World Reserve System

The World's most stable currency

Draft Version: 0.01.01 (very early stage)

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

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 easeof-use 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.
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 limitations[3]. 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 initially[4] 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.

[1] For definitions throughout, see Glossary of Terms

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	Platform
		Block-chain	Quantum-resistency						
1	Bitcoin	100	0	10	10	50	30	10	10
2	Etherium	100	0	20	20	50	30	10	100
3	Cardano	100	0	30	30	30	30	10	100
4	IOTA	100	100	100	90	30	40	10	50
5	World Reserve System	100	100	100	100	100 *	90	100	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 now hovers billions of dollars, and is used by millions of people 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 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.

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.
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

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 fifth Generation

The Blockchain Technology has now reached a point of no return and some sort of maturity. 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

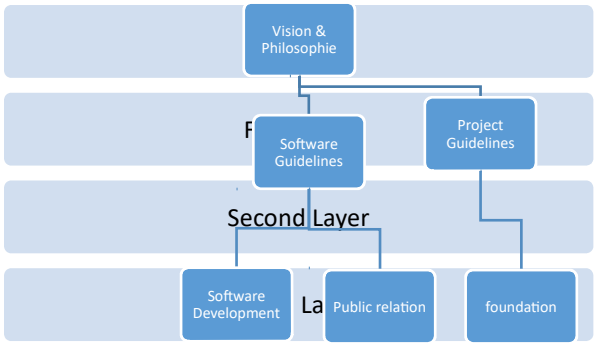
Vision

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.

Fundamental principles

Hierachical behaviour principle

On the top is the fundamental philosophie and Vision of the project. All other aspects has to follow this until changes are made.
On the second level we have established the projects process guidelines. They control the whole process of the design and implementation from a higher level including the way changes can be made to the first level.
On the third level you find all sub-projects that implement the system



First and Second Layer

- Small groups of academics and developers competing with peer reviewed research
- Heavy use of interdisciplinary teams including early use of InfoSec experts
- Fast iteration between white papers, implementation and new research required to correct issues discovered during review

Upgradable system

Building in the ability to upgrade post-deployed systems without destroying the network

Transparent Funding

Development of a decentralized funding mechanism for future work

User experience

Bringing stakeholders closer to the operations and maintenance of their cryptocurrency

Multi-Asset-Layer

Acknowledging the need to account for multiple assets in the same ledger

Abstraction Layers

We recognize that a perfect system can never be designed. We believe in achieving maximum flexibility all implementation must be isolated behind abstraction layers.

Backward compatibility

Just from the beginning all precautions have to be done to guarantee always the backward compatibility of all enhancements of the node software.

Integrating all usefull concepts from existing altcoins

Learning from the nearly 1,000 altcoins by embracing features that make sense.

Research the Ethical and Social Aspects of the project

Explore the social elements of commerce

Regulatory requirements

Find a healthy middle ground for regulators to interact with commerce without compromising some core principles inherited from Bitcoin

The software development

WRS will be a development just from the beginning though it will make reuse as much as possible from existing solution whenever it will make sense.
All developers will work with a preconfigured Integrated Development Environment (IDE). As such we have choosen

the Java Eclipse Platform. The programming language will be Java.
Developers can test the network in a simulation and therefor there is no need to run in the every day work a testnet. For integration tests a testnetb will be provided and will constantly execute tasks in an continious build environment. This approach will help to achieve a robust system and will speed up the development. The sources will be store on the GitHub-Platform.

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. But this concept falls short if all future money supply demands should be fullfilled.
We introduce another concept.
When the network starts, it generates in a main vault a very large amount of TRUST-units for any forseeable future. Lets say the current world wide money supply will be 500 Trillion USD, during the genesis process an amount of 1 Trillion times 1000 Trillion will be generated and assigned to this main vault. Further money supplies occur as transaction out of the main vault to a chain of vaults. The basis for these transactions are mathematical formulas where the input parameters are provided by real life data. Only the source of the data will be controlled by a board of economists. This board will be elected by stakeholders with the largest amount of assets in the system. This will be the equivalent to the control mechanism by the current central banks.

