 World Reserve System

The World’s most stable currency

Draft Version: 0.01.01

Author: Ramin Assisi, Computer Scientist

**Abstract**. A digital token backend by automatic money supply algorithms currency provides individuals and organizations with a robust and decentralized method of exchanging value while using a new coin that’s value is in a stable relation to familiar fiat-currencies. The innovation of blockchains is an auditable and cryptographically secured global ledger. Asset­backed 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 apply for a software algorithmic backed money supply out of a chain of secure treasury vaults. All tokens are premined and kept for the most parts in the treasury vaults. The transfer out of these treasury vaults will be only executed by mathematical formulars without human intervention. The underlaying technology make use of already well established technologies of the blockchain market.The maximum possible money supply will meet all the needs of human kind in the near as well as the far future.

# Table of Contents

Table of Contents 2

Introduction 3

The History of Crypto Currencies 6

**All of the World’s Money and Markets in One Visualization** 7

**All of the World’s Money and Markets in One Visualization** 7

How Much Money Exists? 7

A New Meaning 7

About the Money Project 7

Vision 8

Timeline and Milestones 9

Technology 10

Flow of Funds Process 13

Proof of Reserves Process 14

Implementation Weaknesses 18

For Exchanges 22

For Individuals 23

For Merchants 23

**Conclusion** 25

**Appendix** 26

Limitations of Existing Fiatpegging Systems 28

Market Risk Examples 29

Legal and Compliance 30

**Glossary of Terms** 31

**References** 34

# Introduction

There exists a vast array of assets in the world which people freely choose as a store­of­value, a transactional medium, or an investment. We believe the 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.

We further believe that the Blockchain Technology can revolutionize the way in general how high sensitive data can be stored.

When we use in this paper the term blockchain technology we mean all systems that use in full or in parts a distributed database to store data. There might be systems that do not use a blockchain to store data in the distributed database like for instance IOTA but for simplicity we use this term for all the distributed decentralized crypto currency systems.

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.

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

But on the other side common explanations for the current limited mainstream use of cryptocurrencies include: volatile price swings, inadequate mass­market understanding of the technology, and insufficient ease­of­use for non­technical users.

World Reserve System will overcome these drawbacks and introduces a new token called “Trust”. It will adopt all achievements from the existing systems as well introducing a few new fundamental concepts.

But has been discussed since Dr. Szabo’s proposed BitGold [5]

1 For definitions throughout, see Glossary of Terms

To achieve stability projects have tried to back their assets by existing more stable assets like fita currencies or precious metals. But ther are major concerns that this cannot be the solution for the future. As the crypto currencies capitalization hits new hights these approaches will undermine the stability of the whole financial system as this will counteract the policy of central banks and therfor this will be prevented in the future by regulatory means.

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, market­based, or process­based drawbacks and limitations3. There is one element that can meet the requirement of a stable currency and this will be the money supply.

In our solution with the cryptocurrency called “trust” we have found a solution that will do a trustless method of money supply by software algorithms. As such users can trust the currency and the way can be paved to a world wide accepted currency for real life applications

All trust tokens will initially4 be issued on our own blockchain. All tokens will be locked in a major vault. There will be a target value of each token that is a mathematical relation to major long time history asset data like major fiat currencie and/or precious metals as well as fundamental economic data. As the globalization is already a fact and a goal for the future, the underlaying data is derived only from world wide data. This also prevents for national influenced politics. As such thw World reserve System acts like a Worldwide Central Bank for a crypto currency.

In a farer future the World Reserve System might back its value with additional physical assets.

# The Generations of Crypto Currencies

## General requirements

The requirements for the blockchain technology represents an evolutionary development. In the beginning the goal was the creation of a digital asset as an alternative plan to the existing fiat currencies. While meanwhile more and more use cases are coming up that cover more and more areas of our all lifes.

