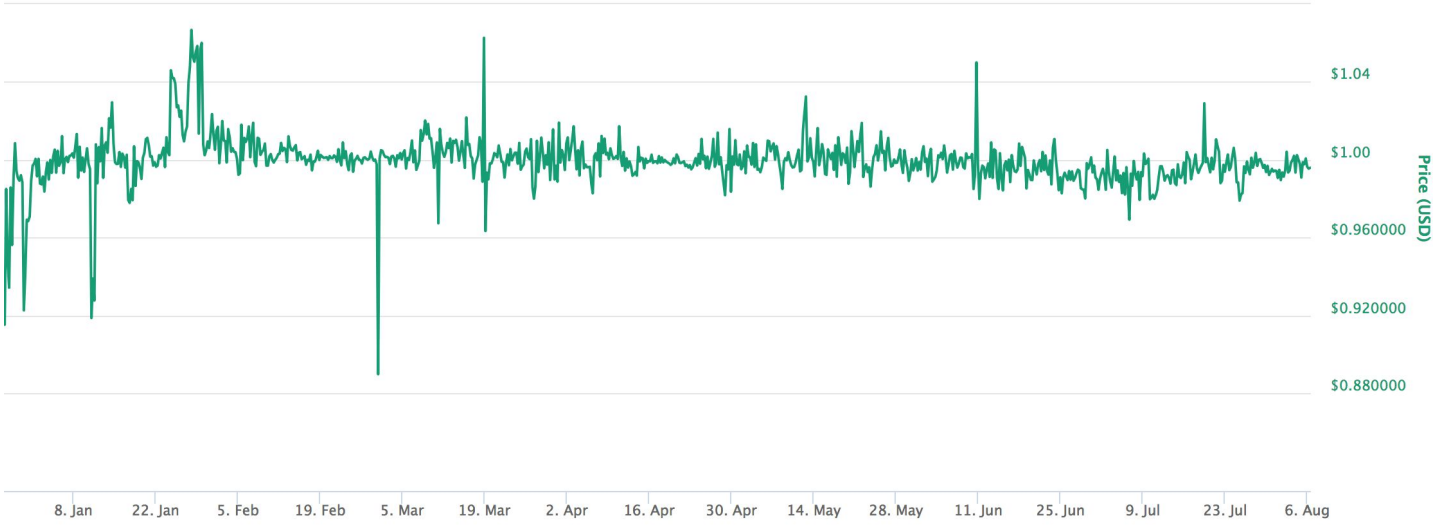
RESEARCH REPORT

Stable Coins

INTELLIGENT
TRADING

(Not so) Stable Coins

Date: 06-August-2018



DAI price chart; source: CoinMarketCap

Summary

The emerging segment of stable coins comprises a lot of controversiality. Some proclaim the stability to be the holy grail of crypto, solving the issue of volatility and opening a path to mass adoption. Others oppose with criticism of stable coins, arguing they compromise the ground ideas of cryptocurrencies. There surely are challenges and issues, such as centralization and trust. However, the sector possesses opportunities to address the market of all of the money in the world by offering a superior solution. This ambitious vision requires tremendous responsibility from the creators of the stable coins. The question is if the developers will be able to meet the expectation while complying with the economic principles of price creation, an open market and pegged exchange courses.

Strengths & Opportunities

- The stability provided for the volatile crypto market
- A strong interest of influential investors and institutions
- Targeting the total addressable market of all money in the world
- Providing an alternative to failed fiat currencies which suffer from hyperinflation

Weaknesses & Threats

- Failing to provide a universally accepted solution that provides privacy, security, and decentralization at the same time
- Need to ensure a trusted data feed from the market
- Vulnerable to regulations and market crashes
- State-issued stable coins as a potential competitor
- The possible threat of stable coins being used for bitcoin price manipulation

Stable Coins

The issue of volatility
- Brief History of Cryptocurrencies
  - Cryptography
  - Digital Money
  - Inception of Bitcoin
- Characteristics of the Crypto Market
  - Price of Cryptocurrencies
  - Nascent Market
  - Volatility in Charts

Solutions for Stability
- How Exchange Rate Pegs Work
  - Buy Wall, Sell Wall, Arbitrage
  - How to Create an Exchange Rate Peg
- Methods
  - One-token
  - Two-token
    - Collateralized
    - Not Collateralized
    - Oracles

Market Analysis
- One-token model
- Two-token model
  - Collateralized
  - Not Collateralized

Strategic Analysis
- Strengths
- Weaknesses
- Opportunities
- Threats

Suggestion for Investment

The issue of volatility

Brief History of Cryptocurrencies

Although the cryptocurrencies led by bitcoin are referred to as a novel invention of these past years, the concept and the technology behind it have their own history.

Cryptography

The cryptography as used in the bitcoin protocol is based on the work of Whitfield Diffie, a public-key cryptography pioneer. He solved the problem of distributing the key to encrypt and decrypt messages in 1976. Two years later in 1978, Rivest, Shamir and Adleman first described a public-key cryptosystem algorithm with asymmetric encryption and called it the RSA algorithm (the first letters of the surnames).

The public-key asymmetric encryption algorithm allowed for encrypting messages and publishing a public key to the message. The other party can decrypt this message with a private key, a large number computed from the public key. Due to its computation requirements, the technology was originally utilized only by governments, military, and big companies. This changed when Paul Zimmerman created PGP (Pretty Good Privacy) with the goal to make encryption available to anyone with a personal computer.

Digital Money

The idea of digital currencies, money that can be only owned and transacted in an electronic intangible form, encompasses several variants. Central Bank Digital Currencies (CBDC) are one example, Cryptocurrencies would be another one. Bitcoin, even though it is considered to be the predecessor of cryptocurrencies, was not among the first digital currencies. There were several attempts to create private digital money using the asymmetric encryption through the 1990's.

In 1994, David Chaum invented DigiCash, an electronic currency using a blind signature technology for untraceable payments. What happened however was that all transactions were validated by a centralized company, owned by Chaum, and when the company went bankrupt, DigiCash failed.

Another project introduced in 1997 was Hashcash, a proof-of-work system that was utilized as a countermeasure technique against denial of service. Then in 1998, Wei Dai introduced the concept of B-money, an anonymous distributed electronic cash system. Like DigiCash and Hashcash, B-money was never fully developed, but these three projects were pioneers and set the stage for the year 2009 and the inception of Bitcoin

Inception of Bitcoin

In 2009, Satoshi Nakamoto published a whitepaper on a peer-to-peer electronic cash system, bitcoin. In this paper, he references the B-money paper and when describing the Proof-of-Work system he quotes the Hashcash project. Bitcoin blockchain was made public and the mining of blocks started. The cryptocurrencies at its inception did not have any clear monetary value, they were not traded nor used as a medium of exchange, only mined by crypto enthusiasts.

