BitMint

Quantum Randomness Money

NON-MOBILE DIGITAL OFFLINE PAYMENT SOLUTION

RBI WEBINAR, JAN 2022

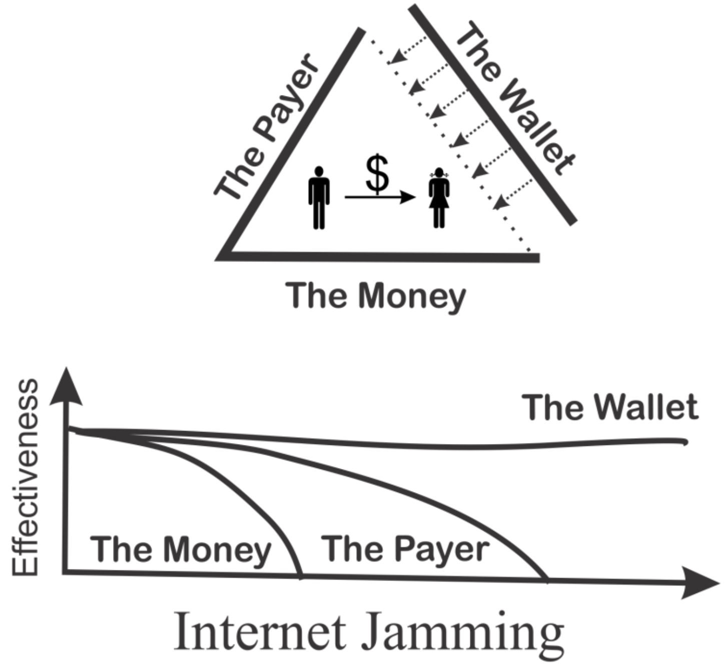
Hard Wallets

- The Critical Third Leg for Payment Trust
- We Trust the **Money** (cash)
- We Trust the **Payer** (credit card, Peers)

And now:

- ***We Trust the Wallet.***

With or without the Internet.



The Transaction Authentication Triangle

BitMint
Quantum Randomness Money

BitMint introduces Security of offline payment solution that are not linked to any external system for conducting consecutive payments.

Introducing New Technology to Achieve Sustained Offline Payment of Digital Currency

The Challenge:

Smart card solutions provide secure environment that many times rely on tamper resistance device that might be vulnerable to:

(i) superior tampering, and

(ii) counterfeit wallets.

And in most cases cannot provide finality of settlements in the offline mode and are limited in number and volume of transactions

The solution:

The proposed BitMint HardWallet [HW], mitigates above challenges.

It is based on the innovative idea of quantum-randomized nanotechnology, utilizing public-ledger technology.

BitMint's HardWallet comes with built-in scalable resistance to tampering – so it stays one step ahead of its attackers.

The HardWallet scalability insures its defense against counterfeiting – through open-ended increased counterfeiting difficulty.

It is a closed enclosure containing the money and the payment software. The secure software erases all money paid out; double spending is prevented.

The HardWallet is pre-charged with genuine coins and recharged by the Mint, and can work continuously for long months without need to electricity recharge.

One HardWallet is paid from another HardWallet, thereby creating a trusted off-line payment regimen for as long as the Internet is compromised.

The HardWallet exploits state of the art nanotechnology and recent development in quantum randomness.

Procedure:

Values are stored locally in the Hard Wallet and transferred peer to-peer without ever having to be online.

The HardWallet will readily split offline the amount of cash it holds, making smaller payments as needed.

Very convenient for use also for nontechnology savvy users.

The HardWallet authentication and the payment are executed by a quick touch of payer's and payee's Hard Wallets, achieving payment finality.

Any tampering attempt will skew the results of the measurements and fail.

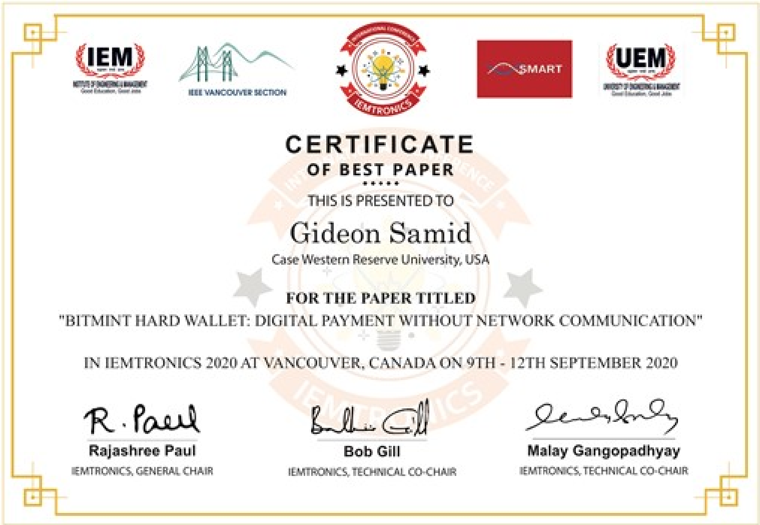
Off-line is defined as a lack of Internet connection and no access to electricity.

