Stable Coin evolution and market trends

Key observations

PwC's market analysis | October 2018

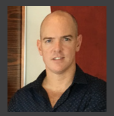
pwc

www.pwc.com.au

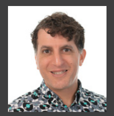
Key observations in Stable Coin Evolution

The stable coin evolution and trends discussed in this paper are the interpretation of information gathered via market research and questionnaires sent to 50+ stable coin projects. They are therefore interpretation of this data from the authors at the time this paper was drafted.

Co-Authors:



John Shipman (PwC)
john.shipman@pwc.com



George Samman
(3rd party expert)
georgesamman42@gmail.com
https://www.linkedin.com/in/georgesamman/

Executive Summary

1

Fiat-backed stablecoins need to establish traditional banking relationships in order to hold the currency that the stablecoin is backed to. There are still several inhibitors for large multinational banks to take on this role and offer this service, due to reputational, regulatory uncertainty and therefore compliance risks. Therefore, in many cases this role falls on the shoulders of regional banks, trust companies or boutique financial institutions. With some of these fiat-backed stablecoins being backed to hundreds of millions of dollars this poses substantial solvency and credit risks. Uptake of stable coin use is therefore in part reliant on traditional banking services.

2

As part of our research, many of the survey respondents' stable coin projects are 1:1 backed to digital assets (100% reserves) as well as real life assets like USD or gold. As the markets take confidence in the liquidity and safety of these new stable digital currency markets, the ability to move to fractional reserves will likely become a reality. (Fractional reserves - where only a % of the digital or physical asset backs the token)

3

An associated set of ancillary services will also need to evolve around the validation, certification and reconciliation of these reserves to digital assets. Accountancies will need to evolve to offer digital asset to physical asset audit services for stablecoins (whether this is a currency, virtual or a physical asset such as gold or iron ore or wheat).

4

A whole new industry is beginning to form around stablecoins-ancillary plays like Corion X and Standard.one also known as Cement Dao (Cement DAO creates a decentralized ecosystem of stablecoin rating agents). The community of BUILD token holders vote to whitelist the "best" stablecoins, allowing them to be added to a diversified basket.

5

Presently there are at least 75 projects that could be considered "stable coin" projects. With the deluge of projects and the amount of capital they have raised, the cryptocurrency space could enter into its own form of quantitative easing. This may be driven by fiat or asset backed funds entering the ecosystem that could find it's way into investing into many of the cryptocurrency projects trading on exchanges.

6

Exchanges are hedging themselves against the risk of only having one asset backed stable coin and adding new fiat-backed (USD mainly) stablecoins onto their exchanges at great pace. Projects to note in this regard are Okex and Huobi who appear to have added a number of stablecoins recently to hedge in this manner.

7

Gemini USD and Paxos Stablecoins, could be seen as the most regulated of all the fiat-backed/asset backed tokens. They are subject to the terms contained In the source code which include the right of forfeiture or seizure and other reasons unrelated to the holding of the stablecoins.

8

One of the key focus areas for some stablecoins achieving their stated stability goals will be to create baskets of uncorrelated assets.

9

Stablecoins should not be equated with the asset they are backed by in terms of safety and stability. The legitimacy and long term viability of some stablecoins will be at the whim of investor expectations. Understanding what these coins truly represent and their functionalities is a must for anyone who is looking to deploy capital into this market.

