TOWARDS STANDARDIZED KYC/AML CERTIFICATES FOR DECENTRALIZED FINANCE FOR GOOD WITH HARDWARE WALLETS

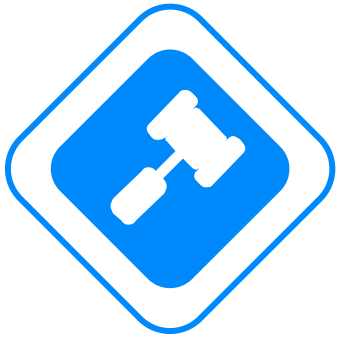
Dr. Jean-Marc Seigneur, https://www.linkedin.com/in/jmseigneur, May 2021

DECENTRALIZED FINANCE (DEFI) FOR GOOD

DEFI FOR GOOD

- **Ecosystem https://www.defi-for-good.com where:**
  - **good people can benefit from decentralized finance, even poor ones**
  - **bad people, like terrorists and criminals, must be excluded**

- **Current Know Your Customer (KYC) and Anti-Money Laundering (AML) are too rigid to work:**
  - **offline**
    - "a Central Bank Digital Currency (CBDC) system should be extremely resilient to operational failure and disruptions, natural disasters, electrical outages, and other issues" [Joint report by The Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors of the Federal Reserve and Bank for International Settlements]
  - **for poor people who don't have official documents (identity cards, proof-of-address by utility bills…)**



Financial Action Task Force (FATF)

- **“Lack of documentation is one of the central reasons for not having an account”** http://www.fatf-gafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf

- **FATF recommendations**
  - **endorsed by 180+ countries**
  - **no universal methodology for conducting AML**
    - document-based identification is NOT mandatory, innovative solutions are possible as long as a risk-based approach is respected
  - **ensure that even DeFi platforms have some form of KYC rules, even if there’s technically no single party responsible for a live network**

KYC/AML Certificates

- It is the reason that we have started discussions on how to standardized digital certificates representing KYC/AML at the ITU

- Example
  - UBS certified that Alice successfully passed KYC/AML on May 18th
    - Name of the certifier
      - Issue of trust (computational web of trust or centralized list)
    - Date of digital signature
    - Date of expiry
    - KYC/AML levels passed
    - …

- Initial implementation based on X509 extensions or W3C Verifiable Credentials

AFFORDABLE HARDWARE

- Poor people who live in harsh environments (slum, desert…) cannot afford expensive smartphones with expensive data subscriptions even if their region is covered and many regions aren’t covered yet

- A few central banks have investigated secure hardware wallets for their CBDC

- China CBDC is the most advanced and serious on this strategic topic:
  - The People’s Bank of China has been the first to define the requirement for dual offline payment of its CBDC with several patents since 2016:
    - “method and system for offline payment adopting digital currency chip card”
    - “off-line payment method, terminal and agent delivery equipment based on digital currency”
    - “blockchain-based offline payment system and method”
  - Trials have already started

BEYOND A HARDWARE DEDICATED TO ONE CBDC

- Unfortunately most contributions for the Chinese CBDC are strongly linked to a central authority:
  - Privacy issue of the (foreign) government even if privacy is protected on the intermediate levels

- In 2020, Visa propose to use hardware security modules and Trusted Execution Environment (TEE) for CBDC because:
  - they are integrated into more and more devices
  - they are even more attack-resistant than previously
    - in 2010, attack cost >100k $ with a high risk of destruction [Tarnovsky]
    - attacks not economically viable for a medium amount of money
      - Moneo e-money hardware wallet showed it can work in real life

- Still the issue of losing the money when the hardware wallet is lost

OUR REPUTACTION HARDWARE WALLET

- **Patent filed at the beginning of 2018** https://patents.google.com/patent/FR3077151A1/en
- **Compatible with any Bitcoin and Ethereum ERC-20 tokens, so including potential ERC-20-based CBDC and existing fiat-backed stablecoins (USDT…)**
- **Solving the major issue of losing the money when the hardware wallet is lost**
- **Anonymous by default but with additional KYC/AML certificates, excluding terrorists and criminals, even offline**
- **Open to deal with any CBDC or interested projects to integrate our solution**

TECHNICAL LAYERS
HIGH-LEVEL VIEW

Coin (Libra/Diem, Bitcoin, Ether, ERC-20 CBDC…)

Wrapped with strong hardware (tamper-proof, water-proof…)

Wrapped with enforced intelligence

(KYC/AML enforced with certificates, even offline, with or without additional computed reputation…)

1: The nomad decides to store 10 Libras before going to the desert (disconnected) in new keys generated by the device that will never be seen by any human, even the owner
Only the device can sign and transfer those keys to other devices
No double-spending is possible, even offline, while being disconnected

2: The nomad wants to buy water

3: The seller KYC / computational reputation is OK

4: The nomads confirms willing to pay 0,1 Libra for the water

5: The nomad’s device transfers key(s) (or signed message(s)) corresponding to 0,1 Libra to the seller’s device
Those keys won’t be able to be double-spent by the buyer and cannot be extracted by the seller who is their new owner
When still offline, the seller can transfer/spend those 0,1 Libra via the device in proximity with another device
When reconnected, the 0,1 Libra can be used or transferred to other Libra addresses directly controlled by the seller

DEFI FOR GOOD

THANK YOU

First conference on June 7th 2021, registration on https://www.defi-for-good.com