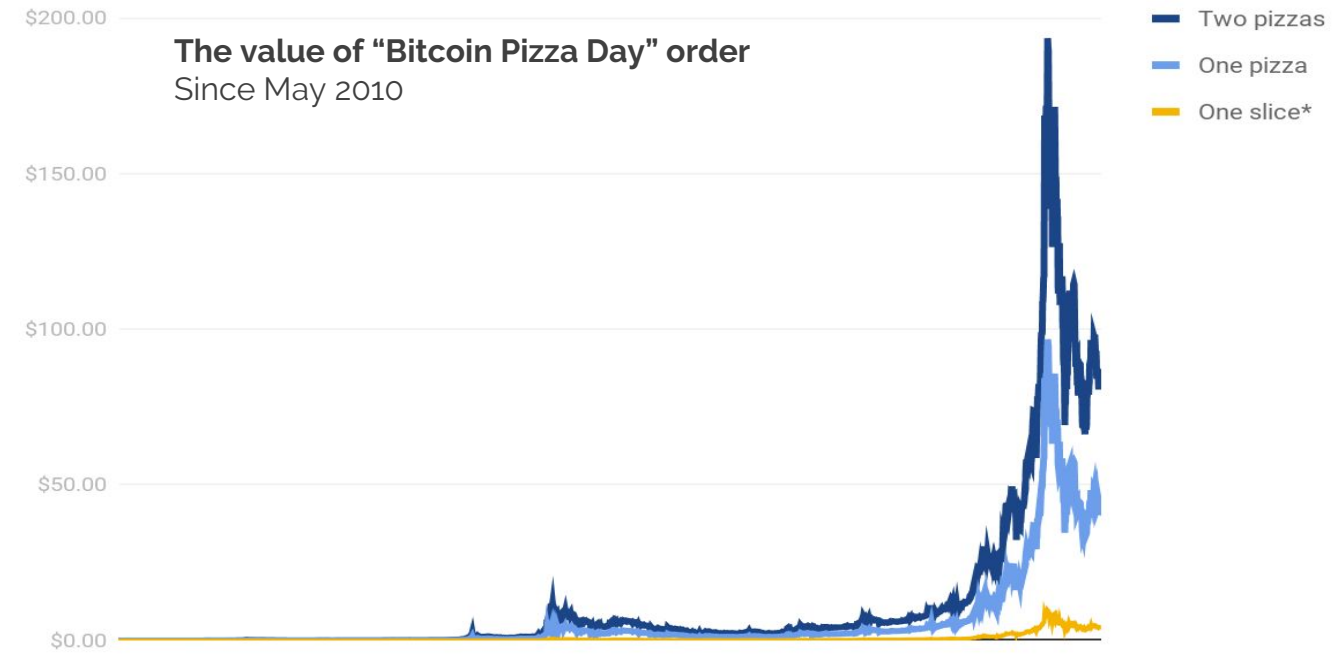
The first time a monetary value was assigned to bitcoin was in May of 2010. On the BitcoinTalk forum, Laszlo Hanyec offered to pay 10,000 bitcoins for two pizzas. At that time, the value of that transaction was around $25 and it got executed and Haynec received two pizzas for the bitcoins. The date marks an important milestone for cryptocurrencies, the first purchase of a physical item with bitcoin. 22 May is celebrated in the crypto community as "Bitcoin Pizza Day".

Laszlo Haynec has become something like a legend in the world of crypto and his pizza purchase a popular symbol. Earlier this year, he recreated it using the Bitcoin Lightning network. The community developed a "Bitcoin Pizza Index", derived from the purchase on 22 May 2010, and they also began the Bitcoin Pizza twitter account devoted solely to the purpose of updating the price of the famous pizza purchase every day.

The issue of volatility

Characteristics of the Crypto Market

Talking about the Bitcoin Pizza Index, we can look at the chart of the updated price of that pizza from the day of purchase to present day. If we were to put together the prices announced on the Twitter account every day, the chart would look like this:



*10 slices per large Papa John's pizza
Source: CoinDesk

When looking at the chart, one thing is obvious. The price of two Papa John's pizzas has changed quite dramatically when paid in Bitcoin. And not only in Bitcoin. Over the following eight years, numerous alternative cryptocurrencies (altcoins) have now emerged, starting with Namecoin in 2011 and adding on with new projects at increasing speed. Today, Coinmarketcap lists over 1736 projects and more are applying each day to be listed.

The reason for new altcoins appearing every day is that although Bitcoin dominates the market, it has several shortcomings. We have described the issue of privacy in our report on Privacy Coins. Another issue represented in virtually every cryptocurrency price chart, not only the one above, is the volatility of the price.

Traditionally, the three functions of any currency are to be: 1) a medium of exchange, 2) a store of value and 3) a unit of account. To fulfill those functions, stability is of crucial importance. In fiat money, the value is backed by governments, with central banks controlling the money supply. Individuals put their trust in government authorities, which is in power to issue new banknotes, influence inflation and the exchange rates.

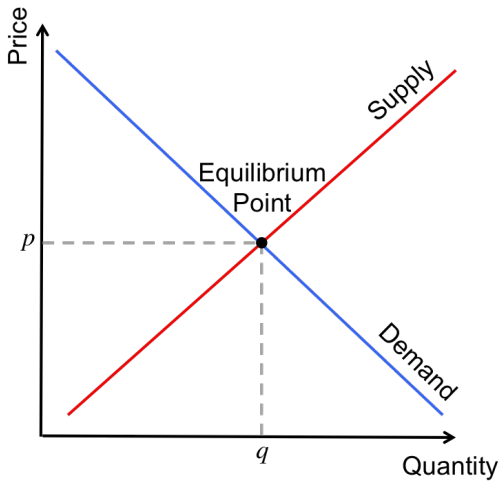
By design. there is no such thing as a centralized authority behind most cryptocurrencies. Also, the vast majority of them follows the Bitcoin example and implements a fixed supply (21 million for Bitcoin), which disables inflation caused by issuing new coins. So what determines the price of a cryptocurrency?

The issue of volatility

Price of Cryptocurrencies

The way the price of the coins with fixed supply (such as Bitcoin) is determined can be compared to any scarce commodity. If there is not a third party to interfere with the market powers, the price is influenced by one of basic economic principles. The law of supply and demand curves, meeting in equilibrium where the demanded amount for a given price is satisfied and the suppliers have sold the maximum amount they were willing to for a given price.

