

A LeVeL Paying Field Coin by BitMint



LeVeL

Quantum Safe

Why LeVeL?

This is a submission for an important competition in which the winner will be selected as the recommended solution strategy for CBDC among the G20 countries. You, the honorable judges, have a slate of fine CBDC proposals, all worthy, all thoughtful. And we, with all due humility, claim priority and advantage, mainly on the following three counts:

- (i) security and durability,
- (ii) privacy v. law-enforcement balance,
- (iii) universality and scalability.

Our most compelling argument is security. Crypto money is flourishing across the land, overtaking legacy banking by storm. To us it looks like the farmers who reap a plentiful harvest on the slopes of a dormant volcano, which is already making rambling noises. The cryptographic community is unified behind the conclusion that quantum computers will undermine the mathematical structure that supports crypto money; the debate is only how soon. Yet, crypto enthusiasts brush it off and indulge in their rosy projections for the future. To the best of our knowledge none of the published solutions properly accounts for the quantum volcano about to erupt.

You, the judges of this milestone competition, should not be swayed into dismissive attitude towards the strategic threat posed by the emergence of quantum computers. 'Quantum Safe' is a requirement that should not be diluted by the momentum of today's crypto trade. LeVeL is not the only digital money solution that claims quantum resistance, but we are the only solution that emulates the way nature behaves. Covid escapes the high-tech vaccines that humanity throws at it, by the evolutionary tactics known as biological mutation. LeVeL escapes the ominous quantum threat through algorithmic mutation, as we elaborate elsewhere.

The payment world is plagued by the unresolved dilemma of the proper balance between privacy and law enforcement. Unbreakable encryption will ensure payment privacy but will enable fraud, crime and abuse. Installing a trapdoor for governments to break strong encryption would raise public suspicion for government abuse and invasive surveillance. There seems to be no satisfactory middle point.

It is this dilemma that BitMint's LeVeL solves with an innovative twist. Level coins are viable on account of their redeemability at the mint that issued them in the first place (e.g.: central banks). A coin that participates in a transaction which raises suspicion can be singled out by law enforcement and posted on a "Hold" ledger, indicating that this particular coin is temporarily unredeemable.

Such posting will instantly render this coin unto 'non-payable' status because it is the redeemability of the coin that gives it 'life'. The owner of the posted coin is well protected behind unbreakable encryption, but they lose any benefit from its possession. It is up to that owner to approach the posting authority (law enforcement), identify themselves, and prove to the authorities that they have received this coin in a bona fide transaction. Once they clear themselves, the coin returns to 'redeemable' status and business continues.

Any coin holder who is unlawful will likely not step forward to surrender to the authorities. He or she will remain hidden behind the strong encryption offered by LeVeL, but will find his or her wrongly gained money – as money no more. No one will accept that digital coin as payment. Poetic justice!

There you have it: the encryption is robust enough to support the most discriminating privacy concerns, but the LeVeL protocol is smart enough to deny abusers, fraudsters, and criminals the fruit of their wrongdoing.

Payment applies to more than cash. Any financial instrument is payable: debit, escrow, stocks, bonds etc. The LeVeL protocol was built to apply to the full canvas of financial dynamics -- extending its robust security, and privacy adjustability to the boundaries of commerce. The LeVeL protocol is designed to offer ready programmability so that the extended LeVeL coin will carry with it the detailed description of the circumstances of its movement, and the history of its trajectory, upgrading LeVeL to a universal financial language to be used by society as an effective tool for progress, prosperity, equity, fairness and justice.

These main three tall flags (security, privacy, universality) mounted on high masts on the LeVeL financial ship give it the deserved priority of sailing over the rough ocean of global finance. –We entreat you as Judges to recognize our fifteen years of dedicated financial design, pull the anchor, and let the LeVeL ship sail forth.