*Bitcoin.*BitMint

Reconciling Bitcoin with Central Banks

Volatility - No; Anonymity - Yes.
Optimal Balance between Privacy and Law Enforcement

Gideon Samid
BitMint, LLC * Gideon@BitMint.com

The sweeping success of the original (2008) bitcoin protocol proves that digital currency has arrived. The mounting opposition from the financial establishment indicates an overshoot. We propose to tame bitcoin into *bitcoin*.BitMint: keeping the bitcoin excitement -- fitted into real world security, stability and fraud concerns.

The basic idea is to excise the bitcoin money generation formula, and otherwise apply bitcoin essentially "as is" over digital coins which are redeemable by the mint that minted them. This will preserve the bitcoin assured anonymity. The new *bitcoin*.BitMint solution will benefit from bitcoin's double-spending prevention, and would otherwise enjoy all the benefits associated with money in a digital form.

bitcoin.BitMint will allow traders to invest in US$, gold, or any other commodity while practicing their trade in cyberspace, anonymously, securely, and non-speculatively.

This "mint-in-the-middle" protocol will allow law enforcement authorities to execute a proper court order to enforce the disclosure of a suspected fraudster, but the community of honest traders will trade with robust privacy as offered by the original bitcoin protocol.

We envision interlinked *bitcoin*.BitMint trading environments, integrated via an InterMint protocol: a framework for the evolution of a cascaded super currency – global and highly stable.

Introduction

From an innovation point of view bitcoin novelties are:

- A transactional system managed by the majority of the traders, resistant to any attempt by a minority to take over the nascent trade system.
- Money is generated (minted) as a reward for a computational accomplishment
- Double-Spending and Anonymity were together solved through total trade visibility of "masked" traders.

Critique: absolute majority rule is (i) not desirable, and (ii) delusional. It's not desirable because money inherently is unstable, and without authoritarian control it is bound one day to spiral down to zero. It is delusional because the protocol is *de facto* maintained by self appointed leaders without an orderly democratic process to hold them accountable.

Money awarded for computational accomplishment favors traders with more powerful computers, and those who gained helpful mathematical insight. *Is that what the community of traders want?*

The solution for double spending and anonymity is flawed on account of (i) its reliance on the unproven mathematics of a particular choice of a one-way function, and on account of (ii) rendering bitcoin into an effective hiding ground for criminals.

Remedy: majority rule may be modified to allow a majority-authorized minority to take executive control of bitcoin operations when things get out of hand.

Money reflecting a consensus without any foundation in real need and actual utility is inherently unstable. Its value versus real human needs may fluctuate unboundedly (except by zero), and at the very least such money will be in competition with similar but distinct 'thin air currency' claiming a finer tuned, or a more fair 'computational workload'. This is therefore the biggest issue with bitcoin -- the baselessness of money, the arbitrariness of value, the idea that money can be agreed upon by traders, and despite the psychological

pendulum sustained by human traders, somehow the consensus value of thin-air money will remain stable throughout.

The remedy is therefore to chuck the “minting thin-air money” altogether. Instead, we should use the fact that money can now be in a digital form, and mint money, which will be super-stable because it reflects the totality of societal wealth. Such money can never become disfavored, it reflects everything we collectively own.

Bitcoin essentially relies on one-way functions, and one-way functions (public key, private key non mutual deductibility assumption), are essentially vulnerable to yet unknown mathematical insight, and faster than expected computing devices. And therefore it is imprudent to let a single breakable one-way function to carry the responsibility of handling a large amount of societal wealth. The remedy here is diversification -- using several bitcoin systems in parallel, intimately networked (InterMint), where each mint may be deploying a different one-way formula.

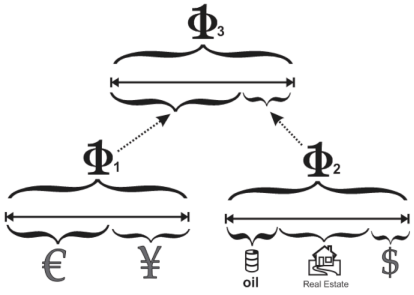
The expected event of a small group of traders, successfully concocting a means to crack the one-way function barrier will not be immediately clear. This group of thieves will likely operate in stealth, trying not to raise suspicion. Here is another case for the argument of having bitcoin run and managed by an executive committee authorized by the majority. The committee will temporarily stop trading, for instance, if it appears that the underlying one-way function was breached.

