



האוניברסיטה העברית בירושלים
THE HEBREW UNIVERSITY OF JERUSALEM

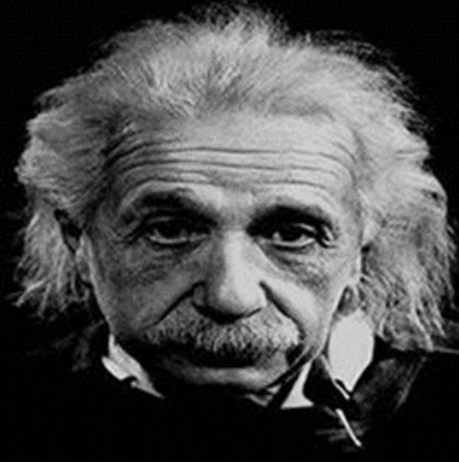
The Hebrew University Fintech Center

Founded by Sima & Shlomo Gershon

The Jerusalem Business school – MBA program

CRYPTO2.0 ★ WEB3 ★ LEVEL QUANTUM-MONEY ★ CBDC ★ SWIFT-VERSUS-INTERMINT

“I am neither clever nor especially gifted. I am only very, very curious.”
-Albert Einstein



Amnon Samid



BitMint



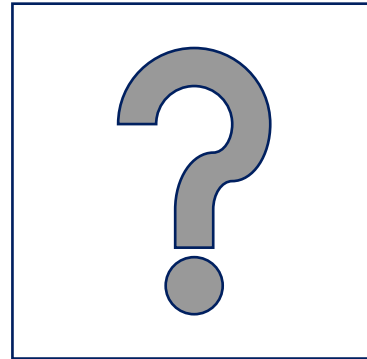
Digital Euro
Association



טבת התשפ"ב

Quantum-Cryptanalytic Resistant Solutions * Fair Money in an Unfair World

Can a smarter actor defeat us?



Hint:



RANDOMNESS 

Replacing Rigidity and Complexity with Randomness and Simplicity

https://www.digitaltransactions.net/magazine_articles/security-notes-cyber-oil-the-undefeatable-equalizer/

Money

Three main attributes of money:

- Store of value
- Unit of account
- Medium of exchange.



Overlooked are other attributes:

- (i) Money creates a bond between two strangers
- (ii) Money is a social lifeline
- (iii) Money is universally desirable

Non Speculative
Digital Money
is introduced
as claimchecks
for paper money



The Abstraction of Money

(i) Creating a bond between two strangers

Neither card payment, nor crypto payment today can replace the minted fiat coins and banknotes because they robbed people from the basic experience of bilateral payment.

Two strangers may pass a bundle of dollars from hand to hand, and no one except them will know about it.

If they use a payment card they surrender the knowledge of the transaction to the card company and to their respective banks.

If they pay bitcoins, the whole world knows about the transaction, and soon enough quantum computers will unveil the identities of the payor and the payee.



Bilateral payment is non-existent today except for discrete passing of cash. This bilateral experience is so important for our well being that as long as technology cannot offer it, the old coins and banknotes will stay in circulation.

An outcome from the evolution by consensus and crypto-based digital currencies is the need for a new approach, quantum-safe, that puts users in charge of their data, money and privacy.



BitMint * LeVeL
Decentralized Math Digital Coin

**Bilateral
Payment
Restored.**

Replacing old cash
with Hi-Tec Cash
Same Privacy for the Law Abiding

Bilateral Payment is the coming revolution

Restore the old way of payment



BitMint * LeVeL
Decentralized Math Digital Coin

**Bilateral
Payment
Restored.**

Replacing old cash
with Hi-Tec Cash
Same Privacy for the Law Abiding

LeVeL enables Bilateral Payment that is homomorphic with cash payment:

- strictly bilateral, when the app is installed in every phone, and
- when instead of a phone you use a nano-technology coin, that is jingling in every pocket, it acts like cash, although digital.
- Privacy will reign, benefitting the law-abiding citizens.
- The Hi-Tec sophistication in this cyber cash will deny criminals from abusing this precious privacy.

