based on the EVM blockchain, one of the most secure and well tested blockchain and public ledger in existence. $BRICS are fully reserved in a one to one ratio, completely independent of market forces, pricing, or liquidity constraints. $BRICS has a simple and reliable Proof of Reserves implementation and undergoes regular professional audits. Our underlying banking relationships, compliance, and legal structure provide a secure foundation for us to be the custodian of reserve assets and issuer of $BRICS. Our team is composed of experienced and respected entrepreneurs from the cryptocurrency ecosystem and beyond.

Since we are focused on making BRICS Chain better everyday this white paper my be subjected to updates. We are also making arranging integrations with existing businesses in the cryptocurrency space. Business like exchanges, wallets, merchants, and others. Please reach out to us at **contact@bricschain.io** to find out more.

Appendix

Audit Flaws: Exchanges and Wallets

Here is a summary of the current flaws found in technology based exchange and wallet audits. In the Merkle tree approach users must manually report that their balances (user's leaf) have been correctly incorporated in the liability declaration of the exchange (the Merkle hash of the exchange's database of user balances). This proposed solution works if enough users verify that their account was included in the tree, and in a case where their account is not included this instance would be reported. One potential risk is that an exchange database owner could produce a hash that is not the true representation of the database at all; it hashes an incomplete database which would reduce its apparent liabilities to customers, making them appear solvent to a verifying party. Here are some scenarios where a fraudulent exchange would exclude accounts and:

"Bitdust" Accounts
Inactive or low activity accounts would lower the chance that an uninterested user would check or report inconsistencies. In some cases these long tail accounts could represent a significant percentage of the exchange's liabilities.

"Colluding Whales" Attack
There is evidence that large cryptocurrency traders are operating on various exchanges and moving markets significantly. Such traders need to have capital reserves at the largest exchanges to quickly execute orders. Often, traders choose exchanges that they "trust". In this way they can be assured that should a hack or liquidity issue arise, they have priority to get their money out. In this case, the exchange and trader could collude to remove the whales account balance from the database before it's hashed.

Key Rental Attack
To pass the audit, a malicious exchange could rent the private keys to cryptocurrencies they do not own. This would make them appear solvent by increasing their assets without any acknowledgment that those funds were loaned to them. Likewise, they could "borrow" fiat currency to do the same.

There are more attacks not discussed here.

Reaching Statistical Significance (reporting completeness): Even outside of these three attack vectors, a database that has been manipulated may never be detected if a sufficient number of users are not validating balances. The probability of getting 100% of the users to verify balances is likely zero, even with proper incentivization structure for users to verify their balances.

Therefore, auditors would need statistical tools to make statements about the validity of an exchange's database based on sampling frequency, size, and other properties. Currently users have no way to receive compensation by legal means in case something goes wrong with the exchange.

For example, when Mt.Gox closed operations, many users might not have independently recorded their account balances (prints screens, signed messages to themselves, etc) in a way that could conclusively prove to law enforcement that this exchange's I.O.U's actually existed. Such users are at the mercy of the exchange to somehow publish a record of that hash tree or original database. The proposed structure in which these audits would be performed still contains some subtle but important flaws. In particular, the data reporting (hash tree) on the institution's website gives no guarantee at all to users, as a malicious exchange could publish different states/balances to different groups of users, or retroactively change the state. Thus it is fundamental to publish this data through a secure broadcast channel, e.g. the blockchain.

Privacy is a barrier to entry for the adoption of an automated/open auditing system. While some progress has been made towards better privacy there is no perfect solution yet. Further, to build up an accurate user verified liability space, these users will have to report account balances with the exchange and addresses. Some users likely would not report this information regardless of the incentive, therefore providing cryptographically secure privacy whilst obtaining the reporting goal is paramount.

Time Series

The Merkle tree hash is a single snapshot of the database at a single point in time. Not having a somewhat continuous time series of the database opens significant attack vectors. Additionally, a time series of user reported information would also be required for piecing together the history of any reported incidents of fraud.

Trusted Third Parties

All of the current exchange audits have relied on some "reputable" trusted third party to make some type of verification. In the Coinbase audit [7], that was Andreas Antonopoulos, in the Kraken audit [8], that was Stefan Thomas. If we absolutely must rely on a trusted third party then some audit standards and procedures should ensure this weaknesses is fortified.

Limitations of Existing Fiat pegging Systems

Here's a list of some of the common drawbacks and limitations of existing fiat pegging systems.