The remedy to the issue of enabling fraud and crime is to apply the privacy solution in force today over normal search and seizure. The police cannot arbitrarily violate a citizen's privacy, but if suspicions are raised, and the court approves -- a search warrant may be issued. We therefore should opt for a means to force a particular trader under suspicion to expose his or her identity.

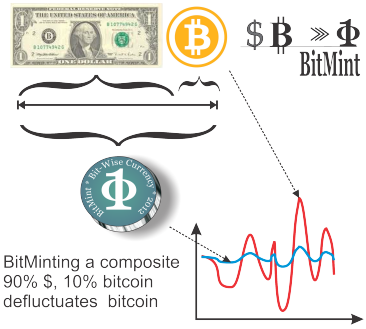
Having identified the necessary remedies to upgrade bitcoin into an effective global currency, we now come to present the *bitcoin*.BitMint solution.

The InterMint

Our proposed solution to the bitcoin faults is the InterMint -- a network of cascading digital mints. The InterMint will evolve into a super-stable global currency, while respecting national fiat currencies, empowering the community of traders, and exploiting the unique benefits of digital currency: prospectively alleviating fraud, reducing waste, minimizing abuse; taking full advantage, and at the same time leveraging the global village into durable prosperity -- that's the plan.

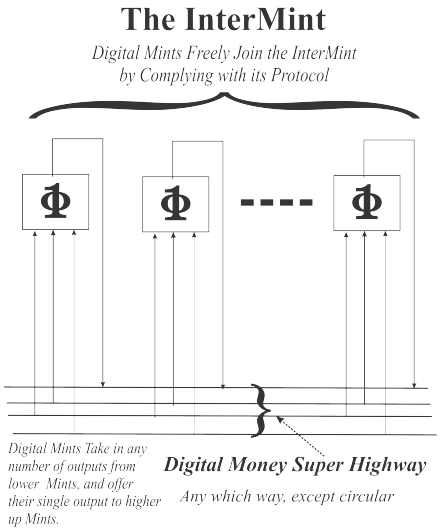


Overview of the InterMint: The network is hinged on baseline digital mints, each issuing a digital claim check against a well specified measure of a well defined commodity of wide spread human need and desirability (e.g. a fiat currency, as $US, gold, oil reserves, etc.). These baseline mints will serve as the basis for the first round of cascading mints defined as a specific mix, cocktail of digital coins issued by the base mints. A second round of mints will be defined over the first round and the base mints, and similarly for a third, and higher rounds of mints. At the top of this cascading structure there will tower a top-mint that would issue digital money backed by an ever broader foundation comprised of the total transactable wealth of society.



The InterMint protocol will govern the communication and the transactions among the various mints of the network.

Each member mint of the InterMint may be tradable via a *bitcoin*.BitMint mint component, where a variant of the bitcoin trading solution is in play.



The InterMint is further covered by: "The InterMint: A Protocol for the Future of Money" See reference.

bitcoin.BitMint

bitcoin.BitMint is a digital currency protocol based on non-speculative digital currency that is traded via a bitcoin anonymity and double-spending control protocol, mandating that the anonymous traders will register with the mint, and as condition for trading, will agree to reveal their true identity against a properly issued court order.

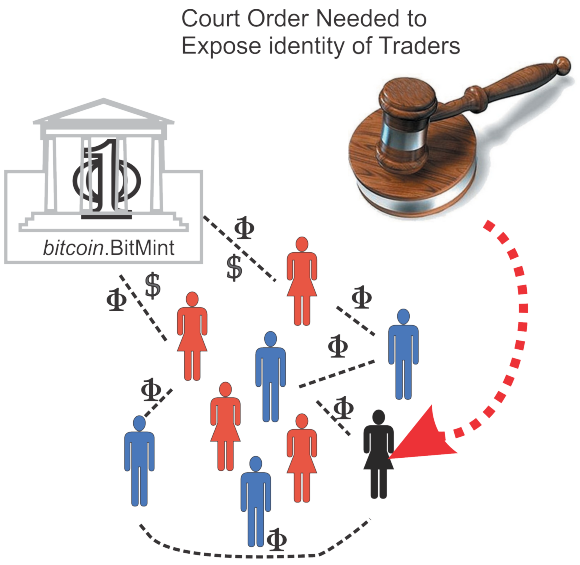
The key differences between nominal (2008) bitcoin and *bitcoin*.BitMint are:

- Trade is carried out by passing digital strings that reflect a well defined measure of a desired commodity, like fiat currencies, gold, silver, real-estate, etc. The value of the string is non-speculative, it redeems for the same amount that it was purchased for.
- Trading is specified, managed, controlled, and is under the responsibility of the digital mint that announces it, and establishes it.
- The anonymity of traders is safeguarded and respected unless a specific court order breaches it.