Off-line payments means that the payer and the recipient should be able to validate that the locally stored digital money are genuine and execute a transaction within seconds, making the payment final.

Peer reviewed article:
Publisher: IEEE

https://ieeexplore.ieee.org/document/9216456

BitMint Hard Wallet: Digital Payment without Network Communication :
No Internet, yet Sustained Payment Regimen between Randomness-Verifiable Hard Wallets



IEM
IEEE VANCOUVER SECTION
IEMTRONICS
SMART
UEM

CERTIFICATE
OF BEST PAPER

THIS IS PRESENTED TO

Gideon Samid

Case Western Reserve University, USA

FOR THE PAPER TITLED

"BITMINT HARD WALLET: DIGITAL PAYMENT WITHOUT NETWORK COMMUNICATION"

IN IEMTRONICS 2020 AT VANCOUVER, CANADA ON 9TH - 12TH SEPTEMBER 2020

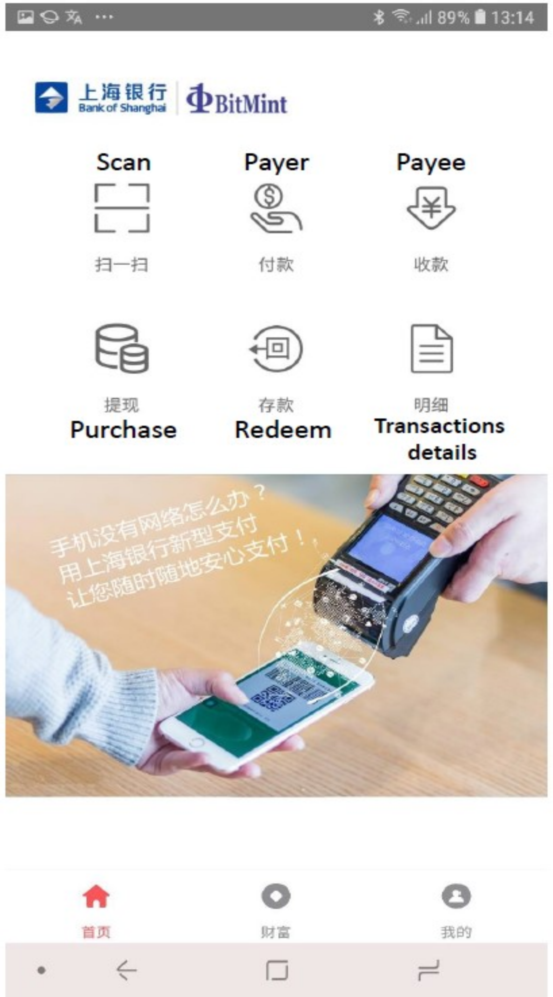
R. Paul
Rajashree Paul
IEMTRONICS, GENERAL CHAIR

Bob Gill
IEMTRONICS, TECHNICAL CO-CHAIR

Malay Gangopadhyay
IEMTRONICS, TECHNICAL CO-CHAIR

Suite of products. Stage of development

Software based solution was built and tested in real world conditions, passed tough banking stress tests, enabling money sent phone to phone also via SMS on featured phones.



