CRYPTIX
LABS

Stablecoins:
A Gentle Introduction, Part One

Stablecoins are a category of cryptocurrencies that were created in order to mitigate the common issue of price volatility in 'traditional' cryptocurrencies such as Bitcoin and Ethereum.

They do this – as their name suggests – by artificially stabilizing their value by pegging it to the price of a particular asset or bundle of assets. There has been a lot of attention and commentary regarding stablecoins in the last few years, conversation not exclusive to the cryptocurrency space; stablecoins are also being used as a proxy technology for the introduction of national cryptocurrencies[1], and global corporate currencies not backed by any government or single bank.[2] In broad terms, a stablecoin can be described as a cryptocurrency, the value of which is pegged to another asset, gained by providing some asset as collateral.

There are many different iterations of these artificially stabilized currencies; this document serves as an introduction to understanding the different broad categorizations and their inherent pros and cons. There are two main ways of analyzing them: by examining what asset they are pegged to, and examining how they maintain this peg (i.e. their stability mechanism). Each of these aspects has a significant impact on the level of security and stability we can come to expect from these coins, as well as their potential price volatility (i.e. how stable they actually are) and any potential restrictions on their use either now or in the future.[3] Whilst "[a] true stablecoin, often referred to as the "Holy Grail of crypto", would offer the benefits of cryptocurrencies without the unusable volatility […] remains elusive",[4] several stablecoins still offer significant advantages and long-term price stability over more standard cryptocurrencies and will be explored herein.

The first categorization referred to above relates to the asset that backs these currencies and is collateralized on their creation or purchase; whether a stablecoin is fiat-pegged, commodity-pegged, or crypto-pegged.[5] One USDT (Tether's[6] coin) is supposed to always be worth $1 and is collateralized with this amount, one DGX (Digix[7] Gold Token) one gram of gold, and one DAI[8] - although also pegged to the US Dollar - is collateralized by another cryptocurrency, instead of another asset. As a way of categorizing stablecoins, although the relative asset they are pegged to is perhaps of slightly less importance than how they try and maintain their pegged price, understanding what this indicates regarding the sort of system built around a particular coin is still of utmost importance, and will be discussed in this document.[9]

Fiat-pegged coins have several advantages over other stablecoins in that they are relatively simple to implement, as someone merely has to deposit fiat currency as collateral and is given the appropriate amount of cryptocurrency in return. As is the case with Tether, this is a 1:1 relationship, and is thus conceptually simple and removes potential confusion standing in the way of onboarding. Furthermore, it requires the least amount of development of all the above referenced coins in order to create and maintain, as there is little blockchain-specific development required. However, these advantages are arguably outweighed by the type of system that this sort of collateralization mechanism necessitates: currencies that must be regularly audited in order

to maintain trust that the currency is actually backed by the corresponding amount of fiat currency, maintaining as they do a close similarity with the sort of banking systems that cryptocurrencies were initially created in order to escape from. With fiat-backed currencies there must be a central party – or at least a centralized set of parties – controlling the bank accounts within which the fiat backing is contained, and thus cannot be said to be greatly (if at all) decentralized. Indeed, it is this form of stablecoin that is being touted as the model to follow for many national or international 'digital currencies', notable mentions being China's state-backed cryptocurrency,[10] and the much-discussed European Union cryptocurrency that has been discussed by the ECB. For the sake of brevity, all that will be said regarding commodity-pegged cryptocurrencies is that they suffer from many if not all of these same issues, and thus can be considered the same as fiat-backed stablecoins for the purposes of discussion.

Cryptocurrency-backed stablecoins such as DAI require a far more complex technical system than fiat-backed coins, and also suffer from the same onboarding issues as many other cryptocurrencies. However, they have historically been more reliable than fiat-backed coins,[11] and are far more decentralized with regards to their technical architecture. Overall these benefits significantly outweigh the disadvantages, which are in fact typical of cryptocurrencies and blockchain technology overall.[12] Although on the surface the process of getting a stablecoin such as DAI is much the same as with a fiat-backed coin such as Tether, under the hood the processes are quite different. MakerDAO, the creators of DAI, utilize a series of smart contracts in order to achieve price pegging alongside the use of a volatile asset as collateral. That all of the coins utilized in these stablecoins exist wholly on the blockchain, they are publicly visible on a block explorer, ensuring that there is no need for audits in the traditional sense, and the price of the currency is maintained by logic embedded within smart contracts.

Just how cryptocurrency-backed stablecoins ensure their price remains truthfully pegged to something like the US Dollar brings us to the end of part one of this two part series, as it requires discussion of the other of our two categories of analysis: the stabilization mechanism utilized by cryptocurrency-backed stablecoins. They use cryptocurrencies as collateral, yet the value of this asset is incredibly volatile: the amount of the asset (e.g. $100 worth of ETH) originally supplied as collateral for (e.g.) 100 DAI might be worth far more or far less mere hours after the purchase of the DAI itself. They do this via complex stabilization mechanisms baked

into the cryptoeconomic design of the smart contracts, which are enabling one of DeFi's most significant advances to occur, and will be covered in detail in part two.

[1] https://www.forbes.com/sites/billybambrough/2019/09/14/the-real-threat-to-bitcoin-crypto-and-facebooks-libra/
[2] The most well-known of these being Facebook's Libre: https://libra.org/en-US/
[3] This information can be used as a rough watermark for how 'decentralized' they are in the sense of their being censorship and collusion resistant, in a broader sense.
[4] https://arxiv.org/pdf/1906.02152.pdf
[5] Although there are instances of non-pegged stablecoins which – as the name suggests – are not pegged to the price of a particular asset, these are not particularly stable as they rely on constant growth in order to maintain price stability, and thus will be omitted from this document.
[6] https://tether.to/
[7] https://digix.global/#/
[8] https://cryptonews.com/coins/dai/
[9] Discussion of the second categorization referred to above – the stability mechanisms implemented by the surrounding system of a stablecoin – will be discussed in part two of this document.
[10] https://cryptopotato.com/china-to-reportedly-launch-gover ment-backed-cryptocurrency-in-novembe/
[11] Even considering that currencies such as DAI are slightly more volatile in value than their fiat-backed cousins, as outlined here: https://medium.com/coinmonks/how-well-do-the-top-stablecoins-perform-a-quantitative-analysis-c56d022719b
[12] And thus are not only being worked on by developers involved in stablecoin projects.