10

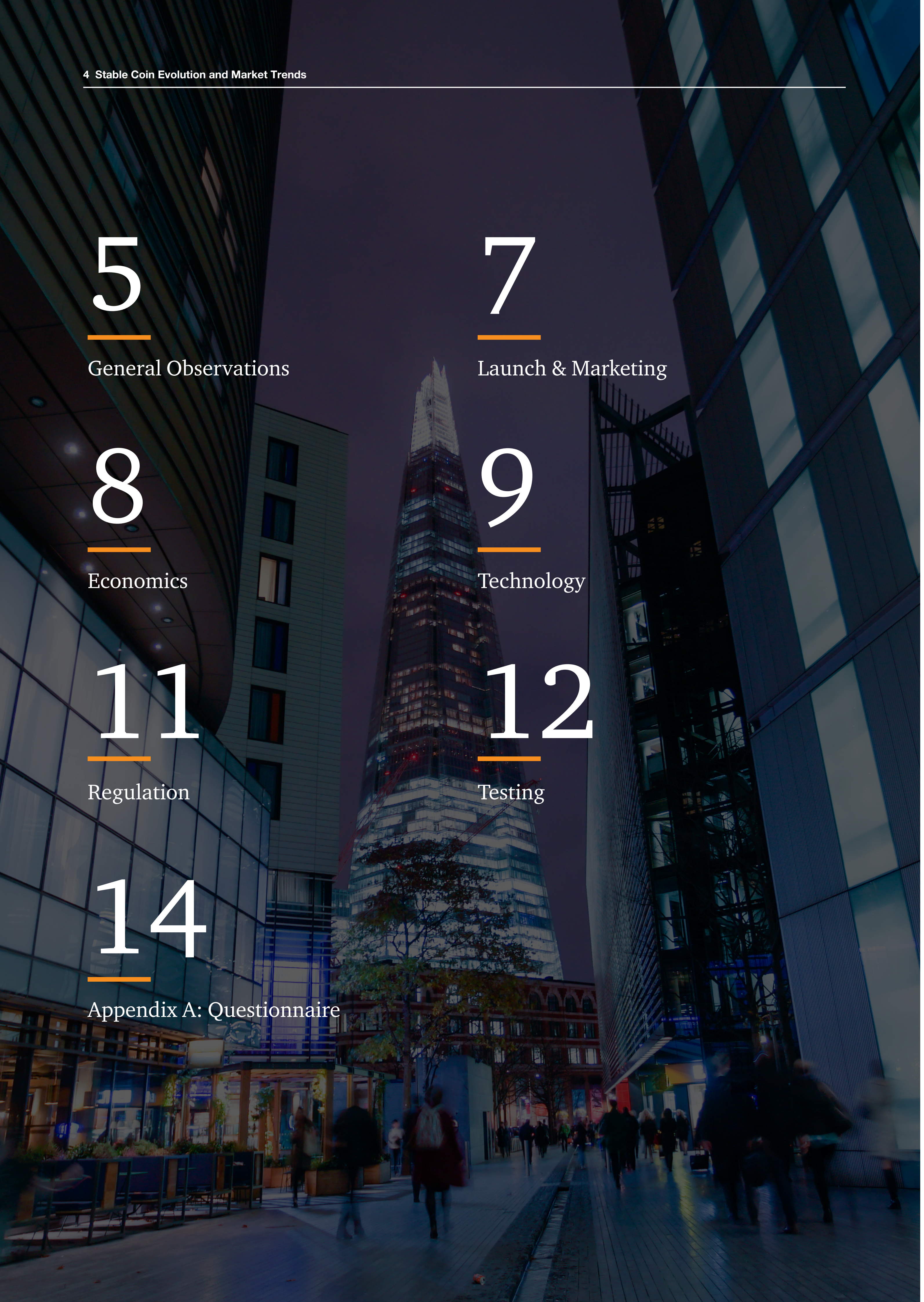
Fiat-backed stablecoins can never be100% censorship resistant, permission-less and trust-less. However they do have substantial benefits versus fiat currencies due to their ability to be programmable (both for money and compliance) and easily transferable.

11

Many of the projects are not simply looking to see their stable coins utilized for trading in the cryptocurrency ecosystem but to compete with fiat currencies on a global scale.

12

We anticipate that the key innovations will come from crypto-backed and algorithmic backed/seigniorage based stablecoins.



1. General Observations

Price volatility is one of the most significant obstacles in the adoption of cryptocurrencies for a number of reasons. Firstly, it keeps the currency attractive mainly for traders and speculators, not ordinary day-to-day users interested in using it as a medium of exchange. Price fluctuations also cause enormous currency risk, as cryptocurrencies can depreciate or appreciate dramatically relative to fiat currencies, generating a loss for users who are holding cryptocurrencies. The loss can either be direct or indirect.

a. Direct in that the cryptocurrencies depreciate heavily against fiat.

b. Indirect when cryptocurrencies appreciate, in that a merchant's products are too expensive, making them uncompetitive. Or, employee salaries and supply chain costs increase, reducing their margins.