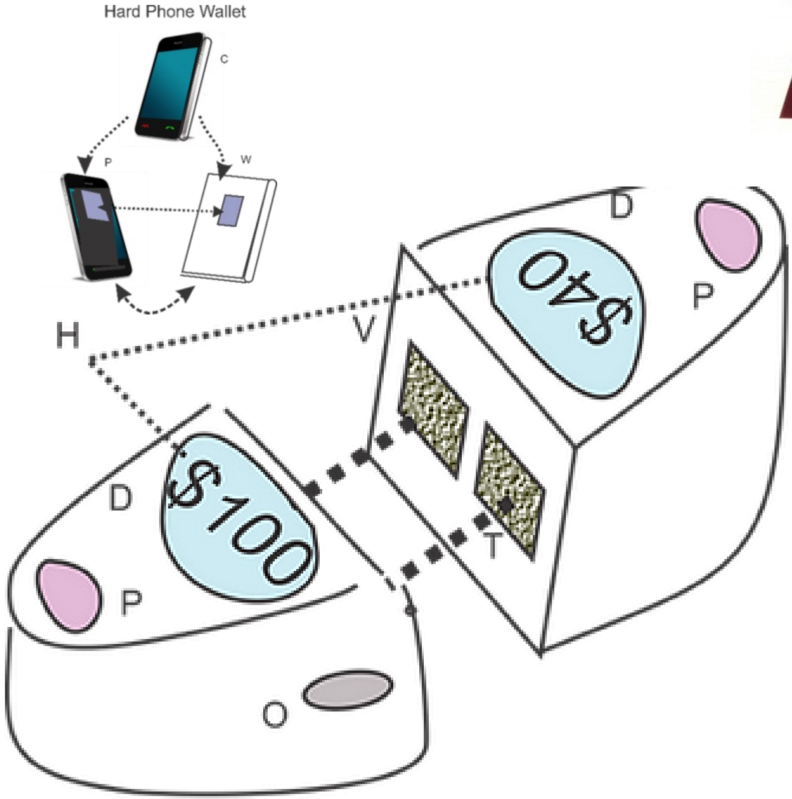
BitMint Hard Wallet creates a trusted off-line payment regimen, enabling payment continuity indefinitely from one trusted wallet to another.

Tamper Resistant BitBox

* light * pressure * radiation

The ultimate Hard Wallet for conducting consecutive payments that are not linked to any external system, no Internet, no mobile phone, is being built (prototype) in our laboratories in the US (Currently testing combination of polymers and metals).

Patent granted.



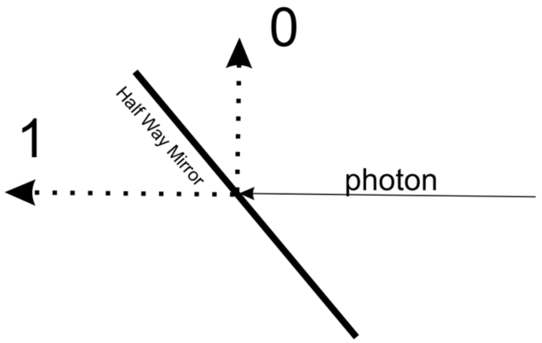
For illustration purposes only. ***Enlarged***.

