Questionnaire - Bitbay

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?**

BitBay has its own blockchain which is based on POS 3 (proof of stake).

ii. **How does the stablecoin work?**

We proposed since 2014 a "dynamic/rolling/moving peg" which is probably the most simple method of controlling price of all. To freeze and unfreeze coins by force. When a user goes to send funds, the history of his coins is tracked. Coins that are marked frozen cannot leave the wallet or must come back as change to the same address. Coins that are liquid can move freely. Each "shard" of liquidity is known. So this also creates premium and subpremium liquid and reserve funds as the coins freeze and unfreeze. The choice to freeze is completely fair and forced. So unlike the weaknesses in NuBits or Basis, we do not offer trading tricks or incentives to park coins. Everyone who holds coins is effected. Users who buy liquid coins retain the properties of the coins they buy until those too are partially frozen. The users are always owners of what was frozen so those coins can unfreeze at a later date to curb dramatic price pumps. This dynamic supply can react to disasters and protect users against bear markets while still offering bullish price

potential and the same system can be used as a hard peg as well. The advantage in using it as a hard peg is if a backer does disappear the currency can dynamically deflate and adjust to new backers to take his place regardless of how little capital they hold. The beauty of the system is it is not reliant on backers or trading tricks or shorts and longs (although those things are always interesting secondary options). "Frozen" coins can be moved with a time lock as a one month delay which opens the doors for them to be treated similar to a bond (since they get higher staking interest) and also as voting power and a "future" (since if you can buy them at a discount and they unfreeze later you could turn a good profit) or even as a "liquidity swap" similar to a loan where users don't need a credit rating to get some liquidity but instead make deals where their frozen funds are returned upon repayment of the liquid funds. The decision to freeze and unfreeze is made by stakers who have a vested interest in the project giving more weight to liquidity holders. So they aren't forced on one algorithm although they will normally choose to automate it. If that turns to be volatile then we can switch to pure algorithm however we think it's nice to be able to allow users to switch metrics without forking. All of this is described on my white paper on bitbay.market. We feel that this removes the need for a market maker and can completely stop mass selling on exchanges as long as they do proper accounting (and they have to because otherwise the blockchain will decline withdraws). Of course there is also decentralized exchange which even better supports are peg since all of these rules are enforced on the chain itself.

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

The coin solves decentralization for stablecoins. So most proposals in the past relied on trading tricks like BitUSD which relied on voluntary shorts and longs which is subject to manipulation and if Bitshares loses ground so does the peg. Basis is centralized because it requires collateral. Their voluntary freeze can't solve the problem alone because it's voluntary. For the past 3 years I had always proposed a forced system of freeze. Other pegs that use baskets rely on the stability of other cryptos. So we are the ONLY true stablecoin that follows Bitcoins original dream of being completely not reliant on third parties. Also the costs are much lower because voluntary pegs require unusually high incentive. This was explained in my paper. Also Bitbays unbreakable contracts solve the problem of theft and deception in society by using deposits as a disincentive. So this solves problems so big it could in theory change history if adopted. I'm not saying it will get adopted as much as we would like but you never know. We want to inspire the space to use our ideas and further this development path. Ideas are so important especially at the early stage and we need to popularize ideas that help protect people from deception and volatility.

iv. When we say something is stable what do you think it means? And when it comes to monetary policy specifically?

When we say stable it means that a person should not fear bank runs, unjust federal seizure, price volatility, loss of value, third party risk or abandonment. A monetary policy should be developed to protect consumers. So I know that different governments want to understand this.

Blockchain gives us the advantage to streamline transactions and avoid bureaucracy. So any coins that attempt to inter-mix with traditional institutions will find themselves with contradictory terms potentially paradoxical. This is not advised. Mixing middle men with trustless systems, policy that is in contrast to blockchain rules, slow paperwork compared to fast transactions. It's possible to notarize all this paperwork and burn it to the chain and electronically sign all of it with digital signatures. This can be done even within the same transaction of deposit and withdraw! It can be done alongside the chain as well. Instead of relying on old fashioned methods! The blockchain can be used to the advantage of regulatory agencies. A stablecoin that uses collateral will find itself facing similar problems to previous economic crisis such as bank runs or delicate banking requirements. Since the blockchain is already a banking alternative this is not necessary. So again because we don't use collateral as the primary mechanism we can get stability to emulate traditional markets and hopefully gain the favor of agencies that want to protect consumers. Because after all, consumer protection is usually against unreliable third parties which in theory Bitcoin and BitBay eliminate.

