DigitalBank Vault SuperEncryption confronts an existential threat to the hyperconnected world.

The ‘modern’ encryption we all use was designed in the 1980s. It was never intended for use in our hyper-connected world. It has done a great job but it’s now failing us.

We see breaches caused by its flaws daily. But there is a bigger problem. Quantum computing poses an existential threat to everyone’s cyber security.

In response the world must begin a global upgrade to replace all encryption technologies. This is an upgrade unlike anything we have seen before.

Patching and mending, and taking risks with incremental improvements to public key encryption, which is no longer fit for purpose, is not the answer.

Symmetric keys and One Time Pad Cipher are secure against any attack, including quantum computing and cannot be mathematically ‘broken’, no matter what computational power will be applied.

But until now, there was no safe and efficient way to distribute them.

DigitalBank Vault SuperEncryption gives you a method to create those keys , securely, at any kind of endpoint device , in a fully air gapped environment, offline, while OTP encryption keys are generated on the spot, by the user, for a few milliseconds, and never stored or exchanged with any third parties.

Organisations with the most stringent security needs still rely on people to transport the cryptographic keys that protect their networks around the globe. Aside from the increased cost and environmental impact, manual key delivery introduces more vulnerabilities and results in poor key refresh rates. All the above mentioned security issues have been solved by the DigitalBank Vault SuperEncryption System.

The security implications of quantum computing for companies around the world are huge. Within this decade quantum computers are likely to break PKI. Core business systems and networks must move away from using PKI. We must do it once and do it right.

So-called post quantum algorithms (PQAs) are not mature enough to be relied upon and will introduce new complications, before being compromised themselves by either classical or quantum attack. No public key algorithm can ever be described as “Quantum Safe”.

Symmetric encryption keys, especially OTP and AES256 Symmetric Algorithm, are known to be secure against quantum attack. DigitalBank Vault has developed a secure way to use them both on the same encrypted files. It is called SuperEncryption, or Multiple Encryption.

Each file is encrypted multiple times, each time with different symmetric keys and different symmetric encryption algorithms. DigitalBank Vault SuperEncryption System has 4 layers of encryption, one on top of the other, two of the algorithms used are OTP and AES256 .

SuperEncryption like the DBV Tech is Unbreakable and Indecipherable, no matter how much computational power you will apply.

In Addition the DBV tech is protecting organisations against future threats from quantum computers and against current remote hacking threats by removing the need for trusted third parties. DBV is working offline, without any server's intervention, no username or registration, no platforms to access, no credentials to be stolen : an architectural concept built around the idea that users, should not inherently trust any connection to a business system, third party providers or application regardless of what trusted device or trusted network it originated from.

With the DBV SuperEncryption System, you can create an infinite number of symmetric keys with just a 'passphrase' each key generated is in the length up to one-time-pad, that is mathematically uncrackable. Keys are never " stored" or "delivered" so they cannot be intercepted or hacked. They are created trustlessly at the offline endpoints. Used once for a few milliseconds and then permanently discarded.

Our team of innovators is world class. Our physicists, mathematicians, cryptographers and engineers have collaborated to create cryptographic innovations in both the quantum and classical realms.