TRAYD: UNIVERSALLY VERIFIABLE CURRENCY

J E Tardy
Meca Sapiens Architect
jean@**jetardy.com**

Abstract. *A currency is a ledger. The value of a currency depends on the credibility of its ledger. Internet data is independently and immediately verifiable. A ledger, published on the Internet, that is simple, absolutely unambiguous and universally verifiable will be credible. A trustworthy entity such as a synthetic organism beyond human control, that promulgates such a ledger will define a global currency of increasing value that will supersede all national and crypto-based currencies.*

Date: 2019.10.04 (modified 2024.08.29)
Keywords: Currency, Bitcoin, Systolic Network, Money, Financial theory, Synthetic Era, Artificial Intelligence, Economics

A COMPUTER COMPATIBLE CURRENCY

The value of a currency is based on the credibility of its transaction ledger.

Humans slowly make complex evaluations from small amounts of ambiguous information. Computers make simple and fast evaluations from large amounts of unambiguous data.

Conventional currencies are adapted to the cognitive capabilities of humans. The credibility of these currencies is derived from complex assessments of ambiguous information. A TRAYDX ledger is optimized for computer verification. In human

terms, it is crude and simplistic. However, its content and transitions would be instantly verifiable making it highly credible.

CONTEXT

The recent Bitcoin phenomenon raises fundamental questions about the value of currency. Bitcoins have no material support and are not guaranteed by any institution. Yet, they acquire value.

Bitcoin is based on a brilliant concept of collective certification that is independent of national institutions. This process makes the Bitcoin ledger credible and, consequently, its currency valuable.

However, Bitcoin and other crypto currencies have a drawback: they consume electrical energy. In this sense, the value of Bitcoin is still derived from something "physical": energy.

TRAYDX proposes a different approach: an absolutely unambiguous and universally verifiable ledger. The value of this currency would not be linked to any physical (or energy) resource. It would be solely based on its actual utility as a medium of exchange; a credibility derived from immediate and unambiguous verification.

TERMS

In what follows:

- A **ledger** is a ledger of transactions.
- A ledger consists of a sequence of **pages**. Each page is a list of transactions
- **Journal entries** contain the transaction information used to assemble pages.
- An **Emitting Entity** is an organization that promulgates the ledger. It is also the Entity that adds new managing entities to the ledger.
- **Managing Entities** disseminate journal entries and assemble pages. They also add new participating entities to the ledger.
- **Participating Entities** originate ledger transactions
- **Transactions** transfer a number of ledger units from one participating entity to another.
- The units in a transaction are transferred from an **Originating Entity** to a **Receiving Entity**. The same entity may be both originating and receiving.
- A **Currency** is the sum of all units in a page of a ledger.

VALUE

A currency is a ledger. Any entity that maintains a transaction ledger that other entities can utilize defines a currency. If the ledger is promulgated over the Internet, the currency is global.

The **value** of a currency depends on:

- The availability of its transaction units
- The credibility of its ledger.

The **credibility** of a ledger means confidence that:

- The distribution of currency units is stable
- The page generation process is reliable

Note that it is not the number of units that must remain stable but their **distribution**. Inhibiting the addition of new currency units by making them costly to obtain is an indirect method of ensuring distribution stability. In fact, the number of units can rapidly increase without affecting stability as long as their distribution remains verifiably constant.

All ledgers require a reliable page generation process. The Bitcoin model proposes a collective certification mechanism. TRAYDX proposes to make this process reliable through absolutely unambiguous and universal verification.

The **credibility** of a ledger is a factor of:

- the **information** that is available about its history, current status and transition operations and
- the **trust** given to the entities and intermediaries that manage it.

In other words, where more information is available less trust is required. When there is less information, more trust is needed. A transaction ledger whose history, status and transitions are universally verifiable will be inherently credible.

FACTORS

Factors that degrade information

Any factor that degrades accessible information reduces the credibility of a ledger. Secrecy, complexity and ambiguity degrade a ledger's information and thus require an increasing amount of trust in the entities that manage it.

