# ChainCash - elastic peer-to-peer money creation via trust and blockchain assets

kushti, scalahub

February 13, 2023

**Abstract**

In this paper we introduce ChainCash, a protocol to create money in self-sovereign way via trust or collateral, with individual acceptance.

## 1 Introduction

Currently, most of monetary value is created by private banks (often, offshore banks as in so-called "eurodollar" system [1]) following central banks requirements. As an alternative, starting with Bitcoin [2] launch in 2009, a lot of cryptocurrencies and DeFi applications on top of public blockchains are experimenting with money issuance. As another alternative, we also have alternative, usually local, monetary systems, such as LETS (local exchange trading systems), timebanks, local government currencies, and so on. Traditional fiat monetary systems usually possessed by big players (with rich getting richer effect) creating money in non-transparent ways (especially in offshore parts) without reasonable limits, on the other side, they have better supply elasticity. Cryptocurrencies (and, sometimes, application and other tokens on top of public blockchains) are usually more decentralized, have known emission schedule, which makes them appealing assets, on the other hand, supply is disconnected from economic activity and not elastic. Local currencies usually considered more fair in segniorage distribution than fiat currencies, they are successfully boosting local economies often, but, in opposite to fiat and crypto-currencies, they are not global and universal. kushti notes : add citations

In this paper, we propose ChainCash, a new global kind of money, with decentralized issuance, elastic supply, and also backed (not necessarily though) by collateral.

We consider money here via its medium-of-exchange property. For existing currencies, there are usually many options to represent value, such as coins, paper or plastic banknotes, digital records in different ledgers, etc. For ChainCash, we define money as a set of digital notes, each has some nominal (not fixed but arbitrary on our case). Value of a note is nominated in some existing unit-of-account, such as gold. Consider that an economy is consisting of known

agents $a_1, ..., a_n$. Then we can define medium-of-exchange property of money via a set of agents accepting monetary objects (i.e. notes).

Usually, set of agents accepting money (local or foreign currency) is fixed. That is, for every monetary object (e.g. a note), an agent is accepting it as a mean of incoming payment, or reject. In opposite, for ChainCash money, similarly to [3], the set is individual for a note, so when agent $a_i$ sees a note $n$, it applies its personal predicate $P_i(n)$ to decide whether to accept the note or decline it.

Then how notes are different in case of ChainCash? We consider that every note is collectively backed by all the previous spenders of the note. Every agent may create reserves to be used as collateral. When an agent spends note, whether received previously from another agent or just created by the agent itself, it is attaching its signature to it. A note could be redemeed at any time against any of reserves of agents previously signed the note. We allow an agent to issue and spend notes without a reserve. It is up to agent's counter-parties then whether to accept and so back an issued note with collateral or agent's trust or not.

As an example, consider a small gold mining cooperative in Ghana issuing a note backed by (tokenized) gold. The note is then accepted by the national government as mean of tax payment. Then the government is using the note (which is now backed by gold and also trust in Ghana government, so, e.g. convertible to Ghanaian Cedi as well) to buy oil from a Saudi oil company. Then the oil company, having oil reserve, is using the note to buy equipment from China. Now a Chinese company has a note which is backed by gold, oil, and Cedis.

Agent's note quality estimation predicate $P_i(n)$ is considering collaterals and trust of previous spenders. Different agents may have different collateralization estimation algorithm (by analyzing history of the single note $n$, or all the notes known), different whitelists, blacklists, or trust scores assigned to previous spenders of the note $n$ etc. So in general case payment sender first need to consult with the receiver on whether the payment (consisting of one or multiple notes) can be accepted. However, in the real world likely there will be standard predicates, thus payment receiver (e.g. an online shop) may publish its predicate (or just predicate id) online, and then the payment can be done without prior interaction.

We propose to implement ChainCash monetary system on top of a blockchain as:

- Blockchain provides instant solution for public-key infrastructure.
- Public blockchain allows for a global ledger solution with minimal trust assumptions [4].
- Global public ledger allows for simple analysis of the notes in existence.
- Smart contracts minimize trust issues in payment execution and redemption. If native blockchain currency and assets on top of it (such as algorithmic stablecoins) used in reserves, trust issues in redemption could

be eliminated at all. If tokenized real-world commodities and fiat currencies (e.g. USDT) are used in reserves, redemption could not be completely trustless (as smart contracts do not have power off the chain), but at least there is transparent accounting in on-chain part of redemption.

We use Ergo as a Proof-of-Work blockchain to implement ChainCash, as it is built on minimal trust assumptions [4], and UTXO transactional model as well as AVL+ trees support are making notes implementation feasible.

# 2 ChainCash Implementation

To implement ChainCash on top of a UTXO cryptocurrency, such as Ergo, two contracts are needed, a note contract and a reserve contract. Reserve contract locks ERGs ro tokens on top of Ergo blockchain and allow to redeem native or custom tokens when a note is presented. Note contract ensures that the note has proper history, allows for not to be split into two parts (payment and change), and allows for note redemption.

## 2.1 Layer1 implementation

## 2.2 Layer2 implementation

## 2.3 Offchain and on-chain part

Off-chain part is the most important piece of ChainCash system, as it allows for recognizing possibly different forms of note and reserve contracts, and also do note value estimation.

# 3 Applications

ChainCash could be seen as a powerful foundation for other monetary systems, and we are going to show it in this section.

## 3.1 LETS

## 3.2 Local Currencies

## 3.3 Timebanks

# 4 ChainCash Drawbacks

# 5 Possible Extensions

## References


[1] F. Machlup, "Euro-dollar creation: A mystery story," *PSL Quarterly Review*, vol. 23, no. 94, 1970.

[2] S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system," *Bitcoin.–URL: https://bitcoin.org/bitcoin.pdf*, vol. 4, no. 2, 2008.

[3] K. Saito, "Peer-to-peer money: Free currency over the internet," in *Web and Communication Technologies and Internet-Related Social Issues—HSI 2003: Second International Conference on Human. Society@ Internet Seoul, Korea, June 18–20, 2003 Proceedings 2*, pp. 404–414, Springer, 2003.

[4] "Know your assumptions." `https://www.ergoforum.org/t/know-your-assumptions/4198`. Accessed: 2023-01-30.