Tether 白皮书：利用比特币区块链交易的法币

摘要：

Tether 是一种代币，为组织或者个人在进行价值交换时，以熟悉的记帐单位，及去中心化加密货币便利。区块链是一个易于审计且通过密码学保障其不被修改的帐本。资产抵押代币的发行者及其它市场参与者都可以利用区块链技术的便利，以及其内置的共识机制，来交易他们所熟悉且波动性小的货币及资产。为了维持可审计性及交易价格的稳定，我们提出了一种代币，称为 **tether**，这种代币与真实世界资产或法币保持 **1:1** 的比例。代币的发行及交易使用了比特币区块链，储备证明（**Proof of Reserves**）及其它审计手段，来证明所发行的代币在任何时候都得到了完全的抵押。

注：本白皮书仅翻译了摘要部分，欢迎到巴比特社区分享读后心得。miner@8btc.com

Tether: Fiat currencies on the Bitcoin blockchain

Abstract. A digital token backed by fiat 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 tethers, and its associated real-world asset, fiat currency. This method uses the Bitcoin blockchain, Proof of Reserves, and other audit methods to prove that issued tokens are fully backed and reserved at all times.

Table of Contents

Introduction

There exists a vast array of assets in the world which people freely choose as a store-of-value, a transactional medium, or an investment. We believe the Bitcoin blockchain is a better technology for transacting, storing, and accounting for these assets. Most estimates measure global wealth around 250 trillion dollars [1] with much of that being held by banks or similar financial institutions. The migration of these assets onto the Bitcoin blockchain represents a proportionally large opportunity.

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 created a new class of digital currency, a decentralized digital currency or cryptocurrency[1].

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[2] 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, and others. One should note that all Bitcoin exchanges and wallets (like Coinbase, Bitfinex, and Coinapult) which allow you to hold value as a fiat currency already provide a *similar* service in that users can avoid the volatility (or other traits) of a particular cryptocurrency by selling them for fiat currency, 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 fiat value 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[3].

[1] For definitions throughout, see Glossary of Terms
[2] But has been discussed since Dr. Szabo's proposed BitGold [5]
[3] Summarized in the Appendix, here: Limitations of Existing Fiat-pegging Systems

In our solution, fiat-pegged cryptocurrencies are called “tethers”. All tethers will initially[4] be issued on the Bitcoin blockchain via the Omni Layer protocol and so they exist as a cryptocurrency token. Each tether unit issued into circulation is backed in a one-to-one ratio (i.e. one tetherUSD is one US dollar) by the corresponding fiat currency unit held in deposit by Hong Kong based Tether Limited. Tethers are fully redeemable/exchangeable at any time for the underlying fiat currency or, if the holder prefers, the equivalent spot value in Bitcoin. Once a tether 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 *tethered* to the price of the fiat currency.

Our implementation has the following advantages over other fiat-pegged cryptocurrencies:

- Tethers exist on the Bitcoin blockchain rather than a less developed/tested “altcoin” blockchain nor within closed-source software running on centralized, private databases.
- Tethers can be used just like bitcoins, i.e. in a p2p, pseudo-anonymous, decentralized, cryptographically secure environment.
- Tethers can be integrated with merchants, exchanges, and wallets just as easily as Bitcoin or any other cryptocurrencies can be integrated.
- Tethers inherit the properties of the Omni Layer protocol which include: a decentralized exchange; browser-based, open-source, wallet encryption; Bitcoin-based transparency, accountability, multi-party security and reporting functions.
- Tether Limited employs a simple but effective approach for conducting Proof of Reserves which significantly reduces our counterparty risk as the custodian of the reserve assets.
- Tether issuance or redemption will not face any pricing or liquidity constraints. Users can buy or sell as many tethers as they want, quickly, and with very low fees.
- Tethers will not face any market risks[5] such as Black Swan events, liquidity crunches, etc as reserves are maintained in a one-to-one ratio rather than relying on market forces.
- Tether’s 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 tethers 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 tethers in circulation and the underlying fiat currency held in reserves. In this paper we provide evidence[6] that shows exchange and

[4] More Bitcoin 2.0 protocols will come soon, like Ripple, Nxt, etc
[5] See Appendix, section: Market Risk Examples
[6] See section: Proof of Solvency Process

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 tethers.

Users can purchase tethers from Tether.to (our web-wallet) or from supported exchanges such as Bitfinex who support tethers as a deposit and withdrawal method. Users can also transact and store tethers with any Omni Layer enabled wallet like Holy Transaction or Omni Wallet. Other exchanges, wallets, and merchants are encouraged to reach out to us about integrating tether as a surrogate for traditional fiat payment methods.