Thus, there needs to be stability within a range of currency values for both upside and downside protection. This in turn will support in protecting incomes, savings, business margins and to allow for more reasonable business planning and forecasting when transacting or saving in this medium. Something akin to a buy wall[1] of a generic currency peg, which prevents the price of the currency from dropping and a sell wall[2], which prevents a large upward spike, is necessary to maintain a stable value of a cryptocurrency such that is comparable to fiat price stability.

Only then will can it be considered a legitimate medium of exchange and store of value by day-to-day users, merchants and savers. It is also difficult for merchants or even simple peer-to-peer transactors to conduct business if there is no consistent measure of value for the cryptocurrency they would like to use. Volatility is therefore a significant contributor to keeping cryptocurrencies as a niche digital asset favoured by speculators. As opposed to its targeted direction as a revolutionary technology that allows a decentralised and secure flow of money.

Most Stable Coin projects we have observed are currently built on top of the public Ethereum network. Most appear willing to change if issues around scalability and sharding aren't fixed relatively soon. Some are building on other blockchains (EOS[3], Hashgraph[4], Dash[5], trialled Ripple[6] and Stellar[7] NXT[8], etc) and others have started by building their own blockchains (Bitbay and Algorand and Kowala and Topl).

The majority of the respondents are fiat backed in a 1:1 capacity followed by cryptocurrencies such as Ether or commodities such as gold. Others are backed by a basket of different currencies (fiat and/or crypto) where they are using different metrics and standards to decide the weightings. Others such as Boreal, are backed from revenues on a decentralised exchange IDEX.

[1] A buy wall happens when the amount/size of buy orders for a particular coin are much higher than the number of sell orders. Traders want to buy more than they want to sell.

[2] A sell wall is the opposite of a buy wall where there are many more sell orders than buy orders. This is price negative.

[3] Havven & SendGold.

[4] Carbon.

[5] Xank.

[6] SendGolD.

[7] Stronghold, The White Company.

[8] RYOcoin.

Stablecoins are in the early development phase at this point in time and the design paradigms are still forming for what may be the future of money.

Most of these coins are stable and being tokenized versus the USD.[9] Based on the responses the USD should be the most tokenized liquid asset in the cryptocurrency space over the next 12-24 months. The other categories are 1) other fiat currencies, 2) a basket of currencies, 3) commodities 4) cryptocurrencies and 5) indexes like the consumer price index (CPI) or a UN FAO Food Index.[10]

Dual token models are being used in some cases. One token is a dividend paying or revenue share, or a price appreciation token that trades on listed exchanges and the other is the token that is pegged to an underlying asset. Some related examples of this are Basis, Havven, X8, Reserve, Staticoin and Sweetbridge.

Being stable[11] has different meanings for different people and projects. This includes their commonalities and differences in what is meant to ensure stability. For a currency, in general stability is seen as its purchasing power (which can be measured relative to an underlying asset or a basket of goods, say) and is desirable so that it can function as a unit of account. The following show the range of responses we understood from the research:

a. Stable means that the coin can buy roughly the same amount of goods and services from one day to the next.[12]

b. A stablecoin should be easily redeemable for the corresponding amount of assets it is pegged to.[13]

c. Stable means easily predictable with respect to price outputs.[14]

d. Stable = grows at the rate of local inflation – it keeps value in real terms.[15]

e. Relative stability versus volatility of other currencies. Stability must be relative to something else.[16]

Revenue models[17] used by respondents (in no particular order):

a. Not for profit.

b. Revenue/dividends or investing part of the asset in a low risk products like goverment bonds or money market funds.

c. Network transaction fees which include workflow execution fees.

d. Withdrawal fees.

e. Vaulting fees in the case of Hellogold for the physical gold (this will probably become more common for other types of commodities as well).

f. Coin creation fees.

g. Loan interest.