This simplified model can be used to illustrate how the price of cryptocurrencies is created. There are numerous complex forces behind both curves. The demand for cryptocurrencies is influenced by the general market hype, the media, public sentiment and behavioral aspects such as FOMO (Fear of Missing out) and FUD (fear, uncertainty, and doubt). The supply can be altered by burning unsold coins, ICOs, airdrops, forks, bounty campaigns, mining algorithm and more.



The value of each cryptocurrency is determined by several factors, starting with the team strength and experiences, the stage and success of development, the utility of the coin/token, and ending with the proficiency of the marketing team. In the dynamic and transparent world of cryptocurrencies, reputation and image play a crucial role in the success of a project.

Nascent Market

All the factors mentioned above are not stable, they are changing rapidly with the rapidly moving market. When the whole environment is still relatively novel, we are speaking of a nascent market. It is a new, developing market for which the rules are not yet firmly set.

In such a market, there is considerable uncertainty about how the authorities will react. Even though there are some attempts to regulate the market, they are not finalised and not unified either. The market of cryptocurrencies has a global reach, however, there is no united approach to regulations. The rules are not set yet.

What was once an advantage can now quickly become a burden. A large number of new companies and projects are entering the market, new users are adopting the technology and creating new demand. Price manipulations can occur, big players can pull down the price or increase it above its market potential.

The infrastructure is not fully created yet and there are a limited number of exchanges and points of sale. This contributes to the facts that nascent markets have a limited liquidity when compared to established markets. To put cryptocurrencies into perspective, as per an article from May 2018, the amount of physical money (banknotes, coins) was $36.8 trillion. When included the money held in accessible accounts, the number raised to $90.4 trillion. The whole market of cryptocurrencies is currently at $302 billion. That is almost a thirty thousand percent difference.

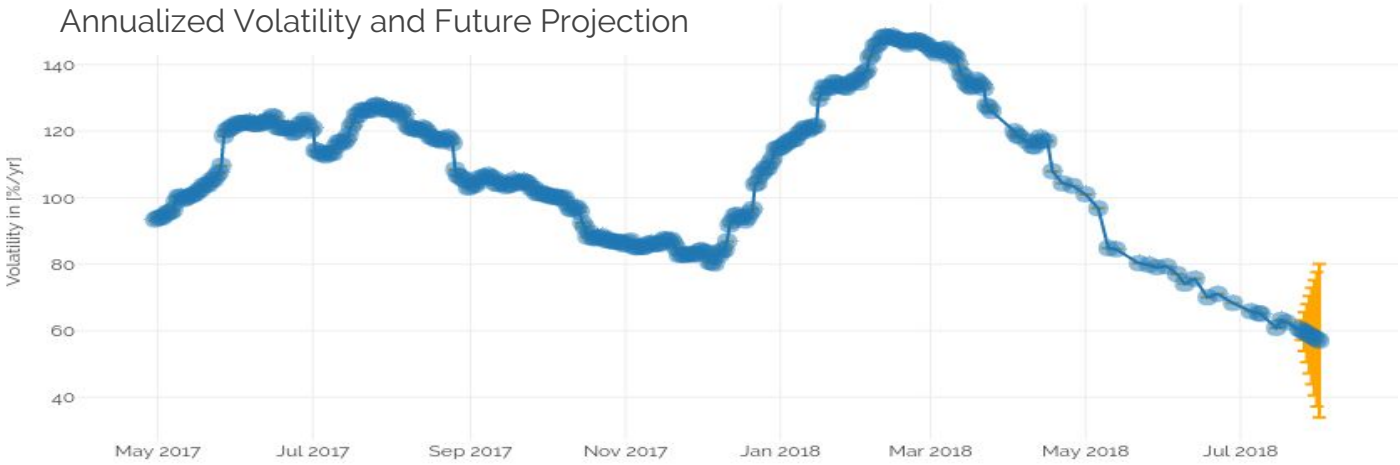
Due to those characteristics, nascent markets are in their nature volatile, move very quickly and thus increase the volatility of commodities traded on them, in this case, cryptocurrencies.

The issue of volatility

Volatility in Charts

We have discussed the origin of cryptocurrencies, the reasons for their volatility and why stability is crucial. Now to connect what we have covered in theory with practical examples, we will take a look at some charts to demonstrate the volatility in crypto markets.

The first chart is a representation of the Cryptocurrency Volatility Index as developed by Sifr Data. This index is composed of six currencies, BTC, ETH, XRP, LTC, DASH, and XMR, weighted by market capitalization. The volatility measures the dispersion of returns on the cryptocurrencies, considering the probability of recording that return and the mean.



The chart above shows a time-series volatility expressed in percent, based on the 90 days of log returns calculated from volume weighted average daily prices. The future projection is shown by the orange dispersion of possible values, slightly more favorable to decrease in volatility. This follows the general trend, however, the value at around 60% is still extremely high. To provide you with perspective, the 12-month S&P 500 Realized Volatility Index is approximately 12.6%.

Volatility of Cryptocurrency Returns

The second chart here shows the 365-day volatility in percent for selected cryptocurrencies. The chart was created with dates from Poloniex on 25 July 2018. On this day, the GLD (SPDR Gold Shares) volatility was slightly above 10%. Bitcoin (BTC), the dominant currency with the lowest volatility, is still reaching values of almost 90%.

Source: Sifr Data

Solutions for Stability

The stability has been proclaimed the holy grail* of cryptocurrencies. With stability as a goal, a new segment originated, stable coins. The ideal form of stable coins combines the advantages of cryptocurrencies with the stability of fiat money (now we are talking fiat like the US Dollar, not like the Venezuelan Bolivar, Zimbabwean dollar or Argentine Peso).

The ultimate goal would be to have a coin that is decentralized, private and scalable and at the same time stable. If the stability is translated in a peg to a certain asset, the coins should also be convertible to this asset and parity should be ensured.

How Exchange Rate Pegs Work

The principle of a currency peg is not new, it has been used in fixed exchange rates systems for years. There is a list of countries that peg their currency to more prominent currencies such as USD or EUR. Fixing the exchange rate against another currency often leads to inflexibility and can be difficult to maintain. However, virtually every stable coin design implies a peg. This is why it is important to learn more about how exchange rate pegs work.

Mostly, stable coins peg to the US Dollar in a way that one coin equals $1. There are other assets stable coins can be pegged against, for example, gold. To explain how the peg works, we need to describe the three background concepts: Buy wall, Sell wall and Arbitrage.