We recognize that our implementation isn't perfectly decentralized[7] since Tether Limited must act as a centralized custodian of reserve assets (albeit tethers 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 Bitcoin blockchain over the long run. Some of these innovations include:

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

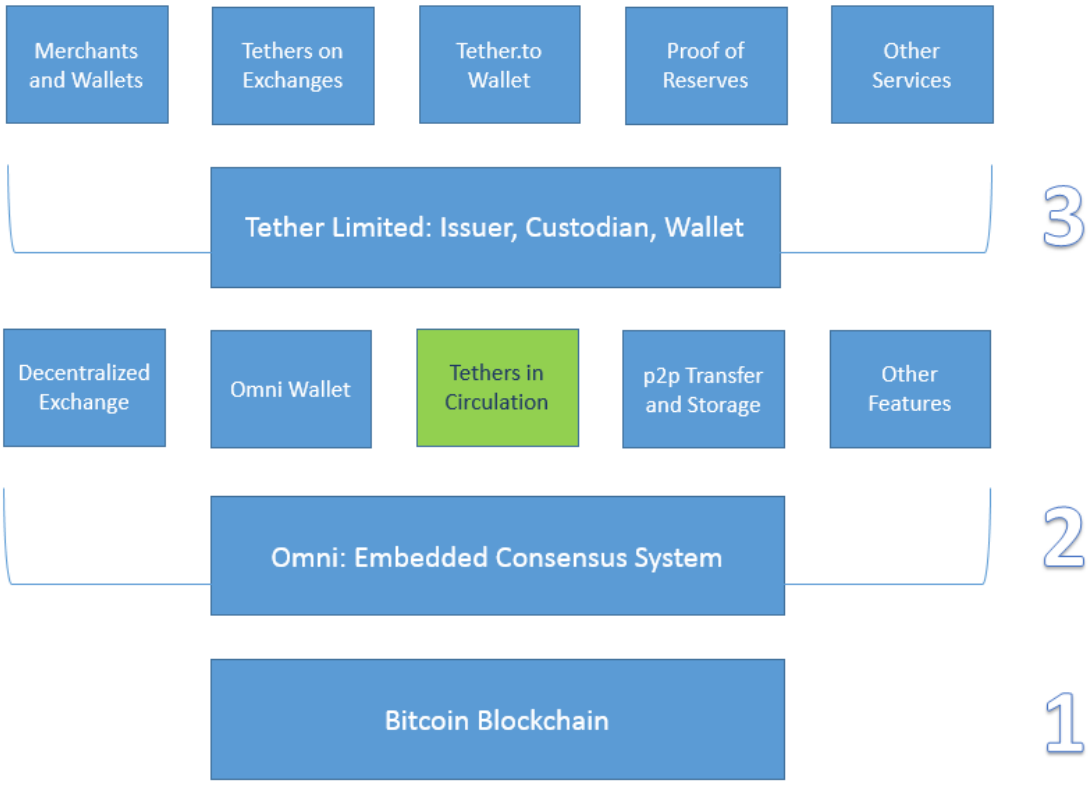
Technology Stack and Processes

Each tether issued into circulation will be backed in a one-to-one ratio with the equivalent amount of corresponding fiat currency held in reserves by Hong Kong based Tether Limited. 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.

Tether Technology Stack

The stack has 3 layers, and numerous features, best understood via a diagram

[7] See section: Implementation Weaknesses



Here is a review of each layer.

1) The first layer is the Bitcoin blockchain. The Tether transactional ledger is embedded in the Bitcoin blockchain as meta-data via the embedded consensus system, Omni.

2) The second layer is the Omni Layer protocol. Omni is a foundational technology that can:
    a) Grant (create) and revoke (destroy) digital tokens represented as meta-data embedded in the Bitcoin blockchain; in this case, fiat-pegged digital tokens, tethers.
    b) Track and report the circulation of tethers via Omnichest.info (Omni asset ID #31, for example, represents TetherUSD) and Omnicore API.
    c) Enable users to transact and store tethers and other assets/tokens in a:
        i) p2p, pseudo-anonymous, cryptographically secure environment.
        ii) open-source, browser-based, encrypted web-wallet: Omni Wallet.
        iii) multi-signature and offline cold storage-supporting system

3) The third layer is Tether Limited, our business entity primarily responsible for:
    a) Accepting fiat deposits and issuing the corresponding tethers
    b) Sending fiat withdrawals and revoking the corresponding tethers
    c) Custody of the fiat reserves that back all tethers in circulation