LeVeL:

- Better Privacy
- Quantum Safe
- **Accommodates Everyone**

Mutated Digital Coin

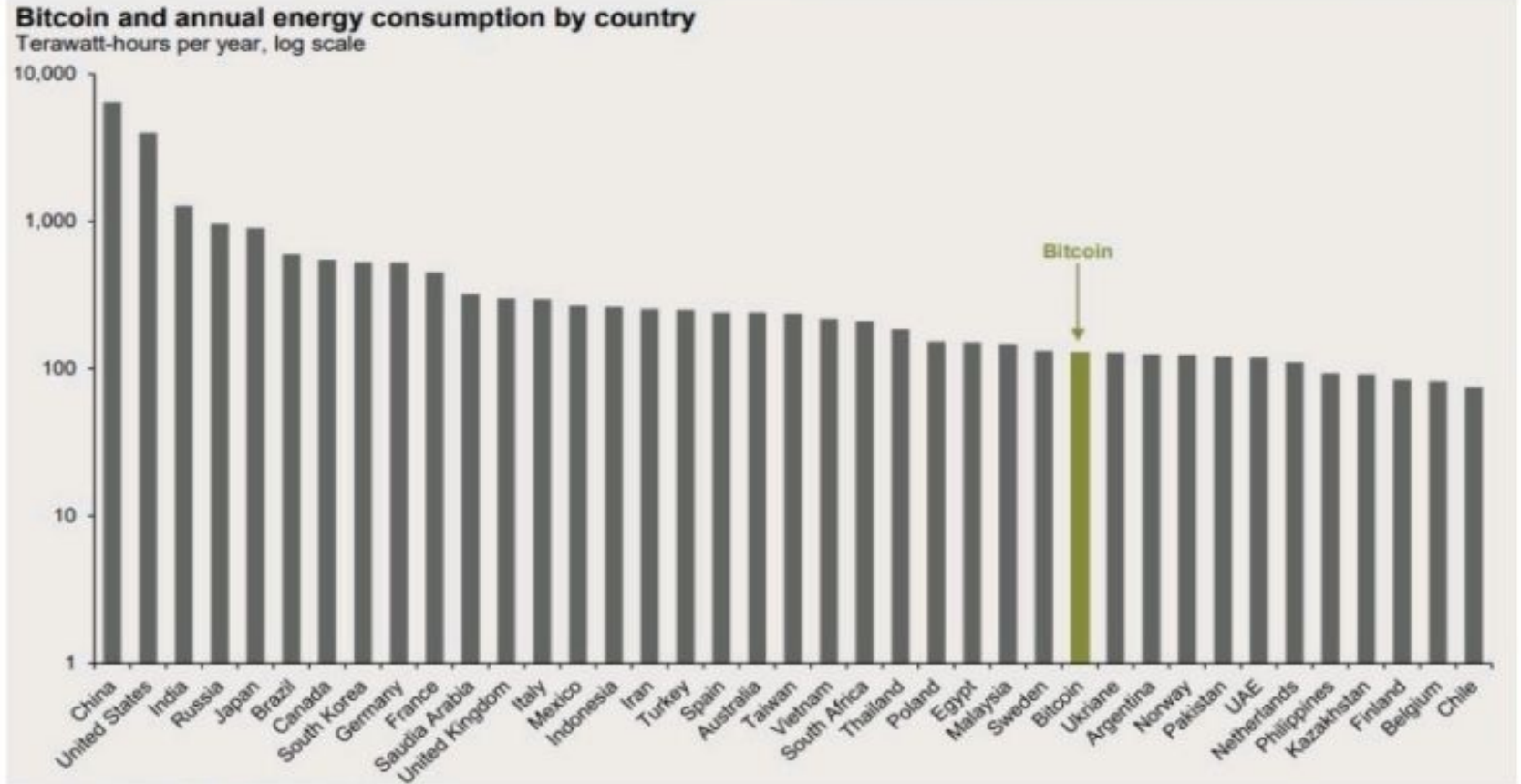
- Allowing each new payee of a digital coin to add their own algorithmic intractability barrier.
- The more a coin passes around, the more difficult it is for the quantum attacker to defeat it.



Decentralized minting is not necessary for achieving decentralized financing

If coins are centrally minted and not via a mining process, and if transactions are directly phone to phone, w/o intermediary, the computing processing power will be lower than current payment rails. It was demonstrated in a real world pilot [*Qpay*, powered by BitMint].

Hedge funds



Sources: Bloomberg, J.P. Morgan Asset Management
Data is based on availability as of August 31, 2021.

(ii) Social lifeline

Purpose-Driven Tethered-Money

Preventing Hoarding, *Eliminating Shortages of Necessities,*
Maintains a Society Under Duress, while preserving freedom of choice

Governments and municipalities should have the power to immediately mint money, inject money and redeem money that is purpose-driven (Tethered).

There will be money for food and money for gas and money for healthcare – pre allotted. This will hinder abuse and fraud.

In the event of a major community disaster, it is paramount to allow people to trade, to exchange, to cooperate into bouncing back.



A digital coin may be cryptographically 'fused' with pre defined terms of payment, preventing misuse, holding off corruption, frustrating fraud.



(iii) Money is universally desirable - which means should create **TRUST**, should be available to all (**inclusive**), not dependent on network or mobile phone.