The purpose of the stablecoin projects (as told by the teams) is to provide the next stage in digital money technology – and in some sense have opposing views:

a. To create a stable, decentralised cryptocurrency—permission-less digital money—that can be secured, saved, and sent instantaneously at almost no cost and with no specific intermediaries.

b. To be compliant and transparent (particularly fiat/asset backed stablecoins).

c. To build trust that the stablecoin can hold its value and in the team behind it.

d. To replace Tether as dollar backed models.

e. To create financial access for those who are currently restricted.

f. To become a medium of exchange and a reserve currency or a store of value.

[9] Specifically, USD denominated deposits in commercial bank accounts.

[10] Pier.

[11] In one case, Augmint is using a DAO for stability.

[12] From Kowala questionnaire.

[13] From Carbon questionnaire.

[14] From Stableunit questionnaire

[15] From Hellogold and Stably.

[16] From Saga and Reserve.

[17] Four of the projects label themselves as not for profit.

2. Launch & Marketing

Bootstrapping[18] is vital as all of these projects require liquidity in the coin. This can be done through incentivizing miners as in the case of Kowala. The ability to convert between deposits in banks accounts and stablecoins are important as is being able to trade on exchanges. Financial transparency is essential in order to prove out the reserve, view transactions and other information via smart contracts or be able to check on gold holdings or other types of assets. Redeemability at any time and any price is also necessary.

Stablecoins rely on attracting users and getting lots of users in order to have long term viability. This is particularly true in the seigniorage model where platform growth is necessary to service the bonds. If growth in the amount of users falls, the prices will fall and more bonds will need to be purchased making it more difficult to pay the interest on the bond itself.

The following methods are being used to increase viability:

a. Dual token models are being used so one can have capital appreciation of one of the tokens while the other token is pegged to an underlying asset in the project.

b. The models that are using baskets are trying to diversify currency risk by being stable versus a basket of different currencies and/or assets instead of just one.

Confidence in the stability of the token will come through:

- Transparency in the code
- Stable banking relationships
- The ability for the technology to work openly and publicly,
- The ability for pegs to hold in times of stress, provable audits,
- Provable reserves
- Accurate asset pricing models.

[18] Bootstrapping is the process of starting with very little at minimal costs with the intended goal of building out a network to a large size.

[19] Formal verification is the act of proving or disproving the correctness of smart contracts with respect to a certain formal specification or property. of autonomous agents (both individual or collective entities such as organisations or groups) with a view to assessing their effects on the system as a whole.

3. Economics

The performance of a stablecoin during worst-case-scenario market circumstances is one of the most important components of a stable coin system.

Black swan events must be prepared for by managing the peg and providing stability during times of extreme stress. Being decentralised and having provable reserves mitigate many risks but with all scenarios it is the unforeseeable that is hardest to prepare for.

The capital for maintaining the exchange rate for the respondents to the questionnaire mainly comes from:

a. Market makers

b. Holders of the (unstable) coin: in the case of crypto the users over collateralised the system

c. Currency auctions

d. Regulated financial institutions

e. Banks

Having an eventuality plan in case of a “black swan” event is critical. ‘Death spirals’ and positive feedback loops can lead to a crisis in confidence in the stablecoin that would be irrecoverable.

Even an event with a 1% annual probability of occurrence can occur without knowing the cause until after the fact.

Most have proprietary stabilisation mechanisms in place or use 1:1 backing so even if the price went to .01 it would still be redeemable according to the projects. Emergency shut-down procedures can be used in some cases as well. Risk diversification is also a tool being deployed particularly by the companies using baskets.

Any pricing model must be robust enough to withstand a black swan event where all token holders sell at the same time. The reserve must have enough money in it pay back all holders in this unlikely scenario.

4. Technology

Since most projects are built on Ethereum and use Solidity, formal verification is not an option. If these projects move to other protocols in the future they will be able to use formal verification if the smart contracting language allows for it.

All the stablecoin projects in the survey are using smart contracts with most fully automated and some semi-automated.

Formal Verification of smart contracts appear to be an under-explored area due to limitations of Solidity code. If these limitations are overcome it will become a necessary inclusion, particularly around verifying components needed for stability.

Trade-offs: Balancing stability with the benefits of decentralisation of cryptocurrency is one of the biggest dilemmas inherent in the structure of stablecoins.