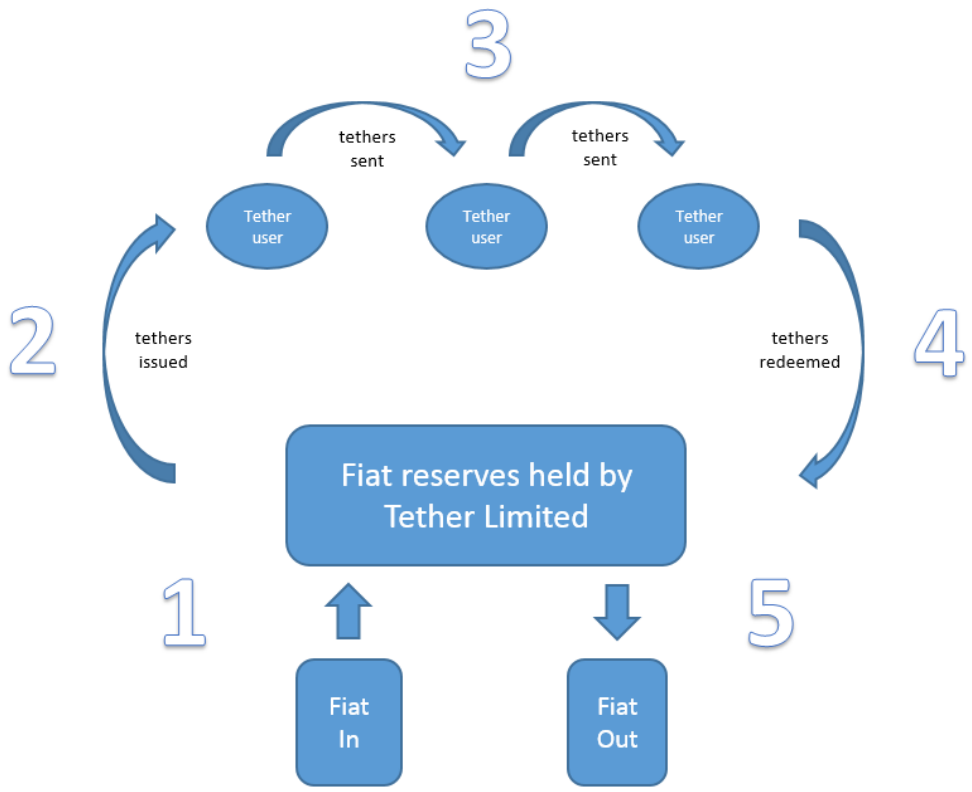
d) Publicly reporting Proof of Reserves and other audit results

e) Initiating and managing integrations with existing Bitcoin/blockchain wallets, exchanges, and merchants

f) Operating Tether.to, a web-wallet which allows users to send, receive, store, and convert tethers conveniently.

Flow of Funds Process

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



Step 1 - User deposits fiat currency into Tether Limited's bank account.

Step 2 - Tether Limited generates and credits the user's tether account. Tethers enter circulation. Amount of fiat currency deposited by user = amount of tethers issued to user (i.e. 10k USD deposited = 10k tetherUSD issued).

Step 3 - Users transact with tethers[8]. The user can transfer, exchange, and store tethers via a p2p open-source, pseudo-anonymous, Bitcoin-based platform.

Step 4 - The user deposits tethers with Tether Limited for redemption into fiat currency.

Step 5 - Tether Limited destroys the tethers and sends fiat currency to the user's bank account.

Users can obtain tethers outside of the aforementioned process via an exchange or another individual. Once a tether enters circulation it can be traded freely between any business or individual. For example, users can purchase tethers from Bitfinex, with more exchanges to follow soon.

The main concept to be conveyed by the Flow of Funds diagram is that Tether Limited is the only party who can issue tethers 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 Bitcoin 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 [9] still remain.