Payment Trust & Simplicity

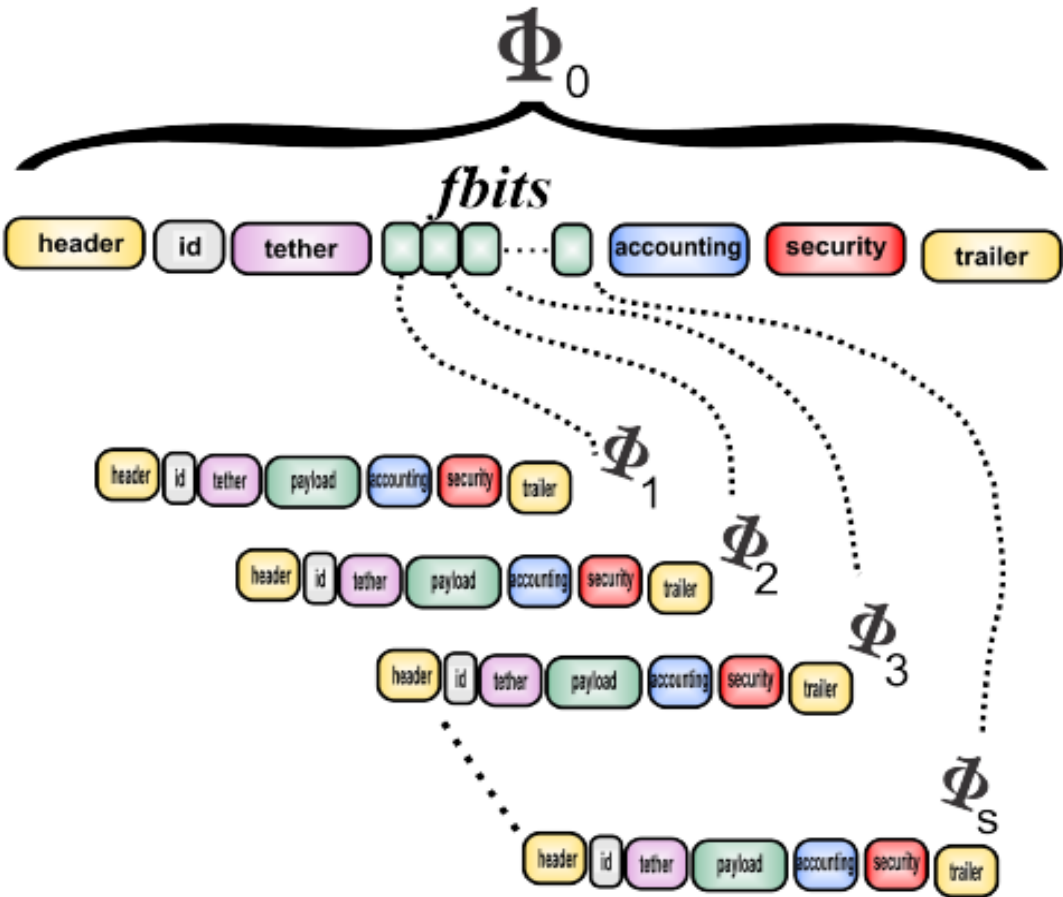
Three ways to create trust:

- **Identifying the "object"** (the coin) in order to trust the money paid (like you trust banknotes or gold coins).
- **Identifying the individual** = trusting the payer (for a payment to occur across a data base, the payer needs to prove that they "own" a spot in that data base, and that this spot has sufficient funds.)
- **Trusting the wallet** (what we name: Hard Wallet) from which payer transfers the coins to the payee (this is relevant for offline payment, when Internet/WIFI is jammed, and also enable to transfer large amount of money).

So, **instead of trusting an algorithm, the payee has a mean to check the wallet** if it is trustable, and then the payee knows that any money that goes out from the wallet is valid and not counterfeit.



Cascade Coin



Cascade Coin is comprised of several Coins. In cascade coin, every fbit is a full coin.



In contrast to SWIFT, the cascade coin can be used in international financial trade. Traders can use cascade coins to do business with less exchange rate influence, which is comprised of Euro and Dollar or other digital fiat currency plus any combination of commodities like gold and silver. The cascade coin will be most stable because of how it is structured.



It can express a multi party contract. All the legal details in the contract will be expressed in the coin. The coin will be redeemed only if all the necessary terms are met. No need for accounting follow up.

Cross border payments

The challenge:

Cross-border payment is still a pain point despite the RTGS, which did not really solve the interoperability between systems; still cause credit risks and settlement risks and the cost is high.

On top, the large sums of money that flow between global and national banks is a persistent attractive target for **electronic thieves**.

Such transfers are **validated by backtracking the history** of the money which is the tedious effort of reconciliation.