The trade-off occurs because pegging a cryptocurrency to fiat currency involves holding reserves of fiat in a central bank or vault or a commercial bank.

Thus, there is no longer a trust minimised system because users must trust that the coin issuer has adequate fiat in the bank to back the value of the coin. Also, cryptocurrencies backed by fiat or other cryptocurrencies still have price information that is not linked to the underlying cryptocurrency. For example, priced in USD/Euro showing Godelian incompleteness. In both cases, the cryptocurrency is reliant on a central entity to ensure its value.

This is either a bank or information source, which re-introduces centralisation into the equation. The first system, built on centralised banking trust, loses the original vision of using cryptocurrencies as a free transfer of value without being subject to control and limitations bound to government-approved identity and affiliation. In order to create stability the fiat collateralised tokens have to some extent compromised on decentralisation.

Oracles are an additional trade-off. Many projects require off-chain information to be brought on-chain. Until a fully decentralised oracle solution is built these projects will have to use a centralised oracle in its place.

Transaction throughput is limited by the protocol and since most are building on Ethereum that limits TPS (transactions per second) to ~15 per second. Most are hopeful for scaling solutions from Ethereum or looking to build on multiple protocols or their creating their own in case this is not solved. For those building on other blockchains (eth fork, EOS, Stellar, and Hashgraph) thousands of TPS are being claimed.

Use of oracles: There are several projects using oracles for management of external prices and other information. Approximately 60% are using oracles. Oracles are a centralised component for any stablecoin project today but most will look and transition to decentralised options as they become available.

Stablecoin designs must balance between three features: stability, decentralisation, and scalability.

Stability is how stable an asset is with respect to a defined base and has two components: the average volatility of the asset, and the worst-case volatility of the asset (how resistant the stablecoin is to significant market downturns).

Decentralisation is a measure of the degree of trust in an entity to ensure the stability of the stablecoin.

Scalability is the number of transactions per second but could have a secondary definition which refers to the amount of tokens that can be minted.

There is an evolution of thinking and technology around the use of full, pseudo or zero anonymity for those people or organisations using tokens. Some central banks have considered tokens that replicate ‘cash in your pocket’ – that is, complete anonymity. Whilst public adoption would be significant, this is at odds with stopping cross-border use of these pegged tokens to avoid money laundering issues. True decentralists like Bitbay and Orcs only subscribe to this direction in our initial analysis and interpretation.

Demand based models mint and burn tokens based on demand. Tokens only get created when there is demand. Once supply goes down (ie a token is redeemed), the token is burned.

Most stablecoins are built on Ethereum so transactions are public. However Bitbay keeps transactions private except between counterparties and Jabril anonymizes identity.

Many of the projects have centralised governance, with an entity issuing the coins and dealing with other centralised entities such as managing the banking relationships. The compliance element and vault selection also tend to be centralised.

5. Regulation

Stablecoins are of course subject to regulation. For example, AML/KYC is being implemented by many of these companies which increases the barriers to entry for those who want to hold and use stablecoins. AML-KYC is being embraced as a key lynchpin to trust for many of the stablecoin projects particularly fiat/asset backed projects.

Regulation is still in the early days and most companies are willing to embrace regulation with the view that they are getting/will get a better response from regulators (fro stable coins) in comparison to other types of cryptocurrencies.

Many projects also believe clearer global coordination and guidance from regulatory bodies is severely lacking and needs to be addressed. This response should also be harmonized rather than fragmented within jurisdictions.

Currently, there is no financial reporting framework that allows for audit conformity of a stablecoin. This means that in today’s world performing an “audit” isn’t strictly possible. One must instead rely on a 3rd party to attest to whether the 1:1 peg is accurate.

6. Testing

The testing and modelling is mainly being done by non-collateralised seigniorage coins, algorithmic-based and those that are trying to use baskets for stability.

Agent based modelling[20] and Monte Carlo simulations[21] are for those projects that are testing their models.

[20] An agent-based model (ABM) is a class of computational models for simulating the actions and interactions of autonomous agents (both individual or collective entities such as organisations or groups) with a view to assessing their effects on the system as a whole.