Buy Wall

A buy wall occurs when there is a large bid (or a number of bids) for a single price. This creates a buy support and the buy orders exceed the sell orders significantly, increasing the market price of the asset. The picture on the right shows a monster buy wall on GDAX on an Ethereum depth chart from a year ago. The steep trend shows that the price was likely manipulated. Even though it was most probably created artificially, it is a clear example of the buy wall.

Source: Reddit

Sell Wall

A sell wall is the exact opposite of the buy wall. This occurs when the sales offers exceed the buy bids. This trend is stopping the price of an asset from going upward. On the right, you can see an extreme example of a bitcoin sell wall (again, created by manipulation by a huge player) on GDAX from the last year.

Source: Carter Thomas

Arbitrage

The term arbitrage means buying an asset at a low price and selling it at a high price at the same time, earning profit on the difference between prices. To demonstrate on a simplified example, it would mean buying 1 unit of a cryptocurrency for $20 on GDAX and at the same time, selling the exact same amount on Binance for $25. The purchase on GDAX raises the market price and lowers the price on Binance. This keeps the price more or less even on all exchanges, supposing that there is not a sell wall on GDAX or a buy wall on Binance.

*Haseeb Qureshi, Nick Tomaino, Forbes, Crypto Future Wealth, Steemit, Bitcoin Talk

Solutions for Stability

How to create an exchange rate peg

Creating a peg would simply mean putting the above described fundamental concepts together. To peg a currency A to a currency B, a buy and a sell wall between those two currencies have to be maintained on a certain exchange. If the party establishing the peg does not run out of currency A or B, the market price on that exchange will remain fixed. On other exchanges, arbitrage maintains price stability.

Put like this exchange rate pegs sound fairly easy. However, it is noteworthy that they can be rigged, manipulated, and often fail. To ensure convertibility and parity of the pegged pair, the system needs to be 100% collateralized. This is capital intensive and can be sustained only as long as the party maintaining the peg possesses enough funds. When there is not enough capital to make up for the differences between the market price and the target price, the peg breaks.

There are numerous examples of failed pegs in the history of fiat currencies. In 1992, an economy-hacker from Hungary George Soros led a group of speculators that outsmarted the European Exchange Rate Mechanism (ERM). Black Wednesday cost the United Kingdom £3.3 billion.

More recent example of a failed attempt to peg currencies is the Zimbabwean dollar. After a history of currency crisis starting in late 1990s, inflationary practices of the central bank and over a billion percent hyperinflation, the Zimbabwean dollar was suspended.

Methods

Now that we know what an exchange rate peg is, the fundamental concepts behind it and the simplified mechanism of creating the peg, we can take a look at how stable coins aim to achieve this.

In general, their methods can be divided into two main classes, a one-token model, and a two-token model. The first of the two is quite simple, a mostly centralized, IOU* model. The second uses a more complex mechanism to maintain the peg. An important distinction between those two models is that whereas the one-token model is not investable, the two-token model offers investment opportunity. We will explain how further below.

One-token

The traditional one-token stable coins are using off-chain assets as a collateral and issuing blockchain-based tokens that correspond to that asset. This maintains a buy wall in the size of 100% of the circulating supply of the stable coin. If the issuer is trustworthy, there should be no problem sustaining the peg.

There are several assets used for collateral. Stable coins are backed by USD (Tether, TrueUSD from TrustToken, Circle USDCoin), by gold (ZenGold, Currensee, and more), or a basket of assets (Globcoin backed by fifteen currencies and gold, AAA Reserve backed by several currencies, government-backed bonds, and AAA-rated credit investments).

There are two main issues with the centralized one-token stable coins: 1) the mentioned trustworthiness of the issuer, and 2) the centralization aspect. This is disabling the advantages of cryptocurrencies, namely decentralization and the trustless ecosystem and creating two potential risk factors: 1) the risk of the issuer corrupting the trust by not keeping the claimed collateral and 2) the risk of governmental interventions focusing on the centralized issuing company or collateral storage.

*Informal document that acknowledges a debt owed, phonetic abbreviation of "I owe you"

Solutions for Stability

One-token

Centralization and trustworthiness

These issues and risks connected to stable coins lead to an uneasy situation. Trustworthiness can be ensured by an audit mechanism. The more detailed and objective (ideally done by a third party) the audit is, the more credible is the claim of collateral. On the other hand, when there is no information about the collateral (e.g. not even disclosing the location), the system can be better protected against governmental freezes and reversals of funds.

There are attempts to decentralize the governance of one-token stable coins, implementing DAOs with an on-chain voting scheme, as in gold backed Digix. The gold collateral is centralized, stored by ValueMax in a vault in Singapore, and the governance of the project is decentralized. The DGD token grants voting rights and DGX is the stable coin. DGX holders pay fees to cover the expenses for storing and securing the gold, which should be waived in the first year of operations of the project.

However, even if the governance will be decentralized, it would not ensure decentralization of the system. When the stable coin is pegged to USD, the underlying asset is centralised and it can be inflated by central governments.

As already outlined, one-token based stable coins are generally not investable. If the peg is maintained, the only gains that the investors can expect come from if the underlying asset increases in value. So in a way, that would mean investing in USD or gold but without compensation for the risk of limited liquidity or trusting a middle-man (issuing party).

Two-token

The two-token approach is based on a model in which the one token is stable and the second token is designed to perform corrections in case of fluctuations. In the case of the centralized one-token based model, the price is not created on the market, rather the price is prescribed to the market by the issuers who use assets to back up this proclaimed price. When the stable coin price is created on the market, there is a limitation in ways the price can be influenced.

The demand, as explained in the section Price of cryptocurrencies, consists of several factors which the issuer can seldom control. The supply, on the other hand, is determined mostly by the issuing party. That is why the supply is used to influence the price, contracted when the price is too low and increased when the price is too high.

In the two-token model, the supply is dynamically decreased by buying the stable coins in exchange for the volatile token. and increased by issuing free coins for the holders of volatile token. The idea of an elastic supply was introduced in 2014 in a paper by Robert Sams A Note on Cryptocurrency Stabilisation: Seigniorage Shares.

In his paper, he outlines the issues of currencies being held for future return, not spent or not traded. This notion dates far back, mentioned in economic theory of the the 17th century. Deflationary cryptocurrencies brought several practical examples of this problem. Sams offers a solution in the form of seigniorage share.

In his proposed method, there are two coins, one that acts like money, an object of stabilization, and one that acts like shares in the system's seigniorage*. The swap between those two is on a voluntary basis and is incentivised by a profit. When the market price of the coin changes, the supply needs to change by the same ratio.