The key similarity between nominal (2008) bitcoin and *bitcoin*.BitMint is:

- The protocol for anonymity and prevention of double-spending is essentially the same.

Illustration: A *bitcoin*.BitMint mint issues digital strings as claim checks against $US. It offers its traders to use their credit card, or banking account to send $US to the *bitcoin*.BitMint mint, against which they receive a bit string



bitcoin privacy and double-spending prevention protocol serves the traders who joined the *bitcoin*.BitMint trading environment set up by the non-speculative digital mint.

thatis always redeemable against the same amount of $US used to purchase it. The trader also passes on a personal public key to the mint. The bit string issued by the mint to the trader is cryptographically signed by the mint (using its private key) to allow every examiner to verify its validity (via the mint's public key). The signed coin will designate the public key of the purchaser as the current owner of the coin. The owner can now 'play' in the bitcoin environment set forth by the mint. That is, he or she can pay the coin, or part thereto to another trader in the same bitcoin-like trading environment set forth by the mint. The payer will effect the transaction using his or her private key, and the recipient (the payee) public key. The transaction will be submitted for approval, and together with other transactions in the same time frame, will form a 'block' that would be examined for absence of fraud and will be signed for validation. The signature of the block will be carried out either by the mint, which runs the 'show' or by fellow traders, who are motivated by a specified fee paid by the payer and the payee in a pre specified proportion (all the specifications are the responsibility of the mint). This is similar to the published 2008 bitcoin protocol, once all the possible bitcoins have been mined. The mint will change the fee for the signer to insure proper balance between computational burden and speed of transactions. The new owner of the described coin, will be able to re-apply the bitcoin protocol to transact the coin, or part thereto to a third trader, and on it goes. Traders may own a number of pairs of public - private keys, and "fake" transactions between them. Any current owner of a *bitcoin*.BitMint coin may, at his or her discretion, hand this coin over to the *bitcoin*.BitMint mint, asking for redemption. The mint will verify the history of ownership of the coin, or part thereto, as the case may be, and if all checks out, it will redeem it to the claimant.