Todays general requirements include the following ones:

* Storing of any sensitive data on the blockchain
* Reasing these data after payments
* Connecting the payment system with real life data or events
* Unique ID for all stake holders including natural persons, organization entities and mashines
* Control of money supply to achieve stability
* Providing a platform for new upcoming concepts and ideas
* Interoperability, decentralized exchanges

What we see today is a constant evolution of the different blockchain technologies. These evolutionary steps occurs because of general requirements that virtually existed already from the beginning but were worked out or discovered later.

One of the drawbacks of these evolutionary steps is that a lot of systems has been developed under old assumptions and now it is difficult or even impossible to migrate or reengineer them into new systems that meet the new requirements.

Our view is, that now the times has come to collect all the concepts and create a new model for all todays and as far as it can be seen also for future requirements. A model driven approach is in this sense the best way to achieve

## Innovations

To meet these requirements every generation of blockchain has made its contribution. Constant innovation is the trademark of all these projects. But we can identify major steps where projects have introduced new fundamental improuvements.

### Bitcoin

The first innovation was Bitcoin itself. Though it was already a blockchain technology, its asset the coin was tightely connected with the underlaying blockchain.

### Blockchain

The second innovation was called blockchain, which was essentially the realization that the underlying technology that operated bitcoin could be separated from the currency and used for all kinds of other interorganizational cooperation. Now all kind of sensitive data could be stored in a blockchain in a cost-effective way.

### Smart Contract

The third innovation was called the “smart contract,” embodied in a second-generation blockchain system called ethereum, which built little computer programs directly into blockchain that allowed financial instruments, like loans or bonds, to be represented, rather than only the cash-like tokens of the bitcoin.

### Better Consensus

The fourth major innovation, the current cutting edge of blockchain thinking, is called “proof of stake.” Current generation blockchains are secured by “proof of work,” in which the group with the largest total computing power makes the decisions. These groups are called “miners” and operate vast data centers to provide this security, in exchange for cryptocurrency payments. The new systems do away with these data centers, replacing them with complex financial instruments, for a similar or even higher degree of security. Proof-of-stake systems are expected to go live later this year.

### Scaling

The fifth major innovation on the horizon is called blockchain scaling. Right now, in the blockchain world, every computer in the network processes every transaction. This is slow. A scaled blockchain accelerates the process, without sacrificing security, by figuring out how many computers are necessary to validate each transaction and dividing up the work efficiently. To manage this without compromising the legendary security and robustness of blockchain is a difficult problem, but not an intractable one. A scaled blockchain is expected to be fast enough to power the internet of things and go head-to-head with the major payment middlemen (VISA and SWIFT) of the banking world.

### Stability

A sixth major innovation will be the achievement of a stabil token at least with the same stability of major fiat currencies.

### Regulatory requirements

Another seventh major innovation is a crypto currency that meets the requirements of future regulatories. This includes the protection against money laundering, fraud and theft.

### Software implementaion

An eight innovation targets the way how the software systems are implemented. Until now the overwhelming majority of the crypto projects are implemented in a way that is not in accordance with standard software pattern. One of the main critic is that the systems are not very good maintainable. Also it will be difficult to undertake major improuvments to the systems. Though the most systems are Open Source the code is normally poorely documented. It is obvious that the most systems are developed under extreme time pressure. To improuve this issue a new system should be developed in accordance with standard software engineering pattern. The best approach would be a model driven one as this will be the best solution to open the system for future enhancements.

### Fees

The first generations of blockchain technology required fees to award the minors of the tokens. Especially Bitcoin minig meant the consumption of a big amount of electrical energy. This is call Proof of Work (PoW). As more critics came up especially to protect the environment a new consensus algorithm named Proof of stake was invented. But even in these systems though much lower, still fees were needed to protect the network.