Solutions for Stability

Collateralized

This principle was adopted in the two-token approach in two ways. The first was by creating a crypto collateral, which could be locked in a smart contract and thus held trustlessly. This on-chain collateral serves as the seigniorage shares, enabling the minting of the stable coins. To withdraw the locked crypto-asset, the stable coin loan must be repaid into the smart contract.

This is the mechanism of creation and destruction of stable coins backed by crypto collateral. If the price goes up, the system mint more stable coins, increasing their supply and decreasing the price. If the price goes down, the system burn more stable coins, decreasing the supply and increasing the price.

The incentive for increasing the supply when the price is up is based on making the condition of the loan favorable towards stable coin creation. For example, if the price increases to $1.01, the terms for deposit of collateral are for example $9 worth of Ether to get $10 worth of stable coin. The incentive encourages more people to deposit the collateral and **increase** the supply by minting the stable coin.

When the price decreases, the mechanism works in reverse, making it more favorable to close the loan and withdraw the collateral. For example, the users locked Ether in the past and minted $10 worth of stable coins. When the system needs to **decrease** the supply of stable coins, it makes new terms for repaying the loan. The users can pay $9 in stable coins to receive their $10 worth of Ether back. This incentivizes them to close their loans, taking stable coins out of circulation.

Examples of this approach are MakerDAO, locking Ether to mint the stable coin DAI, or Havven, using Ethereum collateral to mint eUSD and their own HAV token to mint nUSD, launched in April.

The advantage this approach has over the one-token model is chiefly in decentralization. The trustless nature of smart contracts provides reliability and censorship resistance. On the other hand, the fact that the collateral itself is a volatile asset means that the system fails to implement a strong and predictable currency peg. To mitigate volatility exposure, most of the projects are over-collateralized, but still the risk to a certain extent remains. If the underlying asset declines in value significantly, in case of a “black swan” event, the stable coin will collapse as well.

Not Collateralized

This two-token model is not backed by any asset, off-chain or on-chain. The principle of contracting and expanding supply in order to accommodate it to the market is a direct implementation of the model proposed in Sams’s paper. The smart contract used to issue new coins aims to serve as a central bank in a decentralized, algorithmic way.

There are several ways to control the supply. The most prominent example is the system of “bonds and shares” (introduced in Basis, used in Carbon). When the price decreases and the system needs to decrease the supply of stable coins, it issues “bonds”. Those are actually put options**, offered at some discount to incentivise buyers to pay with their stable coins and thus contracting their supply.

The buyers purchase those options with the belief that in the future they will be able to sell them when the price increases again. This creates the buy wall. Any time the price is under the intended peg of $1, the speculators buy stable coins for the price just below $1. with the purpose to buy shares issued by the system.

*Seigniorage - the difference between the value of money and the cost to produce and distribute it

** An option contract giving the owner the right, but not the obligation, to sell a specified amount of an underlying security at a specified price within a specified time frame. Investopedia

Solutions for Stability

Not Collateralized (continued)

In the reverse case, when the system needs to increase supply and lower the price, it issues new stable coins. These are paid out first to the bondholders and when they are all paid out, the shareholders are rewarded with the rest. The shares represent a claim on future stable coins and are in most systems, while voting rights are associated with the shares.

This system is decentralized and there is no volatile collateral here which could negatively influence the peg when the price drops too low. It can also scale up, responding to the increasing demand. However, the whole system is based on the assumption of future growth. When the price is down, speculators are buying the bonds in belief that it will go up again and they will be rewarded. The growth is supposed to be stimulated by new waves of demand.

The speculators are maintaining the buy wall by believing in the future payback. If they were to lose this belief, they would have no incentive to buy the bonds, taking the stable coins out of circulation. There would be no way to decrease supply and the peg would break.

The issue of future-growth backed stable coins is especially dangerous in the early stage of projects when the growth in demand is not guaranteed by a successful history.

Oracles

When there is a peg to some real asset, like for example USD, the system needs to obtain updated information about the exchange rate between the stable coin and USD. Oracles are the providers of the market information. Even for the stable coins that are the closest to becoming decentralized, there is still the oracle problem. They have to determine the source of information from the market. If they are relying on one source, it adds an element of centralization to the system.

There are different approaches to establishing an oracle in the stable coin system:

1. Trusted oracle
    - Brings centralization, can be manipulated
2. Median from delegated data feeds
    - Delegates elected in stake-weighted voting, can be voted out if they provide faulty data
    - Used in BitShares
3. Schelling point scheme
    - Price inputs are provided by users staking the tokens, weighted by stake
    - Users with value inputs near the median are rewarded with coins
    - Some projects (Carbon) punish users for incorrect forecasting
    - Outliers are smoothed out by using the weighted median and users are incentivised to provide correct answers
    - Introduced by Vitalik, based on the concept of Schelling points
    - Proposed as a solution in the Sams paper, used in Kowala, Basis, Carbon

Market Analysis

To provide a comprehensive market analysis, we will explore each group introduced above to explain the principle on some of the prominent projects that use this specific approach. Further, we will outline a comparison of the two approaches.

One-token model

The one-token model represents the simplest approach to stable coins. That is why it was used in the first stable coins, such as Tether. This model is also leading to centralization, which is why it is favored by authorities such as the major banks, for example, the project from Goldman Sachs-backed Circle. The table below offers a basic comparison, followed by more detail description of both projects.

Tether	Circle
Low-audit, high censorship resistance	High-audit, low censorship resistance
Freedom to transmit capital worldwide	Restricted by regulations
No proven reliability of the peg	Credibility to maintain the peg

Tether (USDT)

Tether is the most prominent example of the one-token model, the first stable coin to reach valuation over a billion dollars. The issuer sells the tokens for $1 each and holds all the dollars from sales as a reserve, Based on the whitepaper, each USDT in circulation is backed by 1 USD stored as a reserve in a bank account. This is also demonstrated on a transparency website, where the company posts their current account balances. However, there is no evidence that the capital is genuinely held by the company and there has been much controversy surrounding whether or not each token is truly backed by fiat USD.

The project is centralized, owned by Tether Holdings Limited, a company registered in the British Virgin Islands. The low-audit character provides censorship resistance, but on the other hand, corrupts the reliability of the project. At the beginning of the year, Tether dissolved their relationship with the auditor company, Friedman LLP, and subsequently issued USDT in the value of $300 million.

In June, they released an FSS report in which they stated that all USDT are backed, however, they did not provide any evidence of this claim. It is also important to note that this report is not an audit, it was conducted by the law firm Freeh, Sporkin & Sullivan LLP (FSS), not the original auditing firm. The report is based on data gathered over two weeks during which the firm had access to company accounts in two banks. FSS chose the date 1. June to provide a snapshot of the balances in those accounts, which was a bit over $2.5 billion.