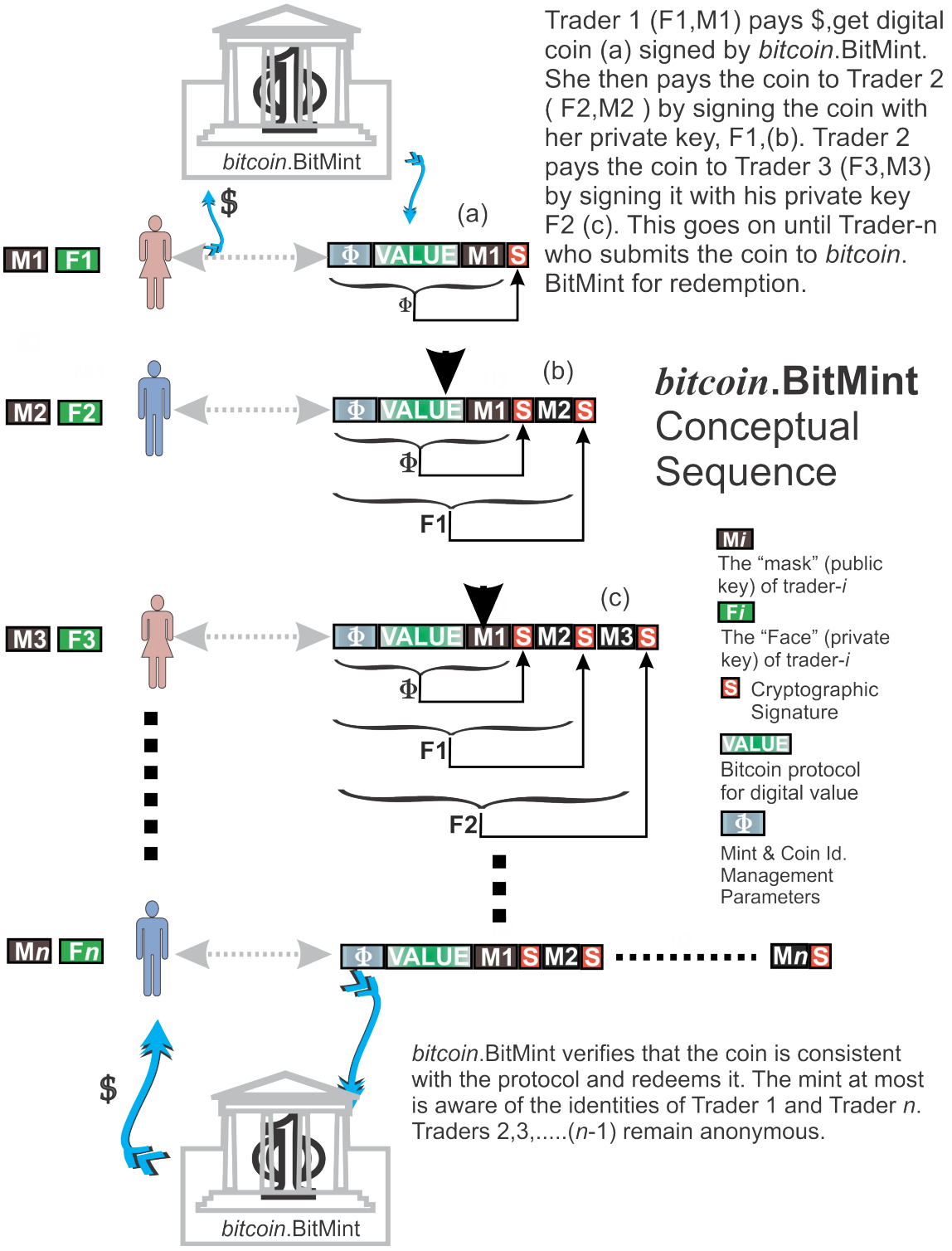
Suppose that Alice purchased a $100 coin from that mint, then paid $80 of it to Bob per his "mask" (his public key), and then Bob paid the money or part thereto to Carla, and she did the same vs. David. On and on, until Zelda decides to redeem the coin (or the part of it, she get ownership of). The *bitcoin*.BitMint mint will know, at most the identity of Alice and Zelda (the purchaser and the redeemer) of its coins, but will be clueless as to the identities of Bob, Carla, David, etc. through which the coin, or part thereto have passed.

This state of affairs is perfectly analogous to Alice withdrawing $100 in cash from her bank account, paying it all, or sum of it to Bob, who pays to Carla, who pays to David, on an on, until Zelda gets a hold some of that cash, and deposits it in her bank account. The bank may know who Alice and who Zelda are, but is clueless as to the identity of the in between.

Double spending prevention, and privacy protection are preserved, just like with the original bitcoin. However, should the authorities focus on a shady trade and spot a suspicious public key passing dirty money, then they would secure a court order and present it to the mint. The mint will contact the unknown public-key holder, and notify him or her that their money will not be redeemable upon demand, and their public key will be listed as non-compliant, and hence non-transactable, until such time that the public key owner comes forth and identifies himself or herself.

This is how the community of traders maintains its privacy, while allowing the law enforcement authorities to flash out bad apples.

Subject to the prevailing law, the *bitcoin*.BitMint protocol may allow the purchasing trader, and the redeeming trader to identify themselves only through their public key, and so even they will remain anonymous.



Trader 1 (F1,M1) pays $,get digital coin (a) signed by *bitcoin*.BitMint. She then pays the coin to Trader 2 (F2,M2) by signing the coin with her private key, F1,(b). Trader 2 pays the coin to Trader 3 (F3,M3) by signing it with his private key F2 (c). This goes on until Trader-n who submits the coin to *bitcoin*. BitMint for redemption.

bitcoin.BitMint Conceptual Sequence

Mi
The "mask" (public key) of trader-*i*

Fi
The "Face" (private key) of trader-*i*

S Cryptographic Signature

VALUE
Bitcoin protocol for digital value

Φ
Mint & Coin Id. Management Parameters

bitcoin.BitMint verifies that the coin is consistent with the protocol and redeems it. The mint at most is aware of the identities of Trader 1 and Trader *n*. Traders 2,3,.....(*n*-1) remain anonymous.

