A Guide to Examination of the LeVeL digital money solution

(and why is such a guide needed)

For decades money was what we now call 'legacy' -- computer accounts manifest as addressable memory locations where currency figures are written. Then came bitcoin and money took a completely new form. No more figures written in a specified memory location, but rather a complex binary string, controlled by another binary string known as a 'private key' -- the locations of these strings were immaterial. These strings could be duplicated and they were programmable. They became money through a technology known as blockchain, empowered by peers' approval. Blockchains today are hinged on a single algorithm known as 'elliptic curve'. There are thousands of protocols that use blockchains and peers' approval in a variety of inventive ways.

When a judge takes a look at a digital money proposal, he or she naturally ask themselves: in what ways does this protocol handle the underlying blockchain, and how does this solution bring about peers' approval: proof of work, proof of stake, otherwise? Alas, using this mental disposition to study LeVeL will result in terminal confusion, and that is why a short guide is needed.

A digital coin by BitMint was designed prior to the bitcoin explosion (first patent filed in 2007). It pioneered the notion that money in digital form has not only a numeric value, but also a unique identity and, as such, its location is not important (as with legacy money). BitMint money can be hosted anywhere - on the cloud, or on a phone. It can be duplicated, it can be split, it can be associated with terms of use, which are cryptographically attached to the money -- a new world of possibilities. The BitMint coin was issued by a central mint, that was also committed to redeem it.

When bitcoin showed up, the BitMint team identified two fundamental innovations: (i) the public ledger, (ii) the use of one-way functions. We also noticed that the dependence of peers' approval, and the reliance on a single one-way function (the elliptic curve) are weaker tenets of the bitcoin solution. So, faithful to the innovation practice developed by the BitMint team, we focused on the fundamental and dismissed the incidental. It was obvious that for a payment to go through, only the payee needs to be

persuaded that the payor is bona fide -- not the entire community of traders. It was further obvious that any single one-way function will eventually surrender to smarter math and to faster computers. We then combined the fundamental tenets from bitcoin, avoided the single-algorithm vulnerable blockchain, and the burdensome requirement of threshold peers' approval and charted a payment protocol based on a network of public ledgers where a payee easily reaches the record of the coin a payor is about to pay to him or her.

While the particular blockchain mechanism is vulnerable to a smarter mathematician and a more powerful computer, the idea of security layers was indeed attractive. We found a way to use it. The emerging LeVeL BitMint coin called for the payor to prove his credentials to the payee only, not to the community at large; after so proving, these secret credentials are known only to the payee, not to other traders. This fact can be used by that payee when they become a payor and wish to demonstrate their bona fide. And so on, each trader demonstrates to the next one that they are the rightful owner of the paid coin by showing to the payee (and not to others) that they have the credentials used previously to pass the coin between former traders. A proper owner will have all the past credentials, and when showing them to the next owner, he or she passes to the next owner the chain of credentials. It seems that a chain of credentials is similar to the chain of blockchain signatures -- but that is not the case. Every owner of the coin can pick and choose their own one-way function to generate a pair of public and private keys where the public key is posted on the public ledger and the private key is held by the coin owner. In other words, the algorithmic stagnation that undermines the security of blockchains is replaced by algorithmic mutation. Thus that the more often the LeVeL coin is traded, the more hopeless is the effort to hack it.

And yes, LeVeL adopted the public ledger, the power of one-way functions, and the abstract notion of security through layers, but it shied away from peers' review and avoided the algorithmic stagnation vulnerability. Any mental attempt to fit the LeVeL into a peer's review blockchain variety of bitcoin will, alas, result in a terminal confusion -- as forewarned above. Hopefully this guide will keep the evaluator of the LeVeL digital payment proposal on the right track, so that it can be examined without mental distortion.