- The systems are based on closed source software, running on private, centralized databases, fundamentally no different than Paypal or any other existing mass market retail/institutional asset trading/transfer/storage system.
- Decentralized systems that rely on altcoin blockchains which haven't been stress tested, developed, or reviewed as closely as other blockchains, like ETH, BSC.
- Pegging processes that rely on hedging derivative meta assets, efficient market theory, or collateralization of the underlying asset, wherein liquidity, transferability, security, and other issues can exist.
- Lack of transparency and audits for the custodian, either crypto, fiat, or relating to their own internal ledgers (same as closed source and centralised databases).
- Reliance on legacy banking systems and trusted third parties (bank account owners) as a transfer and settlement mechanism for reserve assets.

Market Risk Examples

In the collateralization method, market risk exists because the price of the asset being used as collateral can move in an adverse direction to the price of the asset it's backing/pegging. This would cause the total value of the collateral to become less than the total value of the issued asset and make the system insolvent. This risk is mitigated by the custodian closing the position before this happens; that is, when the collateral price equals the pegged asset price then the collateral is liquidated (sold on the open market) and the position is closed. A great approach, with merit, and used in many liquid markets across the traditional banking and financial markets.

However, as we saw from the global financial crisis, situations can arise in which the acceleration of such events causes a "liquidity crunch" and thus the collateral is unable to be liquidated fast enough to meet trading obligations, subsequently creating losses. With the cryptocurrency markets being so small and volatile, this type of event is much more likely.

Additionally, the overall approach suffers from other liquidity and pricing constraints since there must be a sufficient supply of users posting collateral for the creation of the pegged assets to exist in the first place. In the derivatives approach, the price of the asset is pegged through entering one of several derivatives strategies, such as: swap strategies, covered and naked

options strategies, various futures and forwards strategies. Each strategy has their own strengths and weaknesses, the discussion of which we won't engage in here.
To summarize, each of these pegging processes themselves have similar "market risk" characteristics as the aforementioned collateralization method. It should be noted that the two methods are not mutually exclusive and often paired in a specific trading, hedging, or risk management function at legacy system financial institutions.

Finally, understand that we believe some combination of the above approaches may become a secure, reliable, and generally risk free process for backing/pegging assets; however, at this point in time, this is not a direction we feel is feasible to take to ensure liquidity and price stability.

Further, we believe that a reserve based approach will always be in existence and complement these other approaches as the entire industry grows. As advances in technology continue, we will evaluate and incorporate any benefits available while maintaining the guarantee of 100% redeemability.

Glossary of Terms

- **Digital currency**: As defined by http://en.wikipedia.org/wiki/Digital_currency
- **Cryptocurrency or decentralized digital currency**: any type of cryptocurrency that is open source, cryptographically secure, and uses a distributed ledger. See: http://en.wikipedia.org/wiki/Cryptocurrency
- **Real world currency, or fiat currency, or national/sovereign currency**: all types of currency that are not cryptocurrencies as defined above.
- **Cryptocurrency system**: A collection of software and processes primarily created to enable the existence of a cryptocurrency.
- **Legacy financial system**: any financial system that is not a cryptocurrency system.
- **Utility backed digital tokens, a.k.a Dapps**: A decentralized digital token whose value is derived from the usefulness of its application rather than just being a value transfer system. Asset backed/pegged cryptocurrency: Any cryptocurrency whose price is pegged to a real world asset, i.e. its not a "utility backed" cryptocurrency.
- $BRICS(s): a single unit (or multiple units) of fiat pegged cryptocurrency issued by BRICS Chain.
- $BRICS System: collectively refers to all process and technologies that enable $BRICS to exist.
- **Proof of Reserves**: The process by which the issuer of any asset backed decentralized digital token, cryptographically/mathematically proves that all tokens that have been issued are fully reserved and backed by the underlying asset.

Reference

[1] Wikipedia: https://en.wikipedia.org/wiki/BRICS

[2] https://bitcoin.org/bitcoin.pdf

[3]http://www.deloitte.com/assets/Dcom UnitedStates/Local%20Assets/Documents/FSI/us_fsi_BitcointheNewGoldRush_031814.pdf

[4] https://github.com/mastercoin MSC/spec

[5] http://unenumerated.blogspot.com/2005/12/bit gold.html

[6] https://iwilcox.me.uk/2014/proving bitcoin reserves

[7] http://antonopoulos.com/2014/02/25/coinbase review/

[8] http://www.coindesk.com/krakens audit proves holds 100 bitcoins reserve/