The BitMint protocol allows for coin splitting so that the *bitcoin*.BitMint traders can readily split a coin to pay any amount thereof to any other trader.

The *bitcoin*.BitMint protocol may allow a trader to pay a coin to two or more traders on the basis of "each", "all", or "some", and even "conditional" requirements, regarding paying that coin further. For instance, a high ranking supervisor will sign off on some payment, if her underlying accountant did so earlier.

Special Purpose *bitcoin*.BitMints

Digital mints may set up bitcoin trading environments subject to a variety of terms. In some, the traders will have to qualify according to some preset terms. In others, the traders will participate in financial investment and prospecting, and in yet others, the traders will enjoy a steady stream of interest income while they trade in the *bitcoin*.BitMint environment. One must note that any commodity, tethered as it may be, may become the basis of a *bitcoin*.BitMint environment.

*stock.bitcoin.*BitMint

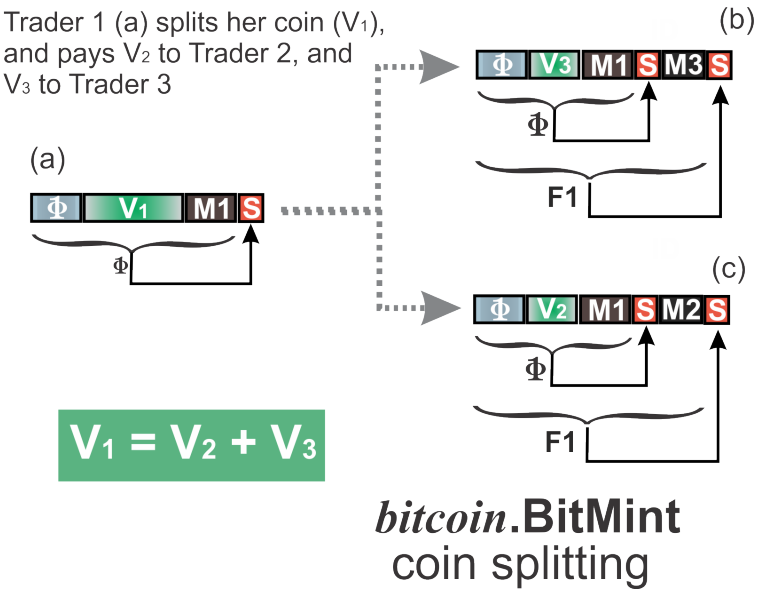
A particular BitMint may be set forth where the digital coins will be issued against a particular stock or a particular financial instrument of any kind. The mint will deposit the stock, as it does with cash, ready at any moment to redeem the same. The *bitcoin*.BitMint traders will trade the same as above. Any trader will be able to ask BitMint to redeem any bitcoin environment traded digital coin she owns, and against which she will receive the nominal amount of deposited stock. The 'betting' element here is with respect to the dollar value of the redeemed stock. If the bitcoin.BitMint traded stock will rise in value, traders might expect it to continue to appreciate, and go on trading with it. If it loses value, the traders might all rush to redeem their stock assets. The point here is that traders will be able to readily use the stock as money, and gamble on its future worth. Such bitcoin.BitMint stocks will be regarded as *stock.bitcoin*.BitMint