### Reliability

The majority of the crypto projects use long time proven cryptographic algorithms like SHA256 to protect the immutability and secretcy of the distributed database also called the ledger. There is a common consensus not to introduce new algorithms. But there is a threat coming up, that could compromise the whole system. This will be the theoretical possibility to break the system by methods of quantum computing. It is discussed that this could happen within the next 10 years. Therfor it will be crucial to protect the system by new post-quantum cryptography. There are now a few projects that claim, that they have found a solution for this. This has to be further studied in the future.

## The generations - Overview

The following table compares the different blockchain generations with each other. The values are from 0 to 100 % where the higher values are alwas the better ones. 100 % fees means for instance that there are no fees at all for transactions.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Gene-ration** | **Exponent** | **Reliability** | | **Fees** | **Scala-bility** | **Sta-bility** | **Imple-menta-tion** | **Regu-latory** |
| **Block-chain** | **Quantum-resistency** |
| 1 | Bitcoin | 100 | 0 | 10 | 10 | 50 | 30 | 10 |
| 2 | Etherium | 100 | 0 | 20 | 20 | 50 | 30 | 10 |
| 3 | Cardano | 100 | 0 | 30 | 30 | 30 | 30 | 10 |
| 4 | IOTA | 100 | 100 | 100 | 90 | 30 | 40 | 10 |
| 5 | World Reserve System | 100 | 100 | 100 | 100 | 100 \* | 90 | 100 |

\* after an initial period until the target value has reached

## Introduction

As we have seen the Blockchain technology is more than a simple replacement of existing fiat currencies. It closes the gap between these assets and the digital world that is already the basis of our economy. While nearly all areas of our economic and social life is supported by computer systems in most centralized way, now there is a need to combine all procedures and protocols and let them smoothely work together. To position our new concepts we want first sum up what happened until now.

### First Generation

The first major blockchain innovation was bitcoin, a digital currency experiment. The [market cap of bitcoin](https://coinmarketcap.com/) now hovers billions of dollars, and is [used by millions of people](http://www.coindesk.com/2016-bitcoin-challenge-100-million-users/) for payments, including a large and growing remittances market.

When Satoshi Nakamoto, whose true identity is still unknown, released the whitepaper [Bitcoin: A Peer to Peer Electronic Cash System](https://bitcoin.org/bitcoin.pdf) in 2008 that described a “purely peer-to-peer version of electronic cash” known as Bitcoin, blockchain technology made its public debut. Blockchain, the technology that runs Bitcoin, has developed over the last decade into one of today’s biggest ground-breaking technologies with potential to impact every industry from financial to manufacturing to educational institutions. Here’s a brief history of blockchain technology and some thoughts about where it might go in the future.

## Second Generation

Even today, there are many who believe Bitcoin and blockchain are one and the same, even though they are not. Those who started to realize around 2014 that blockchain could be used for more than cryptocurrency started to invest in and explore how blockchain could alter many different kinds of operations. At its core, blockchain is an open, decentralized ledger that records transactions between two parties in a permanent way without needing third-party authentication. This creates an extremely efficient process and one people predict will dramatically reduce the cost of transactions.

When entrepreneurs understood the power of blockchain, there was a surge of investment and discovery to see how blockchain could impact supply chains, healthcare, insurance, transportation, voting, contract management and more. Nearly 15% of financial institutions are currently using blockchain technology.

Vitalik Buterin, co-founder of Ethereum and Bitcoin magazine, was also an initial contributor to the Bitcoin codebase, but became frustrated around 2013 with its programming limitations and pushed for a malleable blockchain. Met with resistance from the Bitcoin community, Buterin set out to build the second public blockchain called Ethereum. The largest difference between the two is that Ethereum can record other assets such as loans or contracts, not just currency. Ethereum launched in 2015 and can be used to build “smart contracts”—those that can automatically process based on a set of criteria established in the Ethereum blockchain. This technology has attracted the attention of corporations such as Microsoft, BBVA and UBS who are intrigued by the potential of the smart contract functionality to save time and money.