[21] Monte Carlo simulations are used to model the probability of different outcomes in a process that cannot easily be predicted due to the intervention of random variables. It is a technique used to understand the impact of risk and uncertainty in prediction and forecasting models.

Appendix

Appendix A: Questionnaire

Note: you can decline to answer certain questions (like marketing go to market) which may be trade secrets and we will put in "declined to answer due to current trade secret".

a. General

i. Which blockchain/DLT are you building on top of?

ii. How does the stablecoin work?

iii. What is the purpose of your coin?What does it aim to achieve andwhich problems does it solve?

iv. When we say something is stable whatdo you think it means? And when itcomes to monetary policy specifically?

v. What is your revenue model?

b. Launch and marketing

i. What does the market need to beconfident in the stability of your token?

ii. How are you bootstrapping to that level of confidence?

iii. What are your go-to-market strategies?

c. Economics

i. What is your coin stable with respect to?

ii. How much volatility can this peg withstand? Is that the same for upwards and downwards pressure? How wide is the band of behaviour it can support?

iii. How easy is it to analyse the band of behaviour from which it can recover?

iv. How expensive is it to maintain the peg/stability mechanism?

v. How transparently can traders observe the true market conditions?

vi. Which monetary theory (theoretical) assumptions do you think are not true and how does your protocol account for that?

vii. Does your stablecoin supply scale in response to demand? If so, how?

viii. Who provides the capital to maintain exchange rate peg? How are they compensated? Why do you think they would continue to lock up capital, given other investment opportunities?

ix. An eventuality plan in case of a "black swan" event. The 1% case will happen eventually.

d. Tech

i. Are any novel consensus mechanisms used, over and above the underlying blockchain?

ii. What transaction throughput can the blockchain currently handle and how does it plan to scale? Do its plans coincide with your plans for your estimated demand?

iii. What trade-offs does your protocol make and why did you make those tradeoffs? (supply/demand, temporarily peg breaking) (censorship resistance) (privacy trade-offs) (accuracy of present market data and ease of manipulation of the data feed protocol uses (responsiveness of market and ease of manipulation)

iv. Are there any centralised components of your system? Would any of these be easy for governments to shut down?

v. Does your protocol require information outside the blockchain such as a feed of price data? If so, how does this oracle work? Who manages it, what are the incentives for managing it, and what happens if the data they provide has a glitch?

vi. Which participants can see which transactions? What is the data and meta-data available, and to whom? How does this impact privacy?

vii. Are you doing anything with formal verification? Smart contracts used?

viii. What is the rebase period? (Length of time between currency adjustments.)

ix. Can we make this automated?

x. Do we use a smart contract, or network rules of the blockchain operators?

e. Regulation

i. What are your perceptions of local and global regulation in supporting stable coin, asset backed token economies?

ii. What could be done to improve regulation in terms of speed, quality, value for your company?

f. Testing

i. What kind of simulations have you done and what have they helped you learn? (simulating broad array of market conditions)