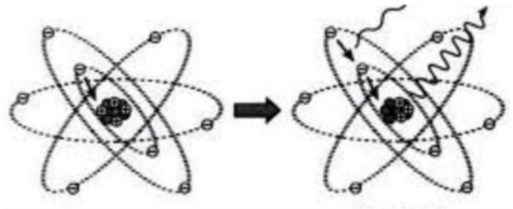
Two-Ways Hard Wallet Payment

A trusted coin

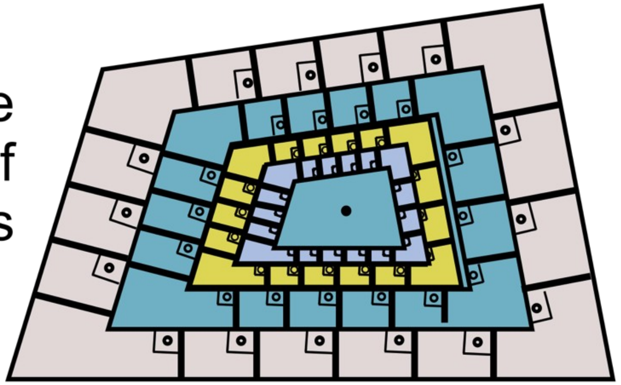
BitMint
Quantum Randomness Money

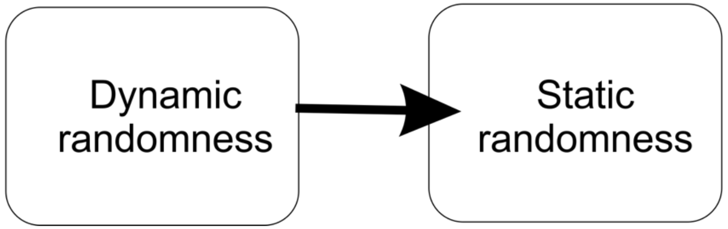
Capturing Quantum Randomness in a Chip





The Rock of Randomness





Dynamic randomness

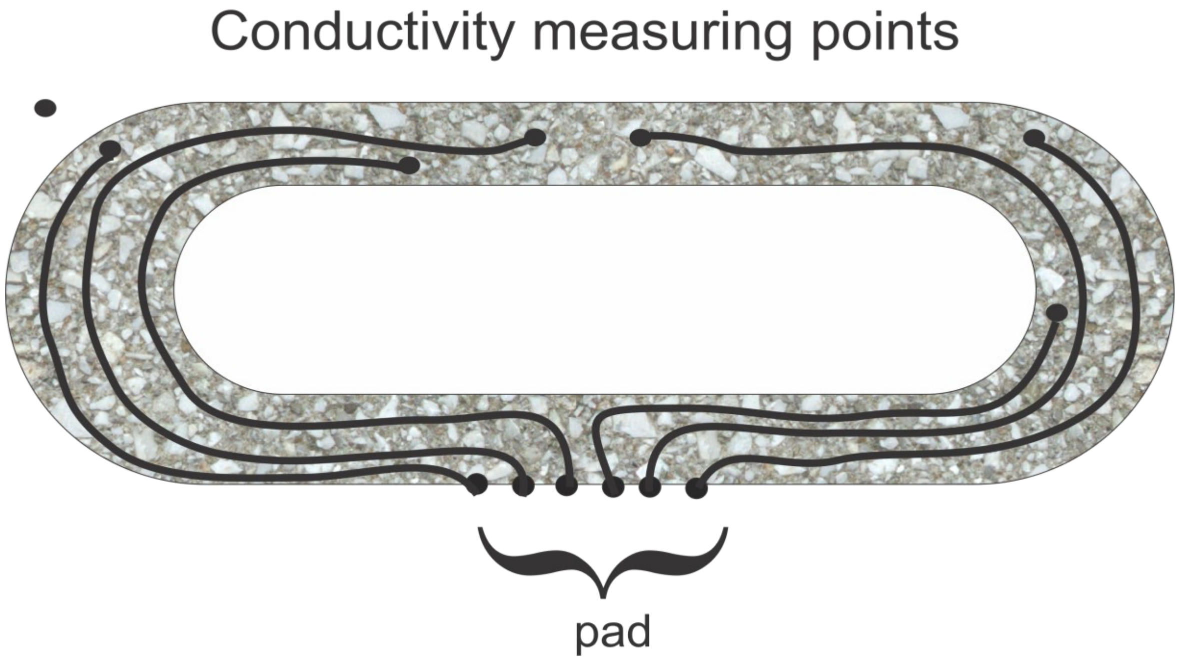
Static randomness

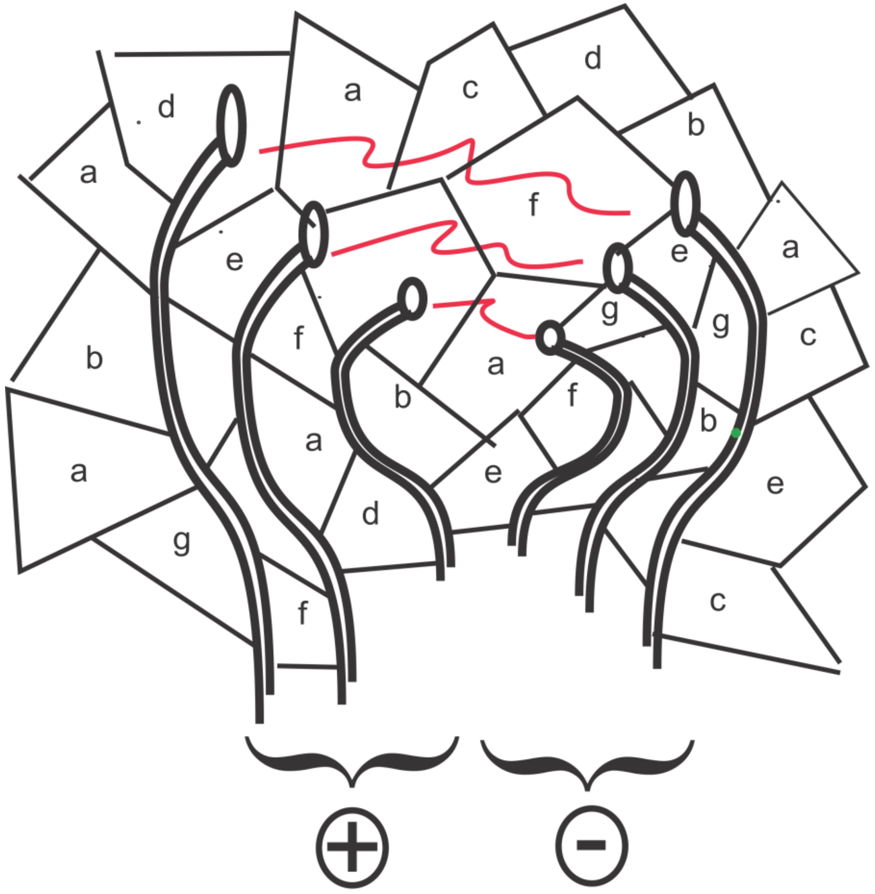
Trust Basis

- The Hard Wallet is trusted on account of being constructed through a nanotechnology process where the input data is

  quantum-grade randomness.