Tether has the second highest trading volume, after Bitcoin, and the BTC-USDT fraction of Bitcoin trading is relatively significant. This enhances the potential danger of USDT being printed without the reserve since they can be used to inflate the Bitcoin price. A study examining the evidence of Tether being used for Bitcoin price manipulation during the 2017 peak showed a pattern of Bitcoin price support.

Market Analysis

Circle USDC

Circle announced a stable coin backed by USD in May of this year. The project has raised $110 million in fundraising led by Bitmain, mining hardware manufacturer. The project is supposed to be released this summer, creating an ERC-20 token backed one-to-one by the dollar.

Circle is registered as a Money Services Business under US money transmission laws and promises to begin publishing USDC-related audited financial statements after the launch of the project. The token serves as a credible and stable mediator between the USD and Ethereum ecosystem. However, it is highly centralized and subject to regulations.

When we compare the one-token models to the two-token models, we can create a summary of the most distinctive features in which they differ. In each group, there are differences in approaches. We have already outlined those for one-token based models and will continue with a more detailed description for the two-token models after comparing both groups.

One-token model	Two-token model
Centralized	Decentralized
Require trust in the issuer	Trustless
No investment opportunities	Opportunities for investment in a volatile coin
Limited scalability	Potential for scalability (not-collateralized)
If honest, secure against crushes	Vulnerable to crashes

One-token models provide more reliability if they are honest with the reserve they hold. The collateral protects the stable coins, promising users the option to redeem their deposits. However, there are several issues with this model.

Centralization is one of issues. It increases exposure to regulations and a centralized monetary system created can be compromised. The issuer can deny the redemption of funds, something that Tether stated in their update in 2017 that they "reserve the right to selectively deny redemption and creation of Tethers on a case-by-case basis".

The third party's reliability and required honesty is also a shortcoming of the one-token model. This eliminates one-token models from utilizing a trustless environment, a native advantage of decentralized cryptocurrencies.

Market Analysis

Two-token model

In the two-token model, the structure is decentralized and utilizes smart contracts to create a trustless system. The flexible supply creates the potential for scalability, together with an opportunity for investment. On the other hand, these systems are vulnerable to crashes, either when the crypto-collateral drops in price or when the investors stop believing in the future growth of the stable coin.

Collateralized

The crypto-collateralized coins win confidence by locking up with another cryptocurrency, specifically and mostly those with a high liquidity (like Ethereum). These projects are frequently over-collateralized to provide a reserve in case of price drops. Two of the most prominent examples, Havven and MakerDAO both started with locking Ethereum as a collateral to their stable coins.

Dai by MakerDAO (DAI)

DAI coin launched in December 2017 as a project of MakerDAO. The platform issues two tokens, MKR is the governance token and DAI the stable token. The majority, over 67% of MKR is held by only three wallets and the MKR voters choose the oracles (the second model as described previously).

Dai coin is issued when users lock their ETH in a smart contract through the Maker webpage. When the user repays the DAI into the smart contract, they redeem their ETH and DAI is destroyed. To incentivize users to create and destroy DAI, which increases and decreases the supply, Maker uses the system as described: they modify the terms of opening/closing an ETH backed loan.

As with other crypto-collateral stable coins, the instability of the underlying asset has been a subject of criticism. The over-collateralization is one attempt to deal with it, Maker introduces an additional mechanism titled in their whitepaper 'Automatic Liquidations of risky CDPs'. This should serve as a safety net in case of a price drop in ETH, selling of ETH for DAI, which is then burned.

Havven eUSD and nUSD

Havven is the project that raised the most funding from the Australian cryptocurrencies with the token sale closed in February at $30 million. On April 11 they launched eUSD, and then, as stated in their whitepaper in order to scale, on June 11 nUSD. The first, eUSD is backed by ETH, the second is collateralized by the platform's own token HAV. Nomin (nUSD) is the stable coin, havvens (HAV) are volatile. The users that hold havvens are rewarded by the transaction fees from the network.

The locked up value of havvens is also over-collateralized, based on the collateralization ratio. This is the ratio of the market cap of havven to the market cap of nomins. The price of havvens (P_h) is created in the open market, influenced the by demand and there is a certain supply of nomins (N) that gives the stable coin the price $1. This circulating amount is controlled by tweaking the C, collateralization ratio.

$$C = \frac{P_n \cdot N}{P_h \cdot H}$$

The decentralized oracles are based on a whitepaper still under development, as well as improved fee structures with dynamic fees and hedging charges,

The Havven project validated their code via a third-party security analysis and has undergone an economic audit by Sigma Prime and Bloctrax.

Market Analysis

Comparing collateralized on not collateralized two-token based models shows advantages and faults of each system. Both models are more crypto-native in comparison to the one-token model. They are decentralized and maintain trust through cryptography and transparent blockchain algorithms.

The crypto-collateral enables fast and cheap liquidation into underlying crypto collateral, based on a simple blockchain transaction. On the other hand, it also exposes the stability to the movements in the volatile crypto asset. What is more, when the asset is locked in the smart contract, it cannot be utilized elsewhere or invested to make additional revenue.

Non-collateralized projects are more vulnerable in the case of a crashes, as they cannot be liquidated in any underlying asset. The fact that the stability depends on future growth has both advantages and weaknesses. On one hand, it is beneficial that the stable coins are risk-independent of other currencies. On the other hand, the project has to maintain growth in order to be able to incentivize the system maintenance.

Two-token collateralized	Two-token not collateralized
Fast and cheap liquidation	Cannot be easily liquidated in case of crash
Stability depends on the value movement of underlying currency	Stability depends on trust in future growth
Inefficient use of the capital locked in the contract	No collateral required, no idle capital

Not Collateralized

Basis

The most prominent example of two-token, non-collateralized stable coins is Basis. The project recently raised $133 million from investors such as Polychain Capital, Pantera Capital, and Andreessen Horowitz. This has drawn our attention to the project and we will be writing the next Project-specific report (previously Cardano, DeepOnion, Zcoin) about Basis, analyzing the project in more detail.

Carbon

Carbon stable coin was introduced in April this year and the coin is still currently unreleased. Investors of its $2 million seed funding include General Catalyst, Digital Currency Group, FirstMark Capital, Plug and Play Ventures and The Fund.