Transactions

Transactions in WRS will be stored on the ledger by the established cryptographic methods. Every transaction comes with additional information. On one side it contains the senders and receivers addresses. These addresses references wallets. The address somes always in a tupel together with the identity-ID of the sender and of the receiver. These identity-IDs are immutable and can identify persons, other legal entities and mashines. In case of a mashine it is associated with a person or a legal entity.
To maintain the privacy all identity-IDs inside the ledger will be cryptographelly encoded and can only be decoded by a known seed. This seed will be a matter of the regulation. The provision of the identity-ID will be organized in the same way today certificates are issued.

How money will be supplied

Once enough money has been supplied and assigned to the main vault, called the main treasury, the initial coin offering starts.
Another vault manages foreign assets like other crypto currencies of physical assets like precious metal. The latter contains data that entitles the system to get access to those stored values.
In this stage new users can buy TRUST-coins with bitcoin tokens and/or other tokens TRUST-tokens

Smart contracts

The core of a smart contract in WRS is a parsable mathematical expression that can be attached to each transaction and will be stored in the ledger. The input for this comes in form of zero value transactions. These zero value transactions contain the name of the input variable as well as a value. Until validation of the expression giving a true result the transaction is considered as pending. If one of the input variables prevents already the expression for becoming true, the transaction will be not executed and reversed. A notification will be issued optional to the sender with optional reasoning.
This approach leads to a completely open and general purpose solution compared with scripting solutions.
Input variables for the expression can be:

- Multisignatures
- Time periods
- Delivery confirmations
- economic data

Expressions for the smart contract will stored as Math Markup Language. So it can be parsed by the software.
We believe that this approach will create a much mor robust system than systems with scripting. The nodes software has only to parse and evaluate the expression. This will be much more safe than executing a script. As financial transaction are a very important and sensitive matter with potentially hazardious effects, it is also to say that the simple storage of a mathematical expression creates a maximum transparency.

Flow of Funds Process

asd

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

The development will happen in several 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.
In the moment the technology for the TRUST token has not been already finally choosen. This will be part

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

Implementation Weaknesses

Here is a summary of the weaknesses in our approach:

- New system, needs some time to become mature
-

For Exchanges

Exchanges will receive in the initial phase a certain amount of TRUST-coins with a predefined initial offering price.
Exchanges are binded by equal and transparent rules to obtain the initial amount of TRUST-coins for free.
Users cannot buy TRUST-coins as a Initial Coin Offering (ICO). Instead they can be rewarded by running a full node.

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. Crypto currencies can solve many of these problems. WRS will help to provide a stable currency. Otherwise they will not use crypto currency in a large scale.

Money lending

WRS as an exchange platforms

Future Innovations

Conclusion

The World Reserve System will establish the first stable crypto currency with the unlimited money supply in the future.
It is a future save investment as all elements for future regulations are considered without compromise the data security of the users.

Appendix

Audit Flaws: Exchanges and Wallets

Market Risk Examples

Legal and Compliance

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.

References

1. https://www.thefinancialist.com/wpcontent/uploads/2012/10/2012GlobalWealthReport.pdf
2. https://bitcoin.org/bitcoin.pdf [3]http://www.deloitte.com/assets/DcomUnitedStates/Local%20Assets/Documents/FSI/us_fsi_BitcointheNe wGoldRush_031814.pdf
4. https://github.com/mastercoinMSC/spec
5. http://unenumerated.blogspot.com/2005/12/bitgold.html
6. https://iwilcox.me.uk/2014/provingbitcoinreserves
7. http://antonopoulos.com/2014/02/25/coinbasereview/
8. http://www.coindesk.com/krakensauditprovesholds100bitcoinsreserve/