The BitMint Financial Alphabet offers Innovation to make cross-border payments all around the world easy, fast, secure and competitively priced

Cross border payments



Security * Reconciliation * Accountability

With BitMint's ALFi all transactions are centrally validated at the mint that issued the transacted digital coin.

No need for backtracking.

As long as the mint's integrity is intact, so is its instant reconciliation process.

With BitMint's ALFi each digital coin has a unique identity, which is associated with its owner.

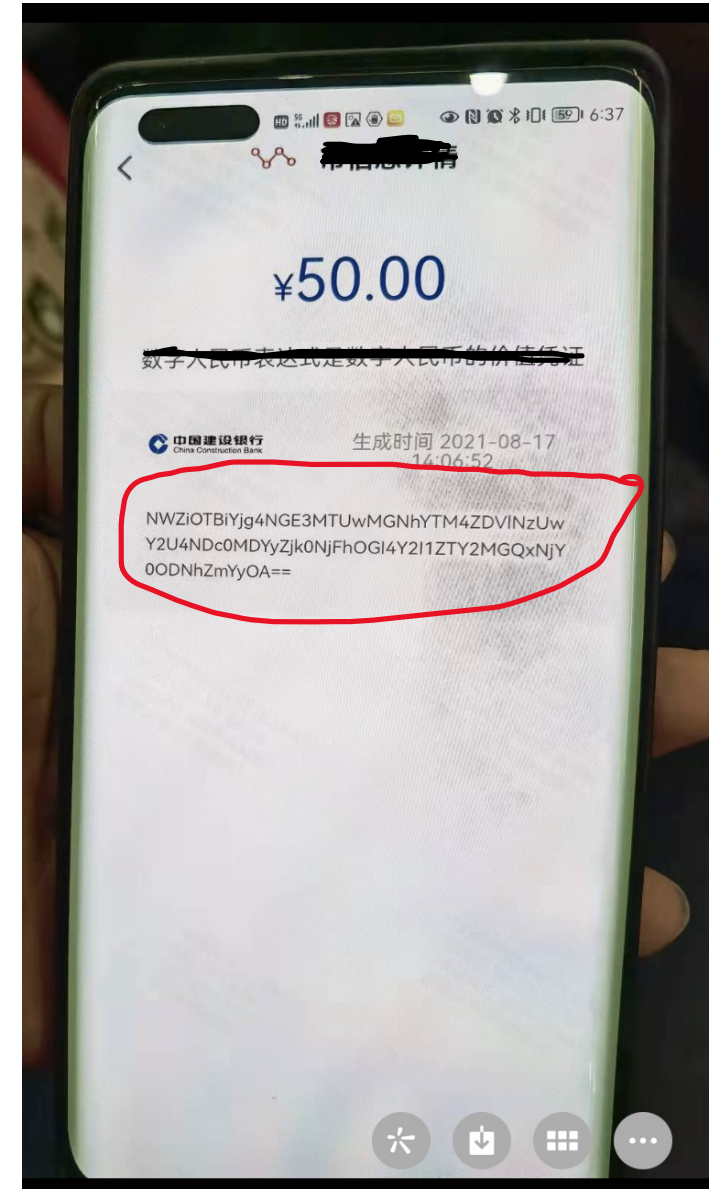
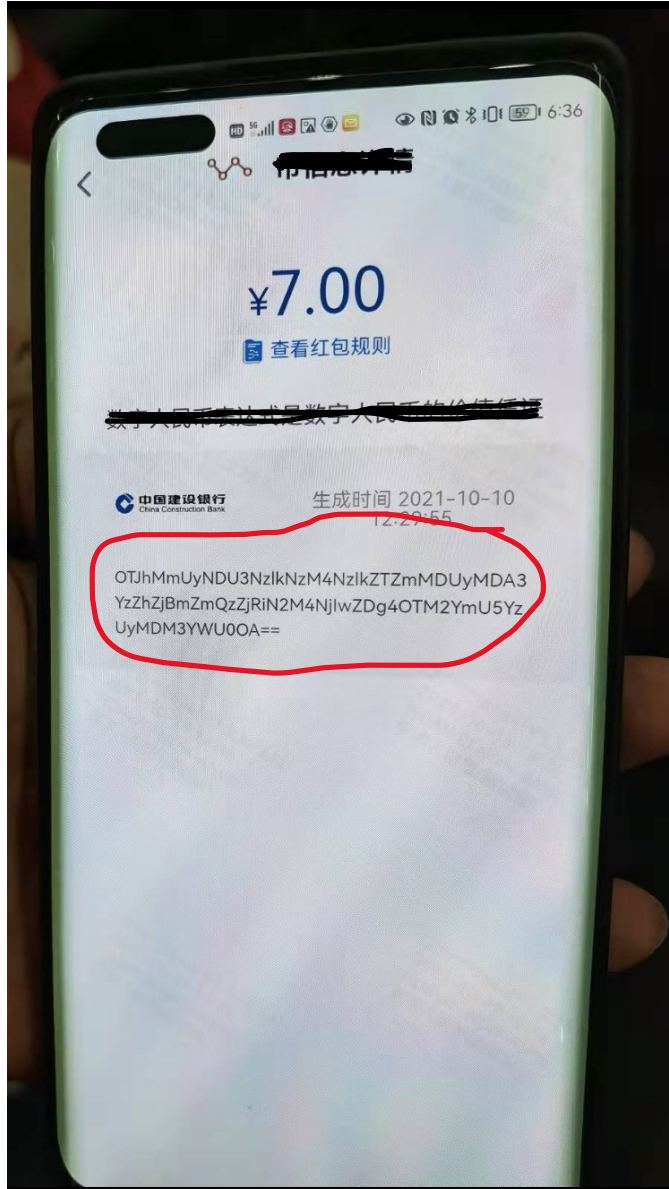
Stealing it will be pointless - a cryptographic lock keeps non-owners from spending the money.