Tether's Proof of Reserves configuration is novel because it simplifies the process of proving that the total number of tethers in circulation (liabilities) are always fully backed by an equal amount of fiat currency held

[8] See benefits of using tethers in the section: Main Applications
[9] See section: Audit Flaws: Exchanges and Wallets

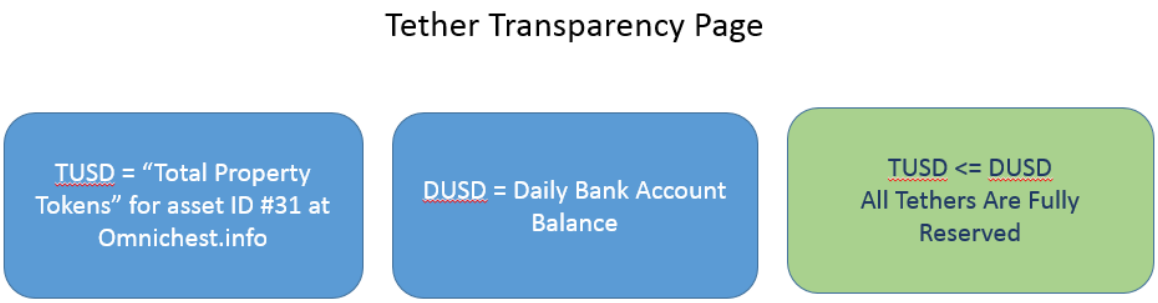
in reserve (assets). In our configuration, each tetherUSD in circulation represents one US dollar held in our reserves (i.e. a one-to-one ratio) which means the system is fully reserved when the sum of all tethers in existence (at any point in time) is exactly equal to the balance of USD held in our reserve. Since tethers live on the Bitcoin blockchain, the provability and accounting of tethers at any given point in time is trivial. Conversely, the corresponding total amount of USD held in our reserves is proved by publishing the bank balance and undergoing periodic audits by professionals. Find this implementation further detailed below:

- Tether Limited issues all tethers via the Omni Layer protocol. Omni operates on top of the Bitcoin blockchain and therefore all issued, redeemed, and existing tethers, including transactional history, are publicly auditable via the tools provided at Omnichest.info.
    - The Omnichest.info asset ID for tetherUSD is #31.
        - Here is a link: http://omnichest.info/lookupsp.aspx?sp=31
    - Let the total number of tethers issued under this asset ID be denoted as TUSDissue
    - Let the total number of tethers redeemed under this asset ID be denoted as TUSDredeem
    - Let the total number of tethers in circulation at any time be denoted as TUSD
        - TUSD = TUSDissue - TUSDredeem
        - TUSD = “Total Property Tokens” @ http://omnichest.info/lookupsp.aspx?sp=31

- Tether Limited has a bank account which will receive and send fiat currency to users who purchase/redeem tethers directly with us.
    - Let the total amount deposited into this account be denoted as DUSDdepo
    - Let the total amount withdrawn from this account be denoted as DUSDwithd
    - Let the dollar balance of this bank account be denoted as DUSD
        - DUSD = DUSDdepo - DUSDwithd

- Each tether issued will be backed by the equivalent amount of currency unit (one tetherUSD equals one dollar). By combining the above crypto and fiat accounting processes, we conclude the “Solvency Equation” for the Tether System.
    - The Solvency Equation is simply TUSD = DUSD.
    - Every tether issued or redeemed, as publicly recorded by the Bitcoin blockchain will correspond to a deposit or withdrawal of funds from the bank account.
    - The provability of TUSD relies on the Bitcoin blockchain as discussed previously.
    - The provability of DUSD will rely on several processes:
        - We publish the bank account balance on our website’s Transparency page.
        - Professional auditors will regularly verify, sign, and publish our underlying bank balance and financial transfer statement.

Users will be able to view this information from our Transparency Page, which will look like:



For clarity, we'd like to acknowledge that the Tether System[10] is different than the Tether.to web-wallet in terms of Proof of Reserves. In this paper, we mostly focus on Proof of Reserves for the Tether System; i.e. all tethers in circulation at any point in time. The Tether.to 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 Tether System.

We're planning the deployment of a PoR-based transparency solution for the Tether.to 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[11] on this topic. Mind you, users can always secure tethers through managing the private keys themselves or through Omni Wallet.

Implementation Weaknesses

We understand that our implementation doesn't immediately create a fully trustless cryptocurrency system. Mainly because users must trust Tether Limited and our corresponding legacy banking institution to be the custodian of the reserve assets. However, almost all exchanges and wallets (assuming they hold USD/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

[10] See Glossary of Terms
[11] See Audit Flaws: Exchanges and Wallets

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

Observe that almost all digital currency exchanges and wallets (assuming they hold USD/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 Tether Limited would go bankrupt but client funds would be safe, and subsequently, all tethers will remain redeemable. Most security breaches on Bitcoin businesses have targeted cryptocurrencies rather than bank accounts. Since all tethers exist on the Bitcoin 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. Tether Limited currently has accounts with Cathay United Bank and Hwatai Bank in Taiwan, both of whom are aware and confident that Tether's 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 Bitcoin and are accepting of Bitcoin businesses. They also provide banking services to some of the largest Bitcoin 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[12].