The volatile token is called Carbon Credit and is used to stabilized the dollar-pegged coin CUSD. The Schelling oracles check the price every 24 hours. When the price is below the target, the smart contract starts offering Carbon Credits in an auction in exchange for CUSD. The CUSD coins are then burned, reducing the supply. To increase the supply in the case of the price rising above the target, free coins are minted and distributed to Carbon Credit holders.

Strategic Analysis

Strengths

The most obvious strength of these altcoins is the stability they promise to provide. With the speed and global availability of cryptocurrencies, they may serve as a great medium of exchange. However, the volatility and fluctuation of prices stop them from becoming a storage of value or an accounting unit. If the projects were to offer a satisfying solution to those shortcomings of crypto, it could be the next step towards a crypto enabled economy.

The great interest of the big names both from the crypto world and from the investors and banks outside of cryptocurrencies represents an advantage, fueling development of stable coins with solid funding.

Weaknesses

There are still several issues that stable coins have to solve. Depending on the method used, the weaknesses differ. However, generally speaking, no project has been able to come up with a solution that would be universally accepted and provide privacy, security, and decentralization.

One-token models are centralized, compromising the trustless character of cryptocurrencies. This makes them highly vulnerable to potential fraud. Stable coins backed by a collateral are dealing with the scalability issues and with inefficient use of capital when they lock the collateral in a smart contract. The two-token models are fragile to the market crashes. All stable coins need to ensure a trustworthy source of data from the market.

Another area of concern lies in the fact that most stable coins are pegged against USD. This may be problematic to some crypto users since it creates a dependency on the American Federal Reserve. Ferdinando M. Ametrano proposes in his paper "Hayek Money The Cryptocurrency Price Stability Solution" to use a basket of commodities as a benchmark for stability.

There are several critics of stable coins, the most vocal of them to be Preston Byrne, founder and former COO of Monax. Bryne criticizes the assumption that stable coins will always be able to incentivise users of their system to purchase their coins and maintain the peg. He argues that the price should be determined by the market, not prescribed to it.

Opportunities

There is ample opportunity for stable coins. The shared goal of the whole sector to become global, fiat-free digital cash targets the total addressable market of all the money in the world. If there were a stable coin that combined the advantages of cryptocurrencies with the stability of fiat money, it would offer a solution to those without access to a stable store of value, An example of such targeted users can be citizens of countries suffering from hyperinflation.

Stable cryptocurrency can serve as a sound foundation for a global crypto-based lending and derivatives market. This could be the next step to mass adoption of cryptocurrencies. The fact that huge banks such as Goldman Sachs (Circle) are looking into stable coins signals the potential of these projects.

In this report, we have covered just some of the most prominent projects as examples of the different approaches to creating a stable coin. However, there are numerous new projects emerging and there has been a lot of interest shown in these. The investments into stable coins serve as a sign of opportunity for the project that would be able to provide the promised features.

Strategic Analysis

Threats

The sector of stable coins is exposed to several threats and challenges. The threat of regulations and a market crash is relevant for all cryptocurrencies, however, the characteristics of stable coins make them especially vulnerable to those.

The centralized one-token solutions are exposed to governmental interventions and can be disabled by regulatory authorities. The two-token models rely on a growth of the cryptomarket, either on the underlying asset or on the growth of demand for the stable coin itself. This demand would be influenced by the situation in the whole market.

A potential threat from governments is not only in the jeopardy of regulations but also in the threat of competition. State-issued stable currencies have already been drafted by several countries. The Russia Blockchain Association announced the launch of CryptoRuble set for the middle of next year, Kyrgyzstan started to prepare for gold-backed state-issued stable coin in 2017 and the Swedish considered IOTA for their e-krona.

Whether those attempts are to be successfully launched and adopted is yet to be seen. An infamous example of such an attempt was the Venezuelan Petro, a state-issued stable cryptocurrency that was supposed to be backed by the oil reserves of Venezuela, announced in December 2017. Pre-sale started in February 2018 and according to President Maduro, raised $735 million. However, there was no evidence of the investment being executed. The opposition declared Petro illegal, unconstitutional and corruptional. It has also been questioned whether or not the Petro was a genuine cryptocurrency, as it can simply be characterized as an oil future.

The threat of state-issued stable coins is not a reality yet. On the other hand, the potential threat of stable coins being used for bitcoin price manipulation was already mentioned. Also, the responsibility for such projects is enormous. If stable coins were to be adopted as a substitute of governmental currencies that failed to provide a stability to all nations, the potential crash could be devastating.

Suggestions for Investment

Currently, the whole sector of stable coins is highly experimental. New models and methods are being tested and in order for them to be verified, there has to be a longer period of maintaining the peg. We have explained the two models and why the two-token model bares the potential for investment. In the report, we have also covered the weaknesses of each approach.

The nature of stable coins is different from other cryptocurrencies, which can serve as a speculative asset. The two-token stable coins are betting on the future growth of the market and increasing demand. This poses a potential risk to both users and investors. Also, the ultimate goal of stable coins is not to serve as an investment, but rather as a store of value.

However, there certainly are opportunities for the sector. Reputable investors have proven their interests and big banks and even governments are also looking into the potential of the sector. In terms of choosing between the two options within the investable two-token category, the collateralized tokens promise better security in terms of being backed by an established cryptocurrency, as this helps with easy liquidation. The self-reliant model based on future growth is more vulnerable in the early stage of existence. That is why it may be more reasonable to withhold investments before these coins can prove themselves in the market.

Be confident about your next cryptocurrency trade

Intelligent Trading Foundation provides you with concise cryptocurrency trading insights so you can make the right trading decision, every time. Take advantage of upside movement, and help manage downside risk.

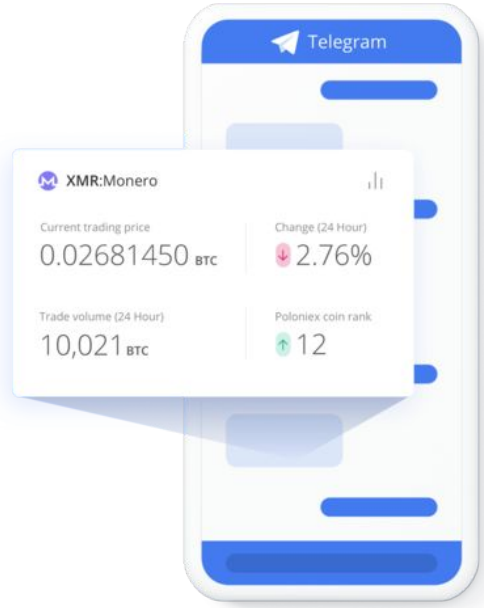
Get real-time notifications when the market is trending

Our Telegram Bot monitors thousands of real-time data points, identifies opportunities using machine learning algorithms and technical analysis, then provides you with actionable alerts you can trade on.