The BitMint digital coin carries with it its full chain of custody, and thereby creating an accounting Tri-log: income books compared to expense records, and both compared to the chain of custody tallied in the BitMint coin. Mistakes are prevented, untoward money routing is exposed.

- On top we propose a **Superposition Currency** for Cross Border Payment: Digital Currency that is traded as a temporary currency indeterminate between the payer's currency and the payee's currency.
- In conjunction with local CBDCs, the superposition money enables the interlinkage options to facilitate efficient cross-border and cross-currency payments between different jurisdictions.

Lessons learned from practical projects.....

by December 2021, a total of 261 million personal wallets have been opened, with transactions amount of 87.565 billion yuan (13.6bn USD)



AI based framework for global Quantum-resistant online/offline value based CBDC, (Powered by BitMint). without the hassles and vulnerabilities of crypto.



A few examples of unique capabilities/features/functions of this
AI based framework for global Quantum-resistant
online/offline value based CBDC



Continuous Payment: Digital Currency for the Internet of Things

Pay-as-you-Go

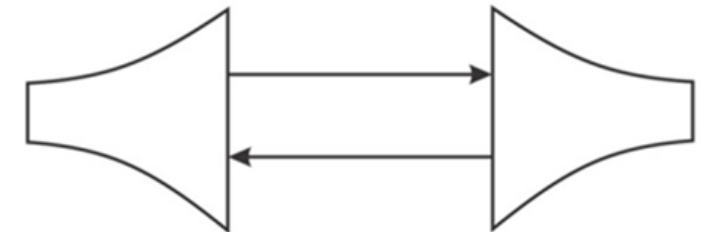
from your car,
from your wallet,
from your phone,
from your refrigerator;

stream-pay your cyber consultant for as long as she pays attention to you,
hop into a taxi and pay as you ride for as long as you ride;
pay to charge your electrical vehicle,
pay for streaming -- while enjoying the movie;

NOW* you can do so --
without post-accounting,
with no next-month-invoice, and
with anonymity to boot.



IOT real time pay for services



Service Provider Node

computational services
data services
device use services
etc.

