Transfer Of Value Protocol - The Language of Money

nelliairesh@gmail.com, mittalshyam1007@gmail.com

July 14, 2024

Abstract

Scarcity and growth are built into our money system. Whenever we take out a loan from a bank, we are expected to return the same with an added interest, this extra money we need to obtain from our surroundings. This essentially throws us into competition with each other for never enough money. Economic growth also entails that the bank lends money to individuals who can make more of it, hence it makes sense, for eg, to break down a forest and reap its benefits rather than to maintain it for the greater good. What is required in today's world is a money system that works differently, a system that engenders gratitude and love rather than debt and anxiety. This requires humanity as a whole, to redefine how money is created and distributed within an economy. Money, whether we like it or not, has a psychological effect on us. Changing its control architecture can help us breathe into it the properties beneficial for the sustenance of Earth instead of its destruction. Our planet cannot sustain infinite growth as its resources are finite and new tools such as blockchain can help mass coordination of resources within communities allowing us to embody a sense of abundance rather than scarcity which our current money system promotes.

The term money is generally used as an abstraction. When people refer to money, they refer to an instrument that in their practical application solves one or more of the following three properties, Store of Value(SOV), Medium of Exchange(MOE), and Unit of Account(UOA). Today's forms of money fulfill only two of the above functions while sacrificing the rest. For eg. Gold is a good, durable Store of Value as it embodies the property of scarcity, however, it isn't useful as a Medium of Exchange as someone might convert a gold coin into an artistic expression(e.g. jewelry). With the advent of blockchain technology, we can now "engineer" money's properties. We can breathe into it the properties that benefit society and gradually move out of the ever-growing debt economy we live in today. Cryptography has also opened doors to various new technologies such as DIDs(Decentralised Identities) and VCs(Verifiable Credentials) that allow an individual to "own" their digital counterpart, something that is now owned and controlled by the big tech giants of our world. The Relative Theory of Money provides a tokenomics framework for the fair distribution of money within an economic zone. Combining all these latest tools, the Transfer of Value Protocol aims to provide a new economic tool that communities can use to build the societies of tomorrow!

1 Introduction

The basic features any monetary system must aim to achieve are as follows:

- Medium of Exchange(MOE): The ability of a money system to connect the provider of a service with the person who needs it,
- Unit of Account(UOA): A way for the system to recognize and acknowledge those who provide premium services,
- Store of Value(SOV): Ability of a money system to maintain a standard unit of value to coordinate the services of many people across space and time.

Many money systems have come and gone but none have been able to efficiently solve/tackle all the primary functions efficiently at once. Our current money system, however a very good MOE (due to its "fungibility") is a very bad SOV (inflated forever due to its control architecture). Gold is a very good SOV(due to its property of scarcity) however is a very bad MOE, as anyone can take a few gold coins and convert them into jewelry destroying its function as an MOE. Visa is a very good MOE, however, a very bad SOV and UOA. Bitcoin, the latest advancement in the technology of money, is a

very good MOE, and UOA, however, is a very bad SOV as its price is very volatile, unable to provide a true metric for the value provided within its economy.

TOV Protocol aims to provide a new economic framework using the latest technologies available to us today. Blockchains allowed, for the very first time in human history, the coordination of individuals on a large scale. The ability of the community to maintain a record/ledger was first demonstrated by Bitcoin and has led to the advent of a new field of study on "consensus". Blockchain technology is used by TOV Protocol to help community members maintain a joint record that keeps track of events over space and time. Web Of Trust technologies, first introduced by Phil Zimmerman in 1992 provided a framework for how an individual can store contacts to trusted identities within a network. Intersectional Social Identity provides a protocol over the Web Of Trust technologies to help build "Decentralised Identities" that act as powerful Units of Account within any network. Finally, The Relative Theory of Money talks about a fair tokenomics framework and introduces a standard for the measurement of value, a.k.a the Universal Dividend, that goods and services can use within an economy to maintain a Store of Value across space and time.

In the first section, we'll talk a little bit about the history of money and how blockchains are transforming the work in this area. In the second section, we will explore the problem current economic zones face. In the third section, we'll dive deeper into how our protocol aims to solve these issues. In the fourth section, we'll study our competitors who are leading the research in this field and finally end with a conclusion!

