

The technology and potential of Stablecoin

B. Ramamurthy and S. Madurai
bina@buffalo.edu, madurai@buffalo.edu
University at Buffalo, NY 14260-6000

1. Introduction

The innovation of the first working cryptocurrency Bitcoin [1], is two-fold: the feasibility of peer-to-peer digital money without an intermediary and the underlying enabling technology in the blockchain trust layer. Bitcoin is still running strong since its inception in 2009, fully supported by the community and without any intermediary. It is built on a robust scientific foundation of more than 50 years of research in sciences, mathematics, and algorithms. Since the introduction of Bitcoin, the blockchain and cryptocurrency ecosystem has evolved significantly. However, the main idea of Bitcoin, a peer-to-peer currency, is yet to be realized on a practical scale. The main reasons preventing ordinary people from exploring cryptocurrencies are (i) rapid advances in the technology, (ii) lack of practical information and education about blockchain and cryptocurrencies (iii) the high volatility in the prices preventing ordinary people and businesses from transacting in cryptocurrency and (iv) lack of clear policies and regulations governing this emerging area. In this brief, we discuss a technical advancement in a digital currency called stablecoin to address these concerns.

2. Cryptocurrencies and Blockchain

Different forms of currency as a medium of exchange have existed since the dawn of civilization. From a barter system, a system of sea shells and precious stones, to today's central bank-issued paper currencies, the currency system has evolved remarkably. But the financial and technology framework supporting today's currency system is highly centralized, resulting in the global economic meltdown of 2008. Blockchain provides the decentralization infrastructure [2], dis-intermediation through smart-contract-based verification and validation, and distributed ledger technology for the immutable recording of transactions. Businesses and governments, including the Whitehouse [3], seek technological advancement and solutions to support digital currencies and digital assets formally. Given this scenario, we need an inclusive digital currency solution that has a low entry point and is resistant to wild swings in cryptocurrency prices. A promising solution is in a concept called stablecoin. The fundamental concepts and feasibility of stablecoin as the solution for digital currency are explained in this paper.

3. Stablecoins

Bitcoin (BTC) and Ether (ETH) of the Ethereum blockchain [4] examples of native coins are generated as rewards for the decentralized nodes (servers) that maintain the blockchain network, confirm transactions and append blocks of transactions to the blockchain. The coins also are required for paying the fees for the transactions on a blockchain. Depending on the total value locked (TVL), popularity, stability of markets, demand, and the current news, the value of that blockchain's native coin (cryptocurrency) varies widely. This variation in the currency's price is a deterrent for crypto adoption in many business trades where the stability of the value is critical for payment and accounting systems. A stablecoin is engineered to address this stability issue. A stablecoin's value is kept at a constant (standard value of one), managing the volatility that concerns ordinary people and businesses. Consider this scenario: A vendor gets paid for a product, say a printer, in Eth (ethereum native coin). By the time they cash it in and settle the account, assume that the payment in Eth goes down by 25% in value. This volatility results in a loss for the business. This unpredictable instability in value cryptocurrencies is a major hindrance in its

broader adoption. The solution is to introduce a layer of stability while keeping all the benefits of the underlying blockchain trustless system. Besides the stable value, a stablecoin has the desirable properties of blockchain-based cryptocurrency: peer-to-peer transactions among trustless parties, decentralized organization, and transparency.

4. Engineering a Stablecoin

4.1 Architecture

A stablecoin is typically implemented using a token instead of the native coin. The token and tokenization [2] provide a stability layer on top of the volatile native currencies. A token standard on the Ethereum blockchain is defined by ERC20 [5]. The ERC20 interface has a well-defined interface of functions enabling stablecoin's standard operations. Figure 1 shows the ERC20 interface. Thus ERC20 token-based smart contract offers a suitable and convenient architecture for engineering and deploying a stablecoin on the Ethereum blockchain.

Stablecoin isA ERC20/EIP20/ERC20
string name;
string symbol;
uint decimals;
mapping (address-->balances);
mapping (address-->mapping(address->uint)allowed);
function transfer(...)
function transferFrom(...)
function balanceOf(...)
function approve(...)
function allowance(...)