Services User Node

pays with BitMint digital
cash – payment bits against
service bits

BitMint Technology enables direct payment, not account based

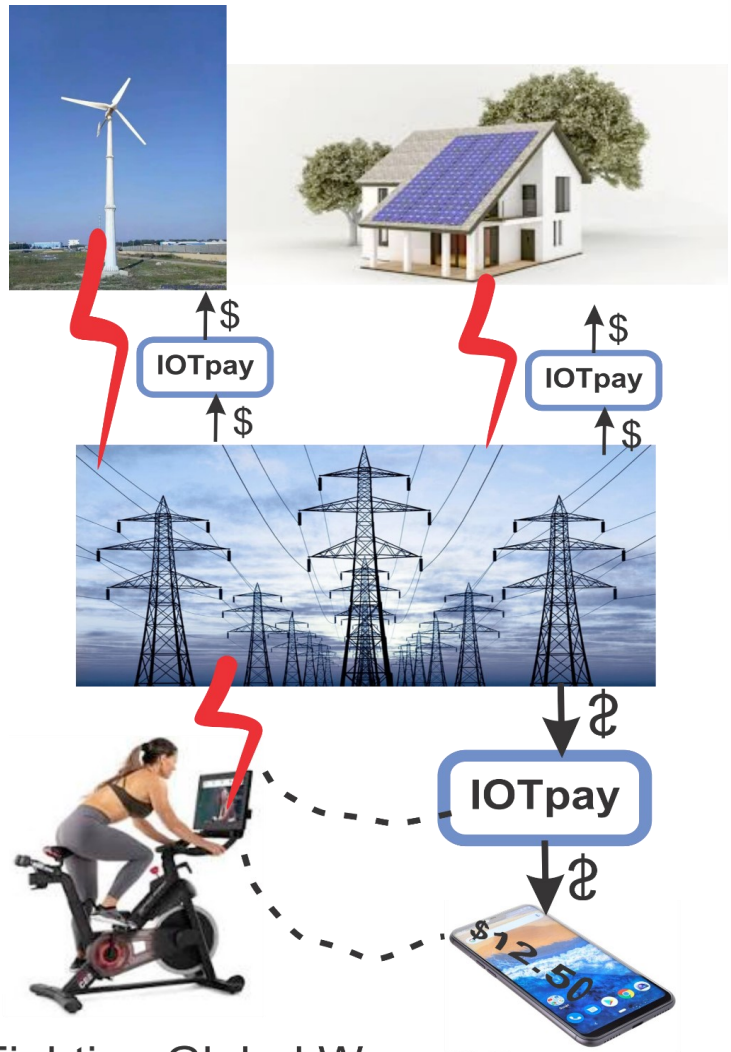
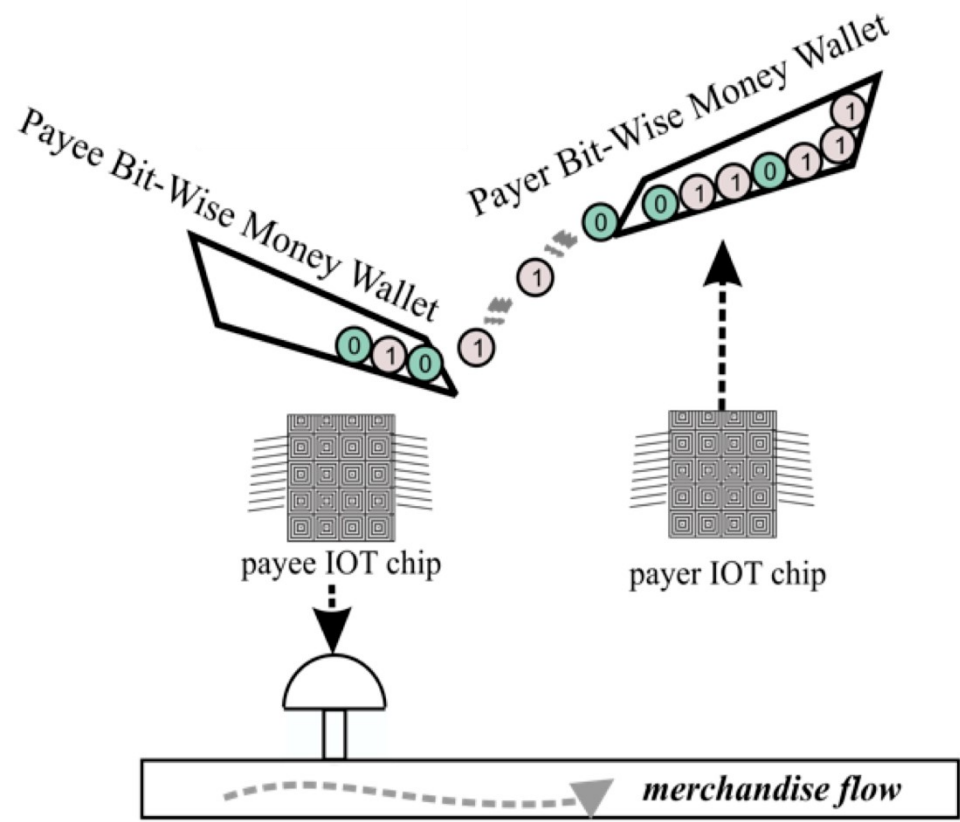
Let the Internet of Things take care of daily routine payments, while you keep yourself free spirited.

*Take advantage of this technology for this smooth continuous payment, close by and cross border, sums as large or as small as desired.



