The Algorithmic Mutations Advantage: LeVeL is Quantum Safe

Algorithmic stagnation is the hidden fault in the sweeping success of crypto currencies, including those with CBDC aspirations. This fault is buried so deep in the annals of cryptographic scholastics that crypto users and financial mavens are oblivious to it, and keep cultivating their preferred crypto currency much as happy farmers who farm on the fertile slopes of a dormant volcano about to erupt.

There is no excuse for a selecting committee to pick a digital currency platform to be of reliable long-term service, which has no good answer to the ticking bomb of the quantum threat. Some of those unprotected digital coins are very attractive on many counts, and some are very successful, traded by millions. Such glaring success can blind the uncareful evaluator, but should not sweep away the good judgment of the judges of this competition.

We would like to assume that this competition is narrowed down to the few who have taken the quantum threat seriously and have developed an antidote. These few are the competitors that LeVeL is positioned to compete against. And that is the case that we make forth.

Ever since the cryptographic community agreed to the reality of the quantum threat, the community announced a global post-quantum cryptography campaign. Indeed a host of quantum-resistant digital money solutions have been published. We at LeVeL examined these post-quantum proposals and found out that they deploy the same strategy: building up an extended computational complexity to be too much of a hurdle against the quantum dragon. We consider this line of thought unproductive. The reason being: the quantum threat is developed behind veils of secrecy. The public knows only what quantum developers want the public to know and not more. You cannot be sure that a computation hurdle will be good enough to forestall an attacking computer you don't know how fast it computes.

The LeVeL team opted for an innovative turn. If you lock your treasure box with a lock, that would take 10 minutes for a locksmith to crack, then you cannot expose it for more than so many minutes. And it would not do, to sweat it and build a stronger lock, which will take 15 minutes for the locksmith to crack, or 20 or 30 minutes. What you can do though, is to fit your box with another lock, say every two minutes. Then, by the time the locksmith cracks the first lock, he will face five more locks, which will take him 50 minutes to crack, but in these 50 minutes you installed 25 more locks. On it goes -- you keep mutating the locks and guarding your treasure. That is the LeVeL quantum defense strategy. Turing machines (today's computers) are so much slower than quantum computers. They cannot compete with cracking codes, but they don't have to. These Turing machines are fast enough to install new codes to be cracked at a pace that will keep the quantum machine always behind.

The LeVeL coin is fitted with another lock every time it changes hands. The more it trades, the more secure it is. Again: the innovative LeVeL solution is not based on adding more and more layers of complexity that eventually quantum computers will crack, but rather on using Turing machines to post more and more computational challenges to the much faster quantum predators, and safeguard digital commerce. The LeVeL advantage.