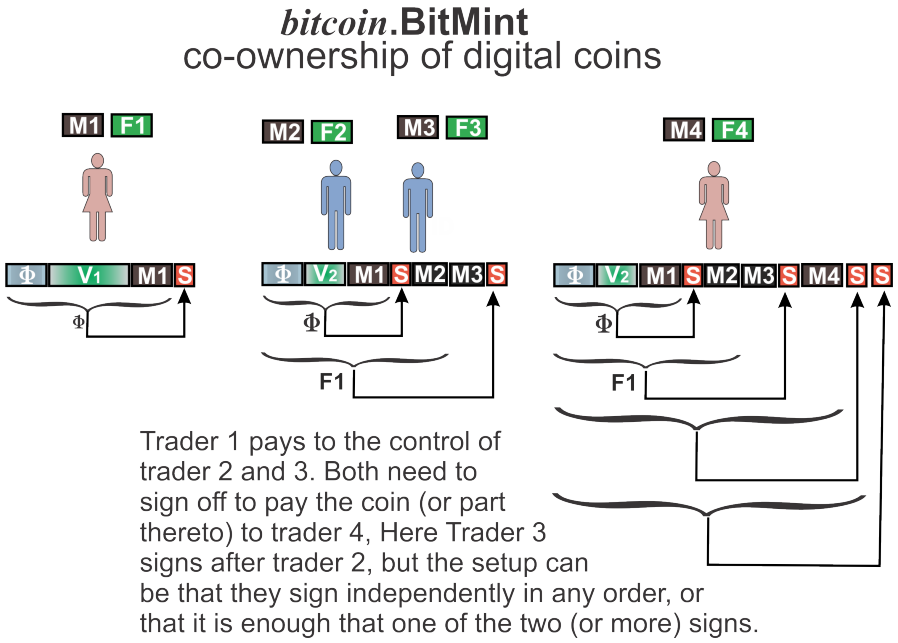
*interest.bitcoin.*BitMint

Since the deposits that traders make with the mint may be deposited in an interest bearing bank account, the mint could offer to split this interest with the traders. This will allow traders to 'play' and 'trade' with each other in that bitcoin trading environment while

their money accumulates interest, as if it were deposited and not used. This might have a durability impact on the coin, or otherwise impact the behavior of the traders.

BitMint will manage its profit by adjusting the fee it charges for purchasing a digital coin, redeeming thereof, and for the *bitcoin*.BitMint services.





Analysis

bitcoin.BitMint identifies the anonymity and double-spending prevention protocol as the 'nugget' of the bitcoin innovation, and applies it over non-speculative digital currencies, in an environment where a multitude of interconnecting mints is forming a global network -- the InterMint, and is set forth to evolve into the rise of a super-stable global currency.

The diversification of the bitcoin concept into a multitude of distinct algorithms, each compliant with the abstract solution, is a considerable remedy to the risk of compromising the single algorithm on which the original (2008) bitcoin relies.

bitcoin.BitMint is based on the notion of a managing mint that builds a bitcoin trading environment under its rules and responsibility. It solves the inherent bitcoin problem of the rigidity of the majority - a rigidity that prevents any executive minority from taking timely steps to safeguard the trading dynamics from eventual spiraling collapse. The mint is also the address for complaints, conflict resolution, and any challenges for wrong doing. On the other hand the concept of the InterMint based on an ever growing interconnecting mints, presents the trading public with a broad spectrum and choice for mints to trust. Eventually well managed, fair, supportive mints will become more popular -- not be decree, not by no choice -- but by public demand.

The managing mint will also be a convenient address for law enforcement to present a court order to expose the identity of a trader under suspicion.

The variety of commodity based, non speculative mints, will be cascaded to 'cocktail' mints, through several rounds that end up establishing one or few global currencies which rely on a broad spectrum of desirable and shared commodities -- the wealth of society. This reliance endows these super digital currencies with a durable stability. Stable global currency is the necessary framework for a smooth and effective global trade, and it serves

as the necessary condition for a bold credit market. It is credit which serves as the leverage for human prosperity.

In summary *bitcoin*.BitMint takes up the shinny nugget in bitcoin, shakes off the over reaching quest to generate money without a foundation of human utility, and corrects for its risk of relying on a single unproven algorithm, by creating the InterMint which relies on a multitude of specific implementation of the brilliant bitcoin concept of anonymity trading, and double-spending prevention.

Reference

1. "Bitcoin: A Peer-to-Peer Electronic Cash System" 2008 Satoshi Nakamoto satoshin@gmx.com www.bitcoin.org
2. "The InterMint: A Protocol for the Future of Money" Gideon Samid, March 2014. Free copy available [info@bitmint.com]
3. "Tethered Money: Digital Currency & Social Innovation" Gideon Samid, 2013, DGS Vitco, Available on Amazon
4. "Bitcoin to BitMint... Alchemy to Chemistry!" on YouTube https://www.youtube.com/watch?v=RuFTGcfh0WE&feature=youtu.be
5. Compendium: "Payment, Banking, Credit Technology and Applications Recent Columns Published in Digital Transactions" Free copy available [info@bitmint.com]
6. "The Battle of the Bits" Linda Punch, Digital Transactions June 2013
7. "Governments Must Co-Opt Bitcoin to Avert Disaster" American Banker, April 17, 2013
8. "The Bitcoin Delusion" American Banker, Nov 2013