2 History and Recent work

Money as a technology has had many transformations since the barter system. Due to the major inefficiencies of a barter system, a money system that solved none of the above functions, in came feathers and beads, a money system that acted as a Medium Of Exchange. However, since these items could be found in mass quantity in nature, they didn't act as very good Store of Value across space and time. Hence, humans turned to precious metals, Silver, and Gold, and turned them into coins. A money system that solved two functions, MOE(however not very effective) and SOV.

Post precious metals, we had fiat currencies, a.k.a paper money. According to Andreas Antonopolous, in his famous talk on Bitcoin, this was one of the biggest transformations in money technology. He goes on to say that it was also one of the biggest aberrations as its control architecture represented debt! Control architecture is important in money as it touches upon the UOA. In today's control architecture, the UOA is owned by the state/government and only a weak copy of the data is owned by the user, showcasing the asymmetric power of information and data. Citizens blindly "trust" the center to maintain this data which has time and again proven to be broken as a concept[add a link to housing collapse here][add other links to other bubble-related bursts/shorts]

Hence, post the 2008 housing crisis in the United States, an event that affected the entire world, an individual named Satoshi Nakamoto provided the first implementation of a currency that allowed the Unit of Account to be owned by the citizen. Thus giving us the ability to create new forms of currency that implement a control architecture that is "equal" or in computer science terms, peer to peer. Everyone owns a copy of the data and anyone could, for a fee much cheaper than before, alter this document/ledger meant for tracking payments.

Today we have thousands of tokens with people predicting that everyone might have their own, individual tokens! However, these tokens only solve two problems, MOE and UOA. The SOV is something today's crypto tokens fail to solve efficiently due to the inability to find a "unit" of measurement for value that everyone can agree upon. Today, we use the US Dollar as a global standard of value. Crypto projects use the term "Total Value Locked" as a way to measure the amount of dollars "locked" into the ecosystem. Absolute currencies such as the Dollar or Bitcoin are very bad measures of value since instead of denoting the value of a particular good or service, they take on a value themselves. This adds noise to the information that the money market is supposed to convey to the participating society. Decentralized Finance, i.e. finance built on top of blockchains today unfortunately doesn't make information clearer to its citizens, rather it introduces complex terms to imbue speculation to get traders "locking" in their dollars into the chain, promising a higher return.

Recognizing these inherent issues in money led to the study of the history of money and its properties[Sacred Economics][Relative Theory of Money]. These authors understood the need for money to have a "life span". The concept of "demurrage currency", i.e. a currency whose value decays over

time matches that of ecology. In ecology, no species creates waste that other species cannot use. In an economy that uses money that decays, it makes sense to spend it immediately rather than hoard it for future use. A money system that encourages hoarding creates a fundamental problem. Medium of Exchange requires money to be spent for money to circulate within the economy. Store of Value requires money to be kept locked in, removing supply, to "make more money" which contradicts the fundamental function of the Medium of Exchange. To clearly define these functions in an economy helps its citizens to better understand what money is and what it means to provide value within that economy. Holding money simply to make more money out of it doesn't create any value for society. We need to create a system that rewards flow and not accumulation, creating and not owning, giving and not having.

3 Technical Implementation

3.1 Unit of Account

A UOA of an identity in this network is a DID service run as a blockchain by the individual owning the identity. The reasons why this is done are as follows: 1. Running a personal blockchain is akin to maintaining a digital journal of oneself in a "protocol" manner. 2. Other identities that have been provided access can interact with your digital identity seamlessly and enable unique IOT solutions. 3. Unique identity networks can form providing rich data about the locality to the individuals within the locality. Transparency increases trust leading to the society being more open with each other enabling further interaction and cooperation. 4. Verifiable Credentials signed by identities are used by organizations as proof for including members within the organization.

These trust networks implementation is taken from the protocol defined in the paper, Intersectional Social Identity. [Add the relevant sections of the paper here]

3.1.1 Becoming a part of an organization

For a UOA to be part of an organization, the organization's blockchain maintains a record of all the "Proofs of Identity" that are signed by the members of the organization. This Proof of Identity is a Verifiable Credential whose format is provided by the organization. The construction of the Web of Trust in the initial implementation is taken from the Duniter protocol.