v. **What is your revenue model?**

BitBay is mostly not for profit and we just benefit from price increases or any business conducted privately. After all, it's an open source project where we feel that we are contributing to the research and common good of the world and the technology used in cryptography.

b. Launch & marketing

i. **What does the market need to be confident in the stability of your token?**

Seeing is believing. They will know immediately when the peg is released in the next few months that there is simply no way to move coins that are frozen. So the stability is not at all based on trust. It's based on code and the code is essentially immutable. We don't need to rely on backers just control of supply. Volume needs only to be in close parity with supply.

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

By showing our actions speak louder than words. Our software has been running unbreakable contracts. The main developer was the first person in the world to make contracting years before Ethereum so he is already well known and respected. There is decentralized markets, many templates, tons of nice security features and all purely peer to peer with no servers.

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

We believe that by giving the world a decentralized stablecoin not based on backers, custodians or trading tricks that we will grab a large amount of volume from dangerous coins such as Tether which are ticking time bombs the moment a banking relationship is pulled or the collateral isn't there. We know with any volume increase for us also increases confidence seeing the system in action and working.

c. Economics

i. **What is your coin stable with respect to?**

Users choose the algorithm and this is far better than tracking a specific basket as we can change it on the fly if we need to improve it. Nonetheless, we start by tracking 1/100,000th the peak price of Bitcoin (which puts us at 20 cents) and then we allow the creation of new peaks if the price triples by letting the price go up a very small margin (much less than the volatile peak). Then we allow a range for the price to move within that for example plus or minus 10%. This encourages a little bit of volume as it attracts both users who want stability and users who are making an investment.

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

This peg can crush ANY volatility. That is because it allows itself to drop supply thousands of times compound. The supply can be easily dropped from a billion coins to a million coins absorbing any chance of flash crash. Then the new supply can gradually adjust as the bear market subsides. The upwards pressure is admittedly a little harder to control however because we can unfreeze coins we can always unlock frozen coins to drop the price if bulls get too aggressive. Even if the supply maxes out at 100% the new peaks it sets can be considered new floors as the market grows into its own. Then if the price starts to drop we freeze until an equilibrium can be reached. If we feel that this still isn't enough we will increase interest rates for staking. Currently it's 1% a year for reserve coins and 2% for people who voluntarily freeze liquid coins which we feel is a conservative and nice bonus to long term holders.

iii. **How easy is it to analyze the band of behavior from which it can recover?**

We feel that this system is extremely transparent. There is no need to be a professional economist or trader to understand it. It should be easy to predict what is going to happen based on the algorithms our users decide to use. However, we also can see this being a competitive voting process which is a good thing in the long run.

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

Unlike collateralized coins which require an unrealistic amount of backing which is of course totally unsustainable (remember our history and all the bank runs on gold backed currency), we think this system is so cheap to maintain that a single person if they controlled the vote could drop the currency to their own comfort level and support it with his own funds if needed. This means it's the perfect system for small cap coins, tribal communities, small communities, promotional tokens that aren't meant to be pumped or manipulated, and really just all kinds of microeconomics.

1. **How transparently can traders observe the true market conditions?**

Very transparent. In fact, you can see the vote change hours in advance which gives them a little time to predict the upcoming trend... however that doesn't mean they will be able to sell all their coins and hurt the price as the moment things start to freeze the floor will go out from under them and it would be profitless to try and sell.

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

I feel that the only true monetary theory is supply and demand. All other systems are based on that. Demand can be coerced through military threat and psychology (which we don't agree with) or simply due to the network effect (everyone else uses it so it's convenient). In the end, the dollar is paper and nothing more or less. They use various methods of capital control like hyper-inflation and taxation(which we don't agree with). However we are entering a technological boom where barbaric old methods of thinking are outdated and we can now use technology in a very innocent and pure way to control the prices of things. I think the concept of commodity backing is still strong (especially when people use the economy for real estate and dividends and company projects) but needs to be decentralized and dynamic supplies help adjust to changes when backers pull out. I'm not a believer that supply matters more than demand as both are needed. However if supply can be dropped to a single coin then there must be some demand somewhere (what is a single idea worth, what is a single art piece worth, everything has some value). The demand comes with the confidence in the technology.