**Transition to Proof of Stake**

Currently, blockchain operates on the proof of work concept where an expensive computer calculation or “mining” is done in order to create a block (or a new set of trustless transactions). Currently, when you initiate a transaction, it is bundled into a block. Then miners verify the transactions are legitimate within that block by solving a proof-of-work problem—a very difficult mathematical problem that takes an extraordinary amount of computing power to solve. The first miner to solve the problem gets a reward and then the verified transaction is stored on the blockchain. Ethereum developers are interested in changing to a new consensus system called proof of stake.

Proof of stake has the same goal as proof of work—to validate transactions and achieve consensus in the chain—and it uses an algorithm but with a different process. With proof of stake, the creator of a new block “is chosen in a deterministic way, depending on its wealth, also defined as a stake.” Since in a proof of stake system, there is no block reward, but the miners, known as forgers, get the transaction fees. Proponents of this shift, including Ethereum co-founder Buterin, like proof of stake for the energy and cost savings realized to get to a distributed form of consensus.

## Third Generation

**Blockchain Scaling on the Horizon**

Since currently, every computer in a blockchain network processes every transaction, it can be very slow. A blockchain scaling solution would determine how many computers are necessary to validate every transaction in a way that doesn’t compromise security.

Today, Bitcoin is just one of the several hundred applications that use blockchain technology. It’s been an impressive decade of transformation for blockchain technology and it will be intriguing to see where the next decade takes us.

## Forth Generation

While the most crypto currency projects rely still on the basis of a blockchain, there has been recently come up a few projects that break with this tradition and they have introduced a new model called Directed Acyclic Graph (DAG). The promiss of this model is, that with the increasing number of nodes in the network the speed of transactions goes up. Mainly intended for the new mashine economy it can also be used for general purposes.

#### The forth Generation - World Reserve System

The Blockchain Technology has now reached a point of no return. All the more it will be vital to achieve the stability that actually is provided by the Central Banks. It is overdue to create such a new crypto currency system that is not backed primarily by physical assets or the promises of governments resp. central banks.

The first attempts to create such a crypto currency like TetherUS or DigixDAO are not future-proof and cannot achieve this goal on a large scale money supply.

Instead our concept is to let algorithms do the job of the money supply. The advantage is, that in our global economy we can achieve a fair and not by politics influenced money stability. So we started this project. The most important part will be to deliver a widely accepted whitepaper and our fundamental model.

# World Reserve System

## Vision

While the current Blockchains target the Banks as the financial providers the World Reserve Systems targets the financial systems as a whole including the Central Banks. Achieving the stability of the Currency compared with real life data by scientific mathematical methods should replace the current Central Banks tasks. This should lead to a world wide more stable Economy. Finally the TRUST coin shell replace money world wide.

## The needed amount of money supply

While existing blockchain projects define a certain target for the number of their currency units in a way that there will be a projected end date where all the tokens had been issued resp. brought into circulation.

Millions, billions, and trillions…

When we talk about the giant size of Apple, the fortune of Warren Buffett, or the massive amount of global debt accumulated – all of these things sound large, but they are actually extremely different in magnitude.

That’s why visualizing things spatially can give us a better perspective on money and markets.

## How Much Money Exists?

This infographic was initially created to show how much money exists in its different forms. For example, to highlight how much physical cash there is in comparison to broader measures of money which include saving and checking account deposits.

Interestingly, what is considered “money” depends on who you are asking.

Are the abstractions created by Central Banks really money? What about gold, bitcoins, or other hard assets?

## A New Meaning

However, since we first released this infographic in 2015, “All the World’s Money and Markets” has taken on a different meaning to us and many others. It’s a way of simplifying a complex universe of currencies, assets, and other financial instruments in a way that people can understand.

Numbers represented in the data visualization range from the size of the above-ground silver market ($17 billion) to the notional value of all derivatives ($1.2 quadrillion as a high-end estimate). In between those two extremes, we’ve added many other familiar measures, such as the GDP of California, the value of equities, the real estate market, along with different money supply metrics to give perspective.

