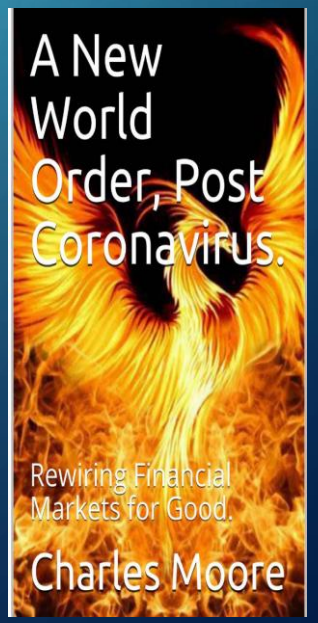
CENTRAL BANK DIGITAL CASH SECURITY

From the author of the book

"A NEW WORLD ORDER, POST CORONAVIRUS. REWIRING FINANCIAL MARKETS FOR GOOD."



THE BASICS

- Todays physical cash and old world payment systems are slow to settle
- All cash-less payments are deferred payments for up to 30 days
- These inherent technology introduced delays afford protection from drain the swamp attack vectors
- Banks self insure against “small value” attacks, rather than secure their payment networks
- Large value networks are hidden behind walled gardens, with no public access to limit the attack surface, this are also self insured as a means of risk management
- All existing payment systems are insecure and mange risk of attacks via limiting the velocity of transitions and deferring settlement
- Central Bank Digital Cash operates at a comparative speed of light (~100 ms) with guaranteed legal finality for all payments

THE SOLUTION

- Mandatory hardware security modules with minimum of FIP 140-2 level 3
- Reduced attack surface
  - No accounts exist, hence no accounts to attack
  - No sessions exist, hence no sessions to attack
  - No protocol states exist, hence not state machine to attack
  - No keys are sent in channel, hence no in channel keys to attack
  - No human identity used, hence no posable identity theft
- All parties have non-repudiable Global Secure Identities
- All transactions are atomic and hence fail safe
- Triple entry accounting coupled with immutable ledgers provides guaranteed auditable transactions
- All transacting parties must provide evidence to support strong mutual authentication
- All Block Chain Ledgers are quantum-hard or safe from future quantum computing attack vectors today
- Mandatory and scalable security policy to allow bindings of a range of secure devices via a risk based policy. Support for low assurance to high devices with accredited Trusted Platform Modules
- Security solution is scalable to match payment risk
- The Digital Financial Market Infrastructure is secure by design.

THE DOUBLE STRAND BLOCK CHAIN

- After some millions of years passed, evolution had “found” a double-stranded RNA analogy (DNA itself), is more robust and stable and hence adopted by most of the living organisms today.
- The double-strand, block chain provides technical redundancy, a risk-managed solution for the global **financial market infrastructure**, and affords **practical quantum safety** with a strand based transaction latency of ~ 100ms today.
- The technologies used to implement the cross-chain atomic swap, must also have zero temporal dependence, otherwise, it will be defeated by future quantum computing advances, rendering all time dependence solutions impotent.
- The Double-Strand Block Chain Ledger combined with the Inter-Ledger Protocol (ILP) is the DNA underpinning Global Marketplaces.
- The double strand block chain ledger is algorithm agile, and hence can evolve its algorithm support to meet any future cryptographic attack vectors.
- The double strand block chain ledger is quantum safe today.

The double strand block chain ledger, is Secure by Design.

FOR FURTHER INFORMATION

- Please, contact Alexander SAMARIN
  - Mobile: +41 76 573 40 61
  - Email: alexandre.samarine@gmail.com
  - Skype: m765734061