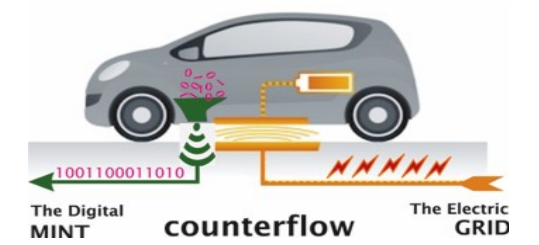
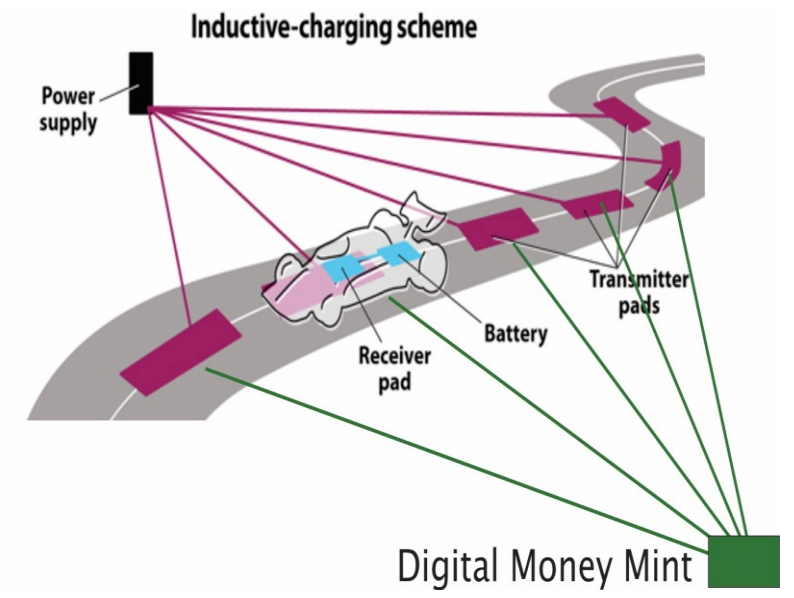
Frictionless Payment

Continuous Pay-as-You-Go!