Act on every opportunity
Our technology does all the grunt work so you can focus on making trades, instead of sorting through massive amounts of data.

Protect your downside
We inform you when the market is trending up, and when it is trending down, so you can minimize your risk and maximize profit.

Easy to understand
The alerts you receive are concise so you will immediately know what action to take, even if you are new to crypto trading.



Make sense of all the noise with easy-to-understand crypto trading alerts. It's the smart way to trade cryptocurrency.

Get free access to the ITF Telegram Bot today!
Visit https://intelligenttrading.org to learn more.

Disclaimers

ITF, is engaged in providing trading services to the cryptocurrency trading market. Through its bot and other services it alerts its subscribers/followers ("Users") to certain market conditions based on those Users' preselected settings and trading preferences. Additionally, ITF does make available, from time to time, written or electronic communications that include research analysis, and/or a opinions concerning the DLT/cryptocurrency markets ("Reports"). The views expressed in such Reports are based solely on information available publicly/internal data/other sources believed to be true. The information is provided merely as a complementary service and do not constitute an offer, solicitation for the purchase or sale of any financial instruments, inducement, promise, guarantee, warranty, or as an official confirmation of any transactions or contract of any kind.

Research data and reports published/emailed/Telegrammed/etc. and or those made available/uploaded on social networking sites (e.g. Facebook, Twitter, LinkedIn, etc.) or disseminated in other print or electronic media by ITF, or entities with which it partners and any subsidiaries or partners thereof ("Affiliates"), or those opinions concerning cryptocurrencies expressed as and during the course of a public appearance, are for informational purposes only. Reports are provided for assistance and are not intended to, and must not, be used as the sole basis for an investment decision. The User assumes the entire risk of any use made of this information.

Reports may include projections, forecasts and other predictive statements which represent ITFs or its Affiliates' assumptions and expectations in the light of currently available information. These projections and forecasts are based on industry trends, circumstances and factors which involve risks, variables and uncertainties. The actual performance of a company, project, token or currency represented in a Report may vary from those projected. The projections and forecasts described in any Report should be evaluated keeping in mind the fact that they:

- are based on estimates and assumptions;
- are subject to significant uncertainties and contingencies;
- will vary from actual results and such variations may increase over a period of time;
- are not scientifically proven to guarantee certain intended results;
- are not published as a warranty and do not carry any evidentiary value; and
- are not to be relied on in contractual, legal or tax advice

Prospective investors/traders and others are cautioned that any forward-looking statements are not predictions and may be subject to change without notice. Reports based on technical analysis ("TA") are focused on studying charts and movements of a given currency or token's price movement and/or trading volume. As such, a Report based on TA may not match with a Report on fundamental analysis. Though Reports are reviewed for any untrue statements of material facts or any false or misleading information, ITF does not represent that ANY REPORT is accurate or complete and again emphasizes that NO REPORT should be relied on in connection with a purchase, investment, commitment, or contract by anyone whatsoever. ITF does not guarantee the accuracy, adequacy, completeness or availability of any information in any Report and therefore CANNOT be held responsible for any errors or omissions or for the results obtained from the use of such information. ITF, its Affiliates and the officers, directors, and employees of either, including analysts/authors shall not be in any way responsible for any direct, indirect, special or consequential damages that may befall any person from any information contained in any Report nor do they guarantee or assume liability for any omission of information from therein. Information contained in any Report cannot be the basis for any claim, demand or cause of action. These data, Reports, and information do not constitute scientific publications and do not carry any evidentiary value whatsoever.

Disclaimers Continued

ITF's Reports are proprietary and are not for public distribution. Reproduction or dissemination, directly or indirectly, of research data and/or ITF Reports, in any form, is prohibited except with the written permission of ITF. Persons into whose possession the Reports may come are required to observe these restrictions. Opinions expressed therein are current as of the date appearing on the report only. Data may be subject to update and correction without notice. While ITF endeavors to update (on a reasonable basis) the information discussed in the Reports, there may be regulatory, compliance, or other reasons that prevent ITF from doing so.
The Reports do not take into account the particular investment objectives, financial situations, risk profile or needs of any person, natural or otherwise. The User assumes the entire risk of any use made of this information. Each recipient of a Report should make such investigation as deemed necessary to arrive at an independent evaluation of an acquisition of the asset referred to in any Report (including the merits and risks involved).

Cryptocurrencies involve substantial risks and are not suitable for all investors/traders. Investors can lose their entire investment relatively easily in the cryptocurrency markets. Before acting on any advice or recommendation in this material, Users should consider whether it is suitable for their particular circumstances and, if necessary, seek professional advice. The price and value of investments referred to in research reports and the income from them may fluctuate.

Certain information set forth in this Report contains "forward-looking information", including "future oriented financial information" and "financial outlook", under potentially applicable securities laws (collectively referred to herein as "Forward-Looking Statements"). Except for statements of historical fact, information contained herein constitutes Forward-Looking Statements and includes, but is not limited to, the (i) projected financial performance of a company, project, token, or currency; (ii) completion of, and the use of proceeds from, the sale of tokens being offered to the public; (iii) the expected development of a company, project, token, or currency's business, projects and joint ventures; (iv) execution of the company's or the project, token, or currency's developers' vision and growth strategy; (v) sources and availability of funding for the company, project, token, or currency; (vi) completion of any projects that are currently underway, in development or otherwise under consideration; (vi) renewal of any material agreements; and (vii) future liquidity, working capital, and capital requirements. Forward-Looking Statements are provided to allow potential investors the opportunity to understand ITF's beliefs and opinions in respect to the future of a given company, project, token, or currency so that they may use such beliefs and opinions as one factor in evaluating an investment.

NO statement issued on ITF's website or in any Report is a guarantee of future performance and undue reliance should not be placed on them. Such Forward-Looking Statements necessarily involve known and unknown risks and uncertainties, which may cause actual performance and financial results in future periods to differ materially from any projections of future performance or result expressed or implied by such forward-looking statements.

Although Forward-Looking Statements contained in this presentation are based upon what ITF and/or its Affiliates believe are reasonable assumptions, there can be no assurance that Forward-Looking Statements will prove to be accurate, as actual results and future events could differ materially from those anticipated in such statements. Neither ITF nor any of its Affiliates undertake any obligation to update forward-looking statements if circumstances or management's estimates or opinions should change except as required by applicable laws. The User is cautioned not to place undue reliance on forward-looking statements.

The User should consult their own advisors to determine the merits and risks of ANY investment.