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

Yes and we have explained this already as it's dynamic so it responds directly to demand.

vii. **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 opps?**

Our peg is not collateralized. Nor should it be as collateral is not a true peg. Bitcoin ideology is open source decentralization. Collateral is centralization even if spread out among many people. If the collateral is based on another blockchain (for example Ether tokens) then the collapse in price in the parent blockchain can crush the child chain. We don't share this weakness because our supply is dynamic. Users won't lock up capital, they will do what they already do naturally and that is support the buy walls on the exchange because they know if the price drops the supply will constrict and they will recover any lost value. This freedom of motion for backers will be much more attractive than locking up the coins in contracts.

viii. **An eventuality plan in case of a "black swan" event.[1,2] The 1% case will happen eventually.**

We don't suffer as many of those because we aren't tied to a volatile asset. The only major threat (the 1% possibility) is someone buying up all the voting power and then abusing the power to break the peg. Still they won't do this if it's profitless unless they want to sacrifice themselves to harm the project (and perhaps some banks will want to try that). If something like that happens, we fork and change parameters to help empower the liquidity holders even more. Although even currently the voting power is much stronger to those who hold liquid coins than those who hold frozen coins. Another way to see it is this... not any

problem can be predicted but most problems can be fixed. Blockchains have the ability to update code if needed.

d. Tech

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

Proof of stake is environmentally safe. We increase the cost for outputs to prevent spam attacks. We also know how to improve randomness in block selection and POS 3 was shown to be very resistant long term as POW coins are constantly attacked and forked historically where POS coins have been shown to be extremely resistant to forks despite hypothetical staking attacks. To scale there is always pruning techniques, dynamic block size and sharing stake rewards as a very simple system that is not over-engineered.

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?

We can handle as much as Bitcoin can. However like mentioned before there is pruning the chain as nodes get more reputable and a certain amount of time passes we prune things to be account driven (and there may indeed by archival nodes). This is already a requirement for the peg database because it tracks thousands of tiny liquidity shards per account and output. On top of pruning there is sharing stake rewards so the burden of processing bottleneck is reduced without needing servers(although powerful stakers might use them). As stakers get rewarded they will want more transactions and more users. So it's natural to allow them to include other stakers in their block to get paid with them (which we can even add some randomness to who they can select if needed). Also this means making the block size dynamic to support this ability to scale. We currently are nowhere near the demand to add those features but they are there when we need it.

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

We don't sacrifice decentralization in anything. Not in our "unbreakable" two party contracts, not for our markets and not for our peg. Control of supply is natural and something I had wanted for Bitcoin since it started. It's no surprise to me to see that others are starting to use the idea I've been preaching for almost four years (despite getting almost no media attention). We don't sacrifice privacy but we don't really focus on it either. We might use the Bitmessage network for anonymous broadcast and could toy with the idea of sidechains and privacy in the future but it's our feeling that blockchains are already very private. We don't worry about data feeds because it's not hard coded. Users check the feeds they think are reliable. If for example coinmarketcap because unreliable we would look elsewhere for prices. The internet is very robust to manipulation of feeds and even short term manipulation of feeds has very little effect on our long term stability.

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

No, that is the point. If we used collateral we could run into banking nightmares, kyc/aml, even sabotage. Users simply experience dynamic supply. This system is made to defend against adversity and not open the door to it.

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?

No it does not. Users set their own algorithms or simply cast a vote manually based on their feelings of market sentiment. We do however use coinmarketcap. There is no need to report the data to the chain as blockchains aren't really always needed for that. The users will just cast the vote based on what the

software sees and if we noticed something is wrong with the votes we just go ahead and use another source or more sources. This can all be fixed by a quick commit to github without forking.