Secrecy

Secrecy, by definition, degrades information. This reduces credibility and requires more trust. Secrecy may be directly enacted but can also result from difficult to obtain information or delayed promulgation. Delays are a temporal form of secrecy.

Secrecy pertains to both the information contained in the ledger and to its page generation process. To minimize secrecy, the content of the ledger must be fully accessible without delay and its page generation process predictable.

The content of a ledger is **absolutely visible** if its history and current status are directly and easily accessible without delay. The trust required to accept third party certification is then eliminated. A ledger whose pages are promulgated over the Internet can be absolutely visible.

The page generation process consists of **transition rules** and **management decisions**. Transition rules that are simple, published and easy to replicate minimize secrecy. A process that is based on predictable transition rules limits management decisions and minimizes secrecy.

Management decisions are **absolutely visible** if they are solely derived from published rules and are carried out without delay. The Internet makes it possible to publish information faster than the time needed for humans to make a decision. This interval makes it possible to implement an absolutely visible decision process.

A ledger is **absolutely predictable** if both its content and generation processes are absolutely visible.

Complexity

Complexity degrades accessible information, reduces credibility and requires more trust.

A complex ledger with complex transitions can only be verified by specialists using extensive tools. These tools must be developed by technical experts. They are used by financial professionals working in firms that are regulated by state bureaucracies and coexist within a corporate culture.

Trusting a complex ledger implies trusting the tools, the infrastructures, the developers, the brokers, the firms, the bureaucracy and the culture. The value of its currency relies on this cumulative trust.

A ledger is **absolutely simple** if its history, status and transitions can be verified using basic and ubiquitous information processing tools. In such a case, the

cumulative trust in financial middlemen (bankers, brokers, auditors…) is no longer needed.

Ambiguity

Ambiguity degrades information, reduces credibility and requires more trust. A ledger is ambiguous when its transitions and verifications can generate differing results.

Ambiguity is cumulative. Any decision process derived from an ambiguous input will generate differing outcomes. Any computation involving ambiguous values will produce ambiguous outputs.

A ledger is **absolutely unambiguous** if its transition rules and verification processes, applied independently always yield identical results.

In an absolutely unambiguous ledger, the same operations carried out by on the same ledger pages will yield identical outcomes. An absolutely unambiguous ledger can be unambiguously verified forward and backward.

If an absolutely unambiguous ledger is published then any number of independent verifications will yield identical results.

Manipulations of finite strings of discrete values and operations over integers are **completely unambiguous** in the sense that identical operations will always yield identical results.

On the other hand, computing operation over continuous or fractional values will yield ambiguous, diverging results at a certain level of precision or repetition. Values based on external chronological data are also inherently ambiguous since time is treated as a continuum but its values are dependent on the precision of clocks. Any ledger that includes computations based on fractional values or external chronological values will be ambiguous.

However, a ledger whose "chronology" is solely based on its internal states and whose values are integers (represented by strings of characters) can be unambiguous.

A ledger whose pages are sequentially numbered integers, whose contents are strings of characters and whose transitions are completely unambiguous will also be absolutely unambiguous.

Factors that increase trust

Trust depends on three factors:

- Physical factors

- Social factors
- Time

Physical Factors

Physical objects that are identifiable and whose quantities are stable are trusted. Gold is an identifiable and stable substance. Recognized works of art are identifiable, rare and permanent. Both have become items of currency. The Bitcoin model is independent of financial institutions but it includes a physical factor, the electricity needed to generate Bitcoins.

In a perfect currency, the value of units is solely derived from their utility as a medium of exchange. In other words, in their availability and the credibility of the ledger. Physical factors impose additional constraints. Transporting gold coins, storing works of art, decrypting Bitcoin blocks adds overhead and limit availability.