Figure 1 ERC20 Token Interface

4.2 Managing the stable value

There are two major classes of stablecoin based on how their values are maintained and supported: collateralized and algorithmic. A collateralized stablecoin is engineered by using traditional collateral or deposit to manage the stable value of the stablecoin. For an algorithmic stablecoin, special algorithms are used to maintain the value of the stablecoin.

4.2.1 Collateralized Stablecoin

For a collateralized stablecoin, a deposit is held as a reserve. The assets include native coins, cryptocurrency tokens, fiat currencies of the traditional financial system, precious metals (gold), or other physical assets. For example, Dai[6] and USDC [7] are pegged to US dollar (USD), and these stablecoins operate on the Ethereum blockchain. Tether organization has released stablecoins for fiat currencies US dollar, Euro, and Chinese Yuan (USD, EUR, and CHN), and these stablecoins are deployed Bitcoin blockchain. Alchemix [8] uses Dai as the collateral for their finance products.

In the case of the collateralized stablecoin, an issuer such as MakerDAO who issues Dai stablecoin will maintain its value by managing a deposit of fiat currency, in this case, the US dollar, by adjusting the supply of Dai and the amount of collateral. An ordinary user of a Dai will buy and use

stablecoin Dai for business or personal transactions without worrying about its volatility. It is also possible an investor of Dai may build a vault and deposit Dai to earn interest. The user may also borrow against the vault deposits while earning interest. An investor can also participate in online governance by owning governance tokens (Maker). MakerDao collateralizes Dai issued by about 150% of its value with Eth deposits. The Dai stablecoin and ecosystem supports other advanced instruments for users.

4.2.2 Algorithmic Stablecoin

Any emerging technology will inspire innovation: stablecoin is no exception. A totally different approach to maintaining the stable value emerged with algorithmic methods to control the stability. The idea is to pair (peg) the stablecoin with another cryptocurrency to keep the stablecoin value at one. The liquidity, or the number of pegged pairs, the stablecoin, and the cryptocurrency, is maintained by the demand and supply using mint and burn operations. Mint is an operation for creating new tokens. Burn is the operation of removing (deleting) tokens from circulation. When the value of the stablecoin moves above one, the pegged pair's liquidity is balanced by minting more stablecoin, thus increasing the supply and bringing down the price. Simultaneously, the pegged cryptocurrency is burnt to strengthen its value. The degree of mint and burn is determined algorithmically. Thus, the name algorithmic stablecoin.

5. Significance of Stablecoin

Stablecoin is an organic next step in the digitization of fiat currency. Recently White House [6] signed an executive order charging congress and federally supported research organization to report on digital currency and digital assets. The stablecoin concept is the answer that addresses the digital currency quest. More importantly, stablecoin, assured by its stability, offers an entry point for ordinary people to partake in the ongoing cryptocurrency revolution. The potential of stablecoin will be fully realized if the central bank in every country issue stable currency collateralized against their fiat currency. The move will enable their subjects and businesses to explore blockchain applications without any concern about the volatility of cryptocurrencies. Given this potential, more research and development is required for engineering a safe and secure model for a stablecoin.

6. References

- [1] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>, 2008.
- [2] Ramamurthy, B. Blockchain in Action, Manning Publishers, NY, <https://www.manning.com/books/blockchain-in-action>, November 2020.
- [3] Executive Order on Ensuring Responsible Development of Digital Assets, <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/>, March 9, 2022.
- [4] Ethereum white paper: A Next-Generation Smart Contract and Decentralized Application Platform, <https://github.com/ethereum/wiki/wiki/White-Paper>, last viewed September 2022.
- [5] ERC-20 token standard. <https://ethereum.org/en/developers/docs/standards/tokens/erc-20/>, last viewed September 2022.
- [6] Dai Stablecoin System, <https://makerdao.com/en/whitepaper#the-dai-stablecoin>, last viewed September 2022.
- [7] A stablecoin by Circle and Coinbase, <https://www.centre.io/usdc>, last viewed September 2022.
- [8] Alchemix Self-repaying loans, <https://alchemix.fi/>, last viewed September 2022.