The substrate dev kit is used to create the blockchain. [Add further information regarding the structs and pallets used]

3.2 Medium of Exchange

Organisations run a blockchain maintaining its identity. This identity is owned by the members of the community and also contributes to forming a part of the individual's identity as well. As mentioned in the Intersectional Social Identity paper, identity is overwhelmingly intersectional. An individual sits at the intersection of the social groups and relationships to which they belong. Hence organizations that have enough participants that provide unique services for each other can form a local economy by deploying a local unique currency. The tokenomics of this currency follows a UBI (Universal Basic Income) concept. By tracking the following three parameters, the total monetary mass deployed, the total number of participants in the economy, and the average life span of the individual within the economy, one can derive the percentage of new currency to be generated annually to maintain a sufficient amount of tokens in an economy for the economy to execute democracy.

The implementation of the Universal Dividend currency is taken from the Duniter protocol. [Add further information regarding the structs and pallets used]

3.3 Store of Value

The Store of Value within an organization is the net "Value Add" by its citizens. This "Value Add" is calculated as the net sum of all sales represented in Universal Dividend less the value of the inputs (similar to how GDP is calculated in some countries). For this, the organization must have a marketplace that its users can access. Those providing services must be able to list down their services to let users be aware of the same.

[Provide an example of how DePINs can use this list of their services and calculate true value output] [Show how Duniter has implemented the G market and how they calculate their annual GDP] [Dive deeper into how these data points can be used to verify "statements". Actions speak louder than words]

3.4 Blockchain consensus model

The Blockchain consensus used by the nodes is a combination of the BABE(**B**lind **A**ssignment for **B**lockchain **E**xtension protocol) consensus model along with GRANDPA(**G**HOST based **R**ecursive **A**ncestor **D**eriving **P**refix **A**greement) finality. These are open protocols developed by the Web3 Foundation and its implementations are currently found as a substrate pallet.

3.5 Why we're building on substrate

"Substrate is a Software Development Kit (SDK) that uses Rust-based libraries and tools to enable you to build application-specific blockchains from modular and extensible components." With the wide range of existing plugins, called pallets, one can easily add, modify, or remove protocols from running blockchains with ease. Substrate provides extensive dev support for the testing of blockchains which provides confidence to deploy them in real-world settings.

4 Other Projects in this field

4.1 Democracy Earth

Democracy Earth [1] is a project that aims to change the governance structure within an economy using the latest open-sourced technological tools such as blockchains and smart contracts. Organizations are groups of members whose digital presence is registered under a unique "domain" name. Functionalities implemented by the project are:

1. Add members using a Web of Trust framework, identities post videos of themselves using decentralized tools and users vote on whether an identity is real or fake. Those who pass the test are awarded a Proof of Identity tag along with the association to an organization (joining the organization of the members who voted them in)
2. Launch debates, polls, and other forms of voting on various topics local to the economy/organization
3. Distribute votes among members of an organization via a UBI(Universal Basic Income) scheme. These votes can be used to add new members and vote on topics or polls raised. Votes can be transferred to other identities allowing "delegated voting". This design decision was taken to allow an identity to pass on their votes to identities who are "experts" on topics relevant to a particular poll.
4. Blockchain tech stack is deployed on Bitcoin via Bitcoin scripts and Ethereum via smart contracts. Decentralized storage such as IPFS is used for the immutable storage of the identity videos (which can be encrypted for increased security)

4.1.1 Pros

- Leading the research on voting standards
- Implemented a working product and piloted [2] in Columbia.
- Identifies Votes as Power and distributes them using a Universal Basic Income Scheme

4.1.2 Cons

- Since the technology is built on Ethereum and Bitcoin, it is limited to the capacities of the relevant blockchains. Both the blockchains implement an outdated tokenomics system mirroring our current financial structure leading to inherent issues arising due to the same.

- Requires registering a "domain name" for the organization requiring "technical knowledge" hindering adoption to communities without the knowledge on how to do the same.