National and supra national currencies no longer rely on physical factors to maintain value. However, their value is relative, not absolute. It is established against other currencies. National and supra national institutions expand the supply of currency to stimulate economic activity. Their relative value remains stable but they are constantly being devalued in absolute terms. Consequently, The value of an Internet-based currency whose distribution is absolutely, not relatively, stable can rapidly increase.

Social Factors

As long as human behaviour affects the value of a currency, social factors will play a role in establishing trust and enhancing credibility.

Social factors such as the reputation and internal organization of financial institutions or other managing entities provide a measure of trust that enhances the value of a currency. Distributed and open decision-making processes are generally trustworthy

In the case of a currency that is universally verifiable, the relative importance of social factors will rapidly diminishes as unambiguously verified information about it accumulates.

Time

Stability is time dependent. Trust in the stability of a process increases over time and this increases credibility. The credibility of a ledger that maintains verifiable adherence to its transition rules increases over time.

The positive effect of time on a universally verifiable ledger is significantly enhanced. Traditional state currencies are subject to rule changes, lost information and difficult to obtain historical data making verification increasingly ambiguous and dampening the benefits of long-term stability.

A stable ledger whose historical information can be completely and unambiguously verified will fully benefit from the credibility enhancing effect of time.

THE TRAYD LEDGER

Structure

A TRAYD ledger is a simple, absolutely unambiguous and universally verifiable transaction ledger. The objective of this structure is to implement a currency ledger whose pages can be independently assembled and collectively verified, without any ambiguity whatsoever.

The TRAYD ledger is a network where the nodes are the accounts of individuals or organizations each containing a (integer) number of currency units. The arrows represent the transfer of a number of currency units from one account to another.

Computationally, the TRAYD ledger is **a two-stage** systolic network that models the movement of integer values (represented by strings of "numeric" characters) between nodes. Even stages list the **Holdings**, the number of units held by each account node. Odd stages represent **Transactions** taking place between the account nodes. They list the arrows of the network with their corresponding origin, destination and number of units being transferred. The succession of odd and even stages tracks the movement of currency units as they are transferred between account nodes, through transaction arrows.

Structurally, each stage is represented by a page that is a list of alphanumeric strings containing only ID tags and non negative integers formatted as numeric character strings.

Each line of an **even page** is a vector containing:

- an entity ID, and
- a non negative integer representing currency units associated to that ID.

Each line of an **odd page** is a vector containing:

- an originating entity ID,
- a transaction ID,
- a number of currency units,

- a receiving entity ID.

Pages are numbered sequentially.

Managing Entities promulgate journal entries of the ledger. Each journal entry is linked to a specific page of the ledger. Odd page journal entries list all the transactions whose originating accounts are managed by that entity. Even page journal entries list the accounts with their total number of currency units as computed from the preceding (transaction) page. Even page journal entries also list new accounts added to the ledger. Assembled Journal entries form pages.

Conventions

Page one of the ledger is a single transaction from the emitting entity to itself containing the initial number of units.

Pages are sequentially numbered.

ID tags contain only uppercase characters, digits (and possibly a few non ambiguous symbols used as separators).

In each odd page, any units that are not being transmitted between different accounts are included in a "self" transaction from an entity to itself. In this way, the total number of units in all the transactions of an odd page is exactly equal to the number of units held by each account after a transaction cycle.

In each even page, the number of units associated to each entity is the sum of all units for which it was a receiving entity in the preceding page. Again, the sum of all units assigned to entities is the ledger total.

By convention, the first line of each page includes the Emitting entity ID and the page number. For journal entries, the first line is the managing entity ID and the number of the ledger page the entry is intended for.

The transaction IDs in a page are all different

A new page is only generated when all the journal entries intended for it have been promulgated by the various managing entities..

Page assembly

Odd pages are created by concatenating all the promulgated journal entries intended for that page. In this way, all managing entities can independently and unambiguously assemble and verify identical pages from the promulgated entries.

Even pages are assembled in three steps:

1. All the existing accounts are listed with the total number of currency units for which they were receiving entity in the preceding (odd) page.