---

[1] https://en.wikipedia.org/wiki/Black_swan_theory

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

Users contracts in BitBay are peer to peer so nobody in the world has access to that data but the two parties. The peg is enforced on chain and is very transparent. All metadata is stored in a different database that scans the transactions to assume what liquidity is for each set of coins. This can be easily queried to know if a set of coins is good. There is also a calculator to see how premium coins are by judging the speed at which they freeze to each target and then giving a general liquidity rating. Privacy is only really connected to IP address which users can obfuscate if they feel like it (proxies, TOR, repeaters, Bitmessage relay services).

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

The software based on BitHalo is the world's first smart contracts. These "unbreakable contracts" are done by both parties putting in a deposit. If they break the deal they both lose their funds. This wonderful amazing protocol is what motivated me to learn coding and build Halo all those years ago. The contracts can be used to create a very trustworthy economy in our coin. This means trustless wires (where stealing a wire means both users losing collateral), unbreakable employment contracts (where employees must not dare lie or risk default), barter, trade, shipping, real estate without escrow(which BitBay has already been used for selling land in California between two countries without escrow) and so forth. These contracts are enforced on chain but the users agreement is private. This helps keep the size of our chain small to scale.

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

The code is pretty much complete but we need to test this part to get a feel for what is good for the temperament of crypto. Currently we see a 1% supply increase or decrease every 200 blocks (or about 3 hours). This might be accelerated so we can adjust beyond 7% per day so we might either allow faster intervals or higher interest. However since we want to avoid reorganizations retroactively invalidating transactions I think the best way is to keep the 3 hour interval and simply increase interest rate or allow a range like 1-4% when votes are counted.

ix. **Can we make this automated?**

Everything is already automated.

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

Those can be made through BitBays unbreakable Halo contracts.

e. Regulation

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

In the same way guns were supposed to be a citizens protection from their government (despite the military intelligence preaching the hypocritical opposite), technology is a defensive tool against imperialism. However we would think that stablecoins should be heavily favored by governments because they aren't going to cause serious losses for consumers unlike scam projects or penny stock style crypto assets. Wouldn't it be an advantage if people didn't risk losing their money when moving from one currency to another? If there is some regulation, how is it enforced if this differs from country to country and two countries can have paradoxical laws in contrast to one another?! We feel the responsibility should fall on the users to do proper KYC, to calculate their own risks when looking at regulation. This is exactly why our software is totally decentralized as we take note from what made Bitcoin so successful. We also encourage

policy makers to see this truth that the users are the ones who are looking for their own financial freedom and ability to trade at the speed of the internet... and they will be the ones to calculate risks. This god given right should not be denied and if regulation is made to protect them let it be to protect consumers from massive fraud and theft instead of protecting private military or state backed interests (such as protecting federal reserve or the media's typical tactics of subversion). This may seem like a charged response but I truly believe in people having their freedom to do what is good and right and natural.

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

We don't see BitBay as a company any more than Bitcoin is a company. When you want to find Bitcoins "owners" who do you contact? However the developer and the investors who push the project forward are happy to talk to regulators to help them understand what the true risks are to consumers and how to properly think about their approach to the market in a mature way. As usual, we think technology is not part of the problem, it's part of the solution and should not be impeded on. This is true for all human rights for example, solar panels should not be banned and not heavily taxed on import to protect coal and oil miners. Solutions should be embraced and their risks understood.

f. Testing

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

1. **Mental models for simulations**

We have personally discussed the ideas over the years. My background in chess allows me to visualize different threat scenarios and constantly fine tune my ideas. Believe it or not, it's all done in my head. Because I have had a few years to think about it, it was honestly natural to code it and the time spent has been worth it.

2. **Econometric models**

We do have some investors with economic backgrounds and actually one of the biggest investors has been advising me over the years and his ideas have literally helped create new little features to the peg that I now feel would have been incomplete without his input. However we both feel the need to get more economists to look at it is important.

3. **Agent-based Modelling / Computer simulations**

To simulate this peg, I need to use a mock exchange so we can test the API calls and their reliability. This is because central exchanges who we partner with will completely rely on accurate accounting and responsive database. This is the one part we have not yet completed so we could see a few months delay until we know what we are going to bring to the table for an exchange since they will have to list two asset classes (BitBay liquid and BitBay reserve).

4. **Other (Please describe)**

I test the changes to the contracting system of Halo, test transactions and carefully look at how the software measures liquidity. So far all of this has been pleasantly comfortable.