Infinite Randomized Features

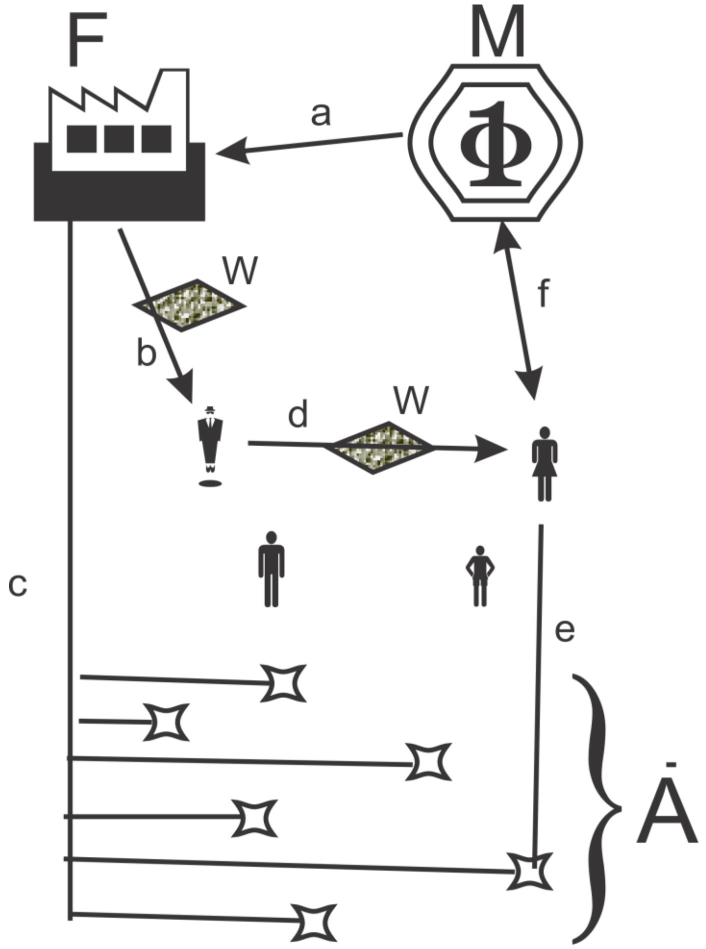




Randomized Rock Resistance

BitMint
Quantum Randomness Money

The Hard Wallet Payment Process



The Hard Wallet Dynamics

Payment is enabled because BitMint money unifies value with identity.

The Mint is accountable for the Money.

The HW manufacturer is accountable for the wallet.

PROBLEM s to be solved	**BitMint Hard Wallet**	**Published offline solutions(#)**
Payment continuity anytime, anywhere………………….	√	partly
INCLUSIVE: for ALL, including non-technology savvy…	√	partly
Finality of settlements in offline mode …………………….	√	Usually not! (unless payee takes the risk)
Quantum-safe {*} ……………………………………………….	√	NO!
Scalable resistance to tampering …………………………….	√	NO
Defends against **counterfeiting ……………………………….**	√	partly
Defends against **double spending …………………………….**	√	Not in offline mode
Two-Ways Wallet. Not limited value & transactions …….	√	One way, until empty
Creating a trusted off-line payment regimen With no Internet and no mobile phones and no electricity for months…………	√	Partly trusted, and requires electricity charging after a few days or weeks

----

(#) based on online publications

{*} The elephant in the room: Quantum computers

World Economic Forum (WEF): "Quantum computing will ultimately impact all financial services as it compromises major data encryption methodologies and cryptographic primitives used for protecting access, confidentiality and integrity of data stored and transmitted. CBDC is no exception". https://www.weforum.org/agenda/2021/11/4-key-threats-central-bank-digital-currencies/

BitMint
Hard Wallet

Q&A

amnon@BitMint.com

Sustained Off-Line Digital Payment Technology
The last hurdle before digital money becomes the money people use