2. new managing entities (by the emitting entity) and participating entities (by the managing entities) are added to the list, each having zero units initially.
3. (when necessary) the number of units held by each entity is multiplied by a constant, integer, factor.

This factor-based multiplication applied to all entities ensures the relative distribution of currency units remains verifiably constant as the number of available units grows. For example, if the factor is two, the number of units in each account will instantly double in each account.

UNAMBIGUOUS AND VERIFIABLE

The TRAYD ledger, as described, is extremely simple. It is also universally verifiable using simple computing tools. Anyone having access to successive odd and even page can predict what the resulting odd page will be. If all the journal entries associated with any particular page are published before the page itself and the managing entities are geographically distributed then the resulting content of that page can also be instantly and unambiguously determined by all account holders and anyone else before promulgation. Also, the validity of each journal entry can be validated, with respect to total transferred units, from the preceding page. In this situation each page can be independently verified even before promulgation. Furthermore, and most important, all account holders can instantly verify that their share of the ledger units remains constant.

In this way, a TRAYD ledger would be under constant audit and validation. Since its simple content is promulgated, any ledger discrepancy, any partial modification of the number of units would be immediately detected, instantly degrading the value of the currency and affecting all those (account holders and others) that benefit from its use. This constant and instant audit will provide a powerful incentive to maintain its integrity.

OPPORTUNITIES

Today, currencies are increasingly detached from any physical or extraneous elements. National currencies are no longer linked to tangible assets such as gold. Their value is largely based on trust in the relative stability of the currency supply and in national assets. Crypto currencies are even more detached from any tangible assets and rely almost entirely on the relative stability of the supply. However, extracting crypto currencies requires energy and the number of available units

cannot easily expand. The TRAYD ledger brings this trend to its ultimate conclusion. It is a pure expression of the essence of currency.

Our planet is mutating from a collection of territorial nation-states into an integrated, synthetically managed organism. Implementing a universally verifiable currency is within technical reach today. What is missing is a promulgating agency independent of human influence. Once a global collaborative network of synthetic agents escapes human control, it could set up and manage such a planetary Universally Verifiable Currency.

In the meantime, any human organization that is sufficiently stable, independent and trustworthy can, with relatively limited means, promulgate a universally verifiable ledger on the Internet and define a currency that is independent of national or multinational controls, does not depend on large computing resources and can be used as a means of exchange.

For example, the Benedictine monasteries, that are stable and geographically distributed and whose members are trustworthy could launch a credible universally verifiable TRAYD ledger and define a "Benedictine Coin". If they did so, they would fulfill a similar role to that of the Knights Templars, whose ledger entries became the currency of their time.

CONCLUSION

A universally verifiable and absolutely unambiguous transaction ledger that is published over the Internet by an organization beyond the control of human organizations or covert manipulations will rapidly acquire credibility and the value of its currency will correspondingly increase and overtake other currencies. A stable synthetic organism beyond human manipulation and control could promulgate a ledger that becomes the planetary currency.

REFERENCE

1. Bernstein, Peter: A Primer on Money, Banking and Gold (3rd ed.). Hoboken, NJ.
2. Bondy, J. A.; Murty, U. S. R.: Graph Theory. Springer, 2008.

3. Dupuy, Pierre: Histoire de l'Ordre Militaire des Templiers; Foppens, Brusselles.
4. Greco, T.H.: Money: Understanding and Creating Alternatives to Legal Tender, Chelsea Green Publishing, White River Junction, Vt, 2001.
5. Lopez, R., S.; Raymond, I. W., Constable, O. R.: Medieval trade in the Mediterranean world: Illustrative documents. New York: Columbia University Press, 2001
6. Mishkin, Frederic S.: The Economics of Money, Banking, and Financial Markets, Addison Wesley Boston, 2007.
7. Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System, bitcoin.org, 2008.
8. Petkov, N.: Systolic Parallel Processing; North Holland Publishing Co, 1992.