We could abscond with the reserve assets - The corporate charter is public[13] 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.

[12] See section on Legal and Compliance for more information
[13] Same as footnote #10

Main Applications

In this section we'll summarize and discuss the main applications of tethers across the Bitcoin/blockchain 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 Bitcoin bestowed upon other asset classes
- Less volatile, familiar unit of account
- World's assets migrate to the Bitcoin 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 tethers, 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 Tether Limited - just manage cryptos
- Easily add other tethered 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 Bitcoin as an exchange can be done with tethers

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 tethers exposes exchange users to less counterparty risk than continually holding fiat on exchanges. Additionally, there are other benefits to holding tethers, explained in the next section.

For Individuals

There are many types of individual Bitcoin users in the world today. From traders looking to earn profits daily; to long term investors looking to store their Bitcoins 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 Bitcoin. For each of these individuals, we believe tethers are useful in similar ways, like:

- Transact in USD/fiat value, pseudo-anonymously, without any middlemen/intermediaries
- Cold store USD/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 bitcoin to also support tether
- Anything one can do with Bitcoin as an individual one can also do with tether

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 tether can help them:

- Price goods in USD/fiat value rather than Bitcoin (no moving conversion rates/purchase windows)
- Avoid conversion from Bitcoin to USD/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 Bitcoin as a merchant one can also do with tether

Future Innovations

Multi-sig and Smart Contracts

Proof of Solvency Innovations

Conclusion

Tether constitutes the first Bitcoin-based fiat-pegged cryptocurrencies in existence today. Tether is based on the Bitcoin blockchain, the most secure and well-tested blockchain and public ledger in existence. Tethers are fully reserved in a one-to-one ratio, completely independent of market forces, pricing, or liquidity constraints. Tether 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 tethers. Our team is composed of experienced and respected entrepreneurs from the Bitcoin ecosystem and beyond.

We are focused on arranging integrations with existing businesses in the cryptocurrency space. Business like exchanges, wallets, merchants, and others. We're already integrated with Bitfinex, HolyTransaction, Omni Wallet, Poloniex, C-CEX, and more to come. Please reach out to us to find out more.

Appendix

Audit Flaws: Exchanges and Wallets

Here is a summary of the current flaws found in technology-based[14] exchange and wallet audits.

In the Merkle tree[6] 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

[14] As opposed to hiring a professional auditor

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 Bitcoin 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 bitcoins 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 Bitcoin 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 Bitcoin 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 Bitcoin.

- 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.

Legal and Compliance

Tether Limited ("Tether") is a limited company incorporated pursuant to the Hong Kong Companies Ordinance. It is wholly owned by Tether Holdings Limited, a BVI business company incorporated pursuant to the BVI Business Companies Act, 2004.

Tether is registered as a Money Services Business with the Financial Crimes Enforcement Network of the U.S. Department of the Treasury (MSB Registration Number 31000058542968). Tether is establishing a relationship with a U.S. financial institution for purposes of better servicing Tether users in the United States.

Tether is concluding a principal–agency agreement with RenRenBee Limited ("RenRenBee"). RenRenBee is licensed as a Money Services Operator by the Hong Kong Customs and Excise Department (Licence No. 13-09-01265). Pursuant to the agreement, RenRenBee will provide anti-money laundering compliance work and customer due diligence procedures as agent for Tether as principal.

Through these and other measures, Tether is undertaking customer due diligence, record-keeping, and reporting procedures consistent with U.S. law and with the Hong Kong Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance.

Tether Limited currently has accounts with Cathay Bank and Hwatai Bank in Taiwan, both of whom are aware and confident that Tether's business model is acceptable.

These banks are satisfied with our processes and also satisfied that our business operates in accordance with Taiwan off-shore banking regulations, as all of the banks had been requested to check this with their own legal, compliance and head-office before opening accounts (also at our own request). It was our goal from the beginning to have a compliant operation and to provide the maximum level of comfort to our banking partners here. In addition these banks have and are working with other Bitcoin based businesses.

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.

Tether(s): a single unit (or multiple units) of fiat-pegged cryptocurrency issued by Tether Limited

TetherUSD or tUSD: a single unit of crypto-USD issued by Tether Limited

TUSD: collective amount of tUSD in circulation at any point in time.

Tether System: collectively refers to all process and technologies that enable tethers 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.

References

[1] https://www.thefinancialist.com/wp-content/uploads/2012/10/2012-GlobalWealthReport-.pdf

[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/