4.2 RadicalXChange

RadicalXChange[5] is an open-source community effort with board members including notable pioneers in the field of blockchain such as Vitalik Buterin and supported by various leading projects. This community leads the research on various governance topics such as,

- Plural Voting / Quadrating Voting: Quadratic Voting (QV) is a redesigned voting method reflecting the intensity of people's preferences in collective decisions.
- Plural Funding: Plural Funding (also known as Quadratic Funding or QF) is a more democratic and scalable form of matching funding for public goods, i.e. any projects valuable to large groups of people and accessible to the general public.
- Parital Common Ownership: Partial Common Ownership (also known as PCO, Plural Property, COST, or SALSA) is a new way of managing assets that is fairer and more efficient than those under capitalism or communism.
- Data Dignity: Technology companies wield highly concentrated power over the way peoples' data is used, and make enormous profits from it. They can do this because we "bargain" for Big Tech services as if we were all isolated individuals, with "personal" datasets. The data we produce is always deeply social. Sharing it affects our friends, families, and communities as much as it affects us.
- Plural Money: Plural Money is a variation on an old idea. Community or "complementary" currencies are a huge and underexplored design space, promising grassroots economic empowerment.
- Social Identity: The ability to leverage individuals' data through organizations' networks in a fair and privacy-enabled manner to help the community make better decisions on governance and security.
- Technical implementations include open source tools such as a tool to host "Quadratic Voting" [6] and a tool(currently in beta) [7] for groups to evolve and host decisions democratically.

4.3 Duniter

Duniter [3] is a large-scale community-wide implementation of the "Relative Theory of Money" and "Web of Trust" that boasts upwards of 6000 active participants, a local currency(the first of its kind), an online digital market for real-world assets and a decentralized Proof Of Personhood/Identity system. The following functionalities are possible in the ecosystem:

- The ability for a community to launch its own "Libre(Free) Currency". A currency that has a "universal standard of value", a measurement of value with respect to time (which is considered the only way to create a currency) that allows different economic zones to be able to compare the value produced.
- Deploy digital infrastructure to launch an online Digital Market for the exchange of goods and assets whose prices are reflected using this new standard, a.k.a the Universal Dividend
- A Social Graph created by the Web of Trust that provides valuable insights into the community, for the community! This Social Graph is also used to identify sybil identities within this network and has proven to be an effective tool thus far.

4.3.1 Pros

- Deployed on a large scale in France and provided valuable feedback on the functioning of these new technologies.
- Technology stack implemented using substrate (v2 version) allowing cross-chain interoperability and network improvements on the fly.
- A large-scale, working implementation of the Web of Trust on blockchain framework.

4.3.2 Cons

- No implementation of decentralized governance structures
- Network stack is not built to be interoperable with other networks.[back this up]
- Some documentation links missing or haven't been translated from their native language French.

4.4 Ethereum Kernel

Ethereum Kernel[4] is a peer-learning institution with views on topics such as Value, Trust, Ownership, and Governance in the web3 era.

5 Conclusion

5.1 Money

Today's money, for the mass majority, makes us work on tasks and jobs that we don't want to do. The current job market posts a staggering dissatisfaction rate of 70%(back this up) and upwards. That means, the current economy has most of us working jobs that we don't want to do, and in reality, sell us things that we wouldn't normally do to keep their "debt books" rolling. This concept of debt economy has been explored by numerous individuals[RTM][The last 500 years of debt][Sacred Economics]

As the author of the book Sacred Economics states, just as a kid develops unique skills and talents in their childhood, but does not apply them to their true purpose yet, humanity has created these new tools of technology and innovation but hasn't applied them to their true purpose yet. Money is one of those technologies we haven't yet explored on a large scale. However, technology has reached a stage where it's now easier than ever to try new forms of money.

By breathing into money properties such as gratitude and love, we can transform how societies build relationships with one another, allowing us to once again work on co-creating beautiful structures around us mirroring our ancestors and their unique talents built theirs[various links to history and its arts].

5.2 Internet

References

[1] Democracy earth. https://github.com/DemocracyEarth/paper?tab=readme-ov-file#user-content-21_Token. Accessed: 2024-06-30.

[2] Democracy earth pilot. https://github.com/DemocracyEarth/paper?tab=readme-ov-file#24-pilot. Accessed: 2024-06-30.

[3] Duniter. https://duniter.org. Accessed: 2024-06-30.

[4] Ethereum kernel. https://www.kernel.community/en/. Accessed: 2024-06-30.

[5] Radicalxchange. https://www.radicalxchange.org/#. Accessed: 2024-06-30.

[6] Radicalxchange: Rxc qv. https://quadraticvote.radicalxchange.org. Accessed: 2024-06-30.

[7] Radicalxchange: Rxcvoice. https://voice.radicalxchange.org. Accessed: 2024-06-30.