Bitcoin is Key

by Charlene Brown

A cryptographic key, given life, or germinated by proof of work, secured by the collective kilowatts transmitted across the network, at the specific moment in time, when that bitcoin block was mined and validated, generates a fingerprint - forever.

The seed phrase, made up of 12-24 words in a specific but nonsensical order, keeps a crypto wallet secure and private.

The pain point is trying to restore access to that wallet without recalling the recovery phrase or mnemonic phrase correctly in and in order, to protect your cryptocurrency assets from theft or loss, but can be a nemesis in and of itself.

Seed phrases are often generated randomly by the wallet software and are unique to each individual user, but not user generated. And though seemingly secure, could be the root of all chaos if misplaced, destroyed or forgotten.

If you lose or forget your seed phrase, it may be impossible to access your cryptocurrency funds. Some wallets may offer the option to create a password for your seed phrase, however that's still just a shorter version of a bigger problem.

Most software encourage people to not share their recovery phrase with anyone, but that's also kind of counter-intuitive, since if you forget it, nobody else can help you recall it. With the lake-effect like brain that sits in my cranium, I email my keys to as many email addresses as I can think of.

A private key is the only way to access bitcoin on the the blockchain. Bitcoin's private key is the fingerprint of every block validate on the blockchain.

The more distributed the key, the greater level of security surrounds each block, the stronger the network itself, and the more valuable each key and every kilowatt of energy maintaining the network.

A record of that fingerprint or birth certificate is distributed on every computer around the world running a node of the bitcoin blockchain.

Fingerprinting technology is becoming the most secure key to unlocking everyday devices, including crypto wallets, due to the uniqueness of each person's fingerprint.

With the threat of AI being used for deep fakes and the limitations of human memory, fingerprint verification is inevitable. Embedding fingerprinting onto the blockchain can provide titanium level security and protect against identity manipulation.

Using the Bitcoin network to validate identity and bitcoin blocks provides verifiable and transparent security. This advancement of more secure technologies allow for harnessing more power from this magnetic planet.

Security is strengthened when everyone can verify the legitimacy of the key associated with accessing anything of value, rather than single point query verification.

Fingerprinting is considered the most reliable method of identification because fingerprints are unique to each individual, and they do not change over time.

Digital fingerprinting detecting technology has advanced to the point where even partial or smudged prints can be used to identify a person with a high degree of accuracy.

The development of the blockchain has been the only real reliable system since the first use of fingerprinting as a form of ID recoded in 1892 by Sir Francis Galton.

Over the next decade this coupling will be the driver of a truly real verifiable unique person protocol identification and a most reliable all access pass.