The end result? A visually pleasing, but enlightening new way to understand the vast universe of global assets.

To get “All the World’s Money” in book or poster form, go to the [*Kickstarter page*](https://www.kickstarter.com/projects/1861039958/visualizing-change-a-data-driven-snapshot-of-our-w) now. Deadline: Oct. 31, 2017

## About the Money Project

# Timeline and Milestones

Based on a Model Driven Design

Based on proven Technology when Mature Stage reached

Controlled by Thousends of Super Users from the Scientific Community in the Future

After reaching the Value Target the TRUST Coin will be kept stable by a mathematical transparent formula developped by leading scientists

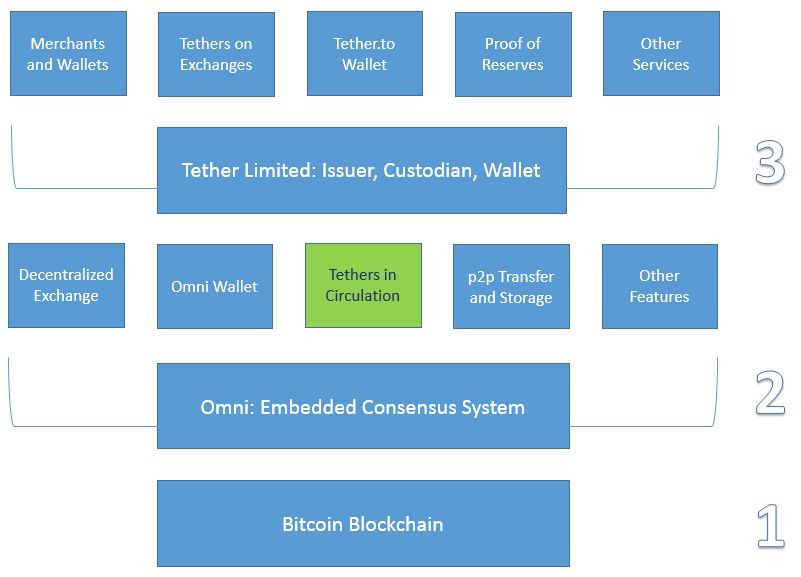
# Technology

At the moment the technology for the TRUST token has not been already finally choosen. This will be part of one of the milestones. Generally speaking our concept is to choose one of the existing platforms that has proven its reliability and performance. First evaluations has pointed in two directions. One is the IOTA-Protocol and secondly the CARDANO-Platform.

Above the chosen platform in the future will be a Model Driven Approach which has already started. The underlaying crypto platform will be used as the crypto engine, where our own platform will design the whole money supply chain. The Model Driven Design has the advantage to be maximum transparent and can be evaluated and maintained by a large community in the future. All our software will be open sourced. Our Role Model for the participation is the CARDANO system and community approach.

Each tether issued into circulation will be backed in a one­to­one 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.

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



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 meta­data via the embedded consensus system, Omni.
2. The second layer is the Omni Layer protocol. Omni is a foundational technology that can:
   1. Grant (create) and revoke (destroy) digital tokens represented as meta­data embedded in the Bitcoin blockchain; in this case, fiat­pegged digital tokens, tethers.
   2. Track and report the circulation of tethers via Omnichest.info (Omni asset ID #31, for example, represents TetherUSD) and Omnicore API.
   3. Enable users to transact and store tethers and other assets/tokens in a:
      1. p2p, pseudo­anonymous, cryptographically secure environment.
      2. open­source, browser­based, encrypted web­wallet: Omni Wallet.
      3. multi­signature and offline cold storage­supporting system
3. The third layer is Tether Limited, our business entity primarily responsible for:
   1. Accepting fiat deposits and issuing the corresponding tethers
   2. Sending fiat withdrawals and revoking the corresponding tethers
   3. Custody of the fiat reserves that back all tethers in circulation
   4. Publicly reporting Proof of Reserves and other audit results
   5. Initiating and managing integrations with existing Bitcoin/blockchain wallets, exchanges, and merchants
   6. Operating Tether.to, a web­wallet 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 tethers8 . The user can transfer, exchange, and store tethers via a p2p open­source, pseudo­anonymous, Bitcoin­based 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, Real­Time 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 non­trivial 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 one­to­one 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 System10 is different than the Tether.to web­wallet 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 web­wallet operating on closed­source 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 PoR­based 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 appendix11 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

* Re­centralized 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 compliance12.