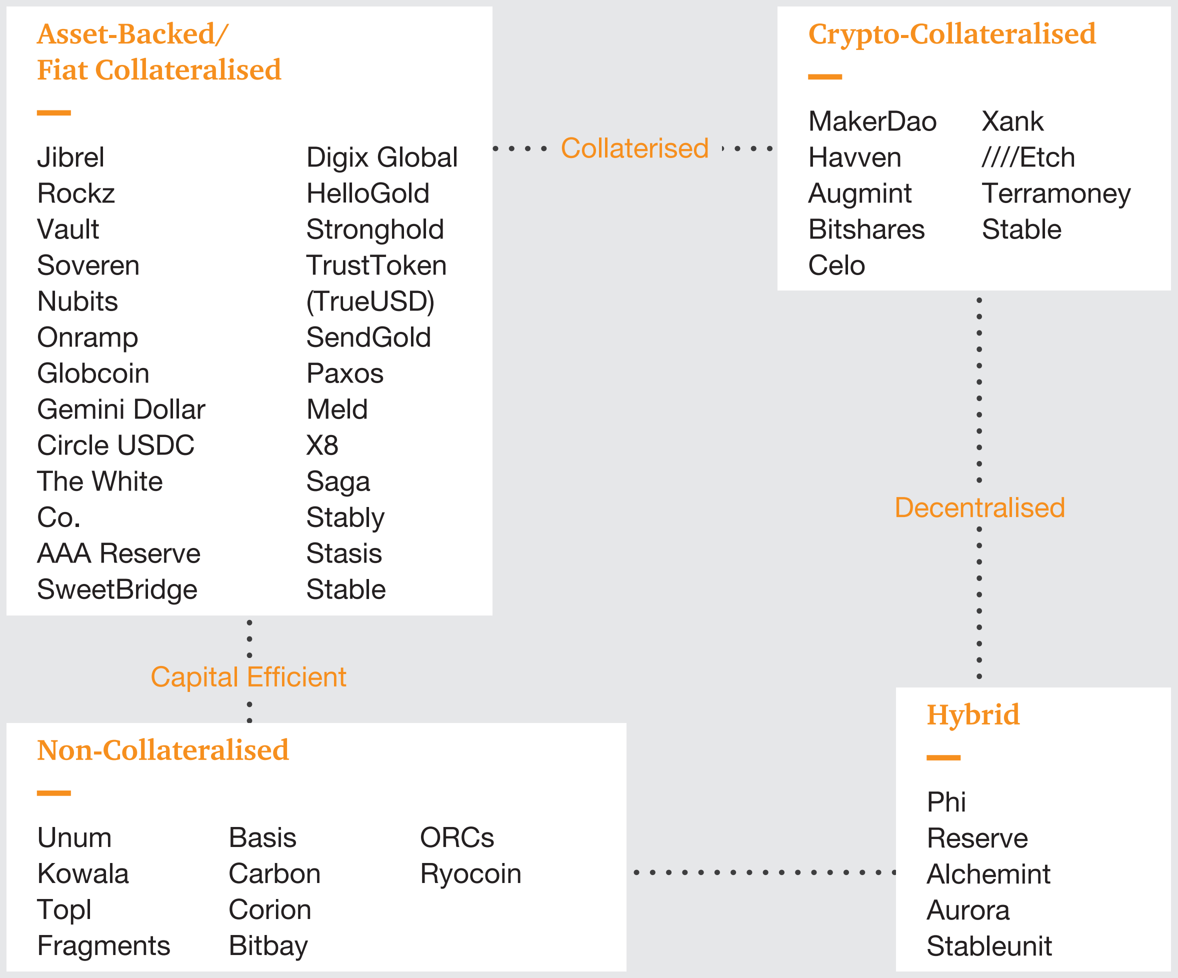
ii. Mental models for simulations

iii. Econometric models

iv. Agent-based Modelling/ Computer simulations

v. Other (Please describe)

Broad classification of responding projects as interpreted by authors



Asset-Backed/ Fiat Collateralised

Jibrel
Rockz
Vault
Soveren
Nubits
Onramp
Globcoin
Gemini Dollar
Circle USDC
The White Co.
AAA Reserve
SweetBridge
Digix Global
HelloGold
Stronghold
TrustToken (TrueUSD)
SendGold
Paxos
Meld
X8
Saga
Stably
Stasis
Stable

Crypto-Collateralised

MakerDao
Havven
Augmint
Bitshares
Celo
Xank
////Etch
Terramoney
Stable

Non-Collateralised

Unum
Kowala
Topl
Fragments
Basis
Carbon
Corion
Bitbay
ORCs
Ryocoin

Hybrid

Phi
Reserve
Alchemint
Aurora
Stableunit

Contacts

John Shipman

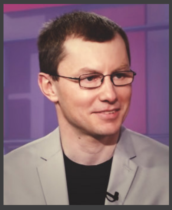
Financial markets partner

john.shipman@pwc.com

Henri Arslanian

ICO and Crypto Leader

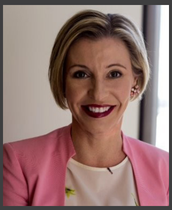
Henri.arslanian@hk.pwc.com



Steve Davies

Global Blockchain Leader (UK)

steve.t.davies@pwc.com



Grainne McNamara

US Blockchain Leader

grainne.mcnamara@pwc.com

www.pwc.com.au

© 2018 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.