*We could abscond with the reserve assets* ­ The corporate charter is public13 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.

*Re­centralization 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

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
* 3­7 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 crypto­fiats 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 crypto­processes
  + Multi­signature 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 tech­savvy 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, pseudo­anonymously, 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 crypto­fiat 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 fiat­crypto features
  + Microtipping, gift cards, more
* Anything one can do with Bitcoin as a merchant one can also do with tether

Future Innovations Multi­sig and Smart Contracts Proof of Solvency Innovations

# Conclusion

Tether constitutes the first Bitcoin­based fiat­pegged cryptocurrencies in existence today. Tether is based on the Bitcoin blockchain, the most secure and well­tested blockchain and public ledger in existence. Tethers are fully reserved in a one­to­one 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, C­CEX, 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 technology­based14 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

e 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 long­tail 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 Fiat­pegging Systems

Here’s a list of some of the common drawbacks and limitations of existing fiat­pegging systems.

* The systems are based on closed­source software, running on private, centralized databases, fundamentally no different than Paypal or any other existing mass­market retail/institutional asset trading/transfer/storage system.
* Decentralized systems that rely on altcoin blockchains which haven’t been stress­tested, developed, or reviewed as closely as other blockchains, like Bitcoin.
* Pegging processes that rely on hedging derivative meta­assets, 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 pegged­assets 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 risk­free 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 reserve­based 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.

13­09­01265). Pursuant to the agreement, RenRenBee will provide anti­money 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, record­keeping, and reporting procedures consistent with U.S. law and with the Hong Kong Anti­Money Laundering and Counter­Terrorist 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 off­shore banking regulations, as all of the banks had been requested to check this with their own legal, compliance and head­office 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 open­source, cryptographically secure, and uses a distributed ledger. See: <http://en.wikipedia.org/wiki/Cryptocurrency>

**Real­world 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.

**Utility­backed 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.

**Asset­backed/pegged cryptocurrency:** Any cryptocurrency whose price is pegged to a real­world asset,

i.e. its not a “utility­backed” cryptocurrency.

**Tether(s):** a single unit (or multiple units) of fiat­pegged cryptocurrency issued by Tether Limited

**TetherUSD or tUSD:** a single unit of crypto­USD 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 asset­backed decentralized digital token, cryptographically/mathematically proves that all tokens that have been issued are fully reserved and backed by the underlying asset.

* STABILITY
* Stability by Software-Driven Money-Supply
* Automatic Comparison with a FIAT-Currency-Basket and Real Life Economic Worldwide Data

# References

1. [https://www.thefinancialist.com/wp](http://www.thefinancialist.com/wp)­content/uploads/2012/10/2012­GlobalWealthReport­.pdf
2. https://bitcoin.org/bitcoin.pdf [[3]http://www.deloitte.com/assets/Dcom](http://www.deloitte.com/assets/Dcom)­UnitedStates/Local%20Assets/Documents/FSI/us\_fsi\_BitcointheNe wGoldRush\_031814.pdf
3. https://github.com/mastercoin­MSC/spec
4. <http://unenumerated.blogspot.com/2005/12/bit>­gold.html
5. https://iwilcox.me.uk/2014/proving­bitcoin­reserves
6. <http://antonopoulos.com/2014/02/25/coinbase>­review/
7. <http://www.coindesk.com/krakens>­audit­proves­holds­100­bitcoins­reserve/