Fighting Global Warming

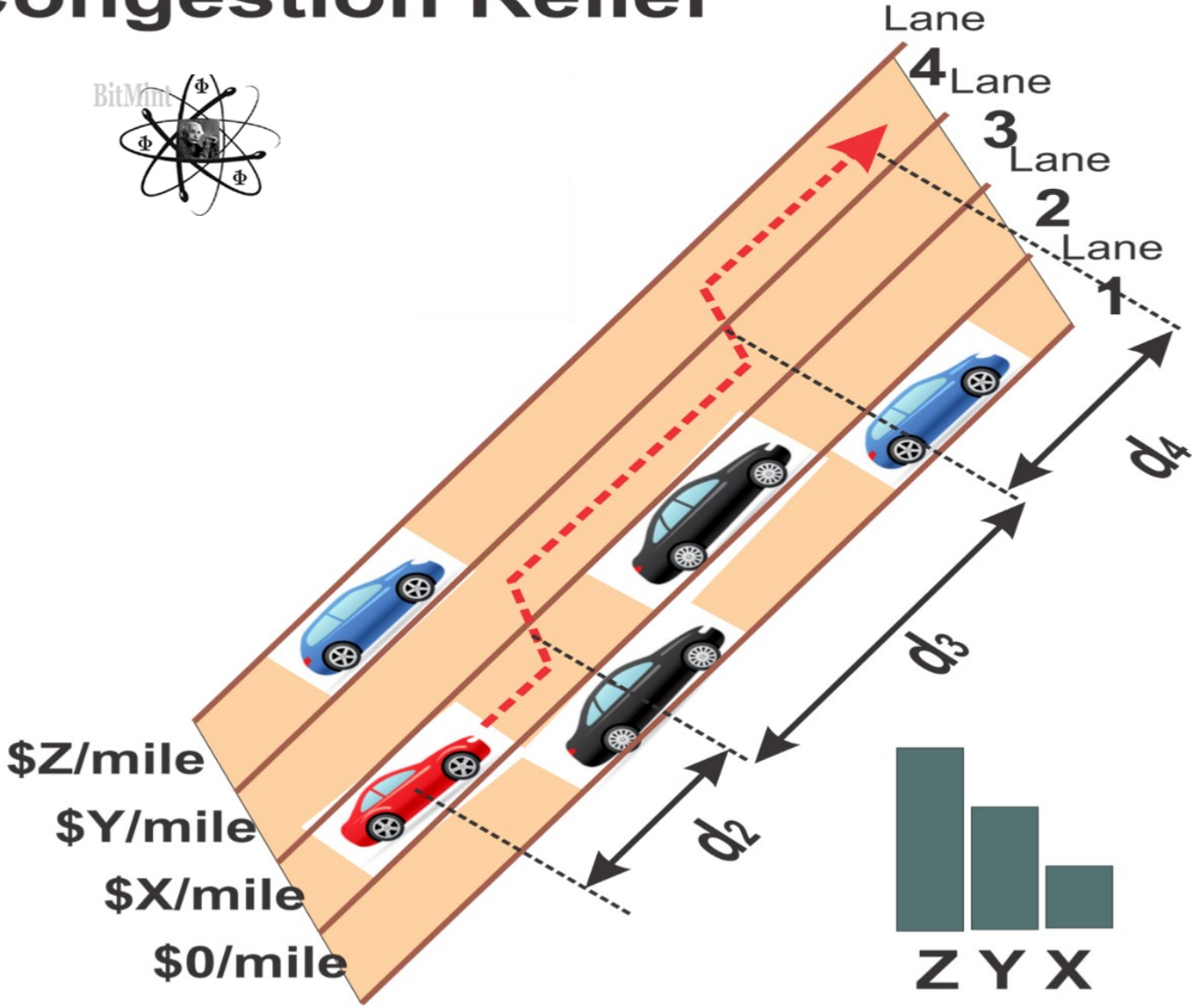
Payment is executed automatically



In-Vehicle payments

auto continuous pay

Congestion Relief



Pay = \$X*d2 + \$Y*d3 + \$Z*d4



Smooth payment systems in time of crisis

BMTS has a vital role to play to maintain social order in time of crisis. Smart, secure and smooth payment systems are among the underpinnings of social tranquility, and we are the custodians of those systems

Our solutions are based on the following principles:

- In a time of crisis there has to be strong centralized controls and governance.
- Distribution of funds made available has to be frictionless and tightly monitored
- The lack of the two above points will promote
 - Interaction on the marketplace not being driven by consistent factors
 - Opportunistic behaviors to generate revenue
 - Fragmented supply chain, including not matching supply to needs
 - Entropic behaviors due to lack of governance
- Focus on small to medium sized business means the only opportunity to monetize during crisis.

BMTS will support local governments in managing supply and demand priorities.

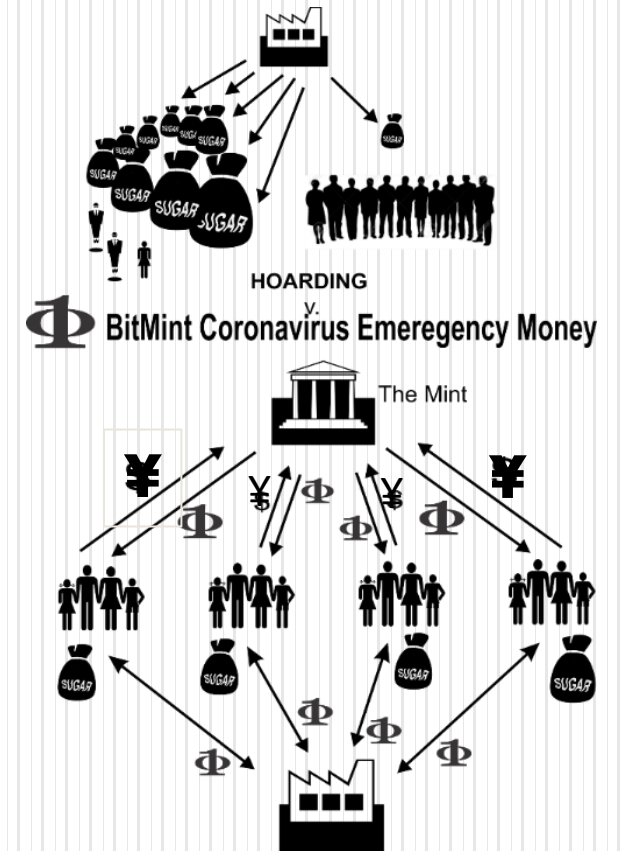
Value Proposition - Key Benefits:

Closed loop frictionless payment

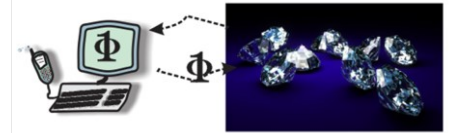
Puts control in the hands of the appropriate authority

Eliminates hoarding, black markets and price gouging

Enables SMEs to stay productive during crisis disruption



New Trading Capabilities



BitMint allows people to trade fiat currency, gold, gems, or any other valuables of choice by safekeeping these valuables with centered top-level physical security while transacting digitally convenient **IOU claim notes** for the same.

1st use-case: **Gold trade with digital claim checks**

Protect your wealth with gold digital claim checks backed by real gold stored at a storage of your will

A claim check for a certain amount of gold, X, is like a key to a readily available box where the actual gold is placed.

If you owe X ounce of gold, then, by passing the digital claim-checks to someone else, the new digital claim-check holder has the gold at their disposal. And the new holder, can pass the entire amount of gold, or any portion of it, to another trader.

As long as these traders trust that the gold is readily accessible and stored in a reliable place, the digital claim-check is a valid trading instrument.

These digital claim checks can have split value, and, can be tethered (can regulate their movement).



No risk of stealing

Easy trading P2P any portion of your gold

Relax your mind-set during these overwhelming-scary times

Convenience * Security * Opportunity

Digitally evidencing ownership and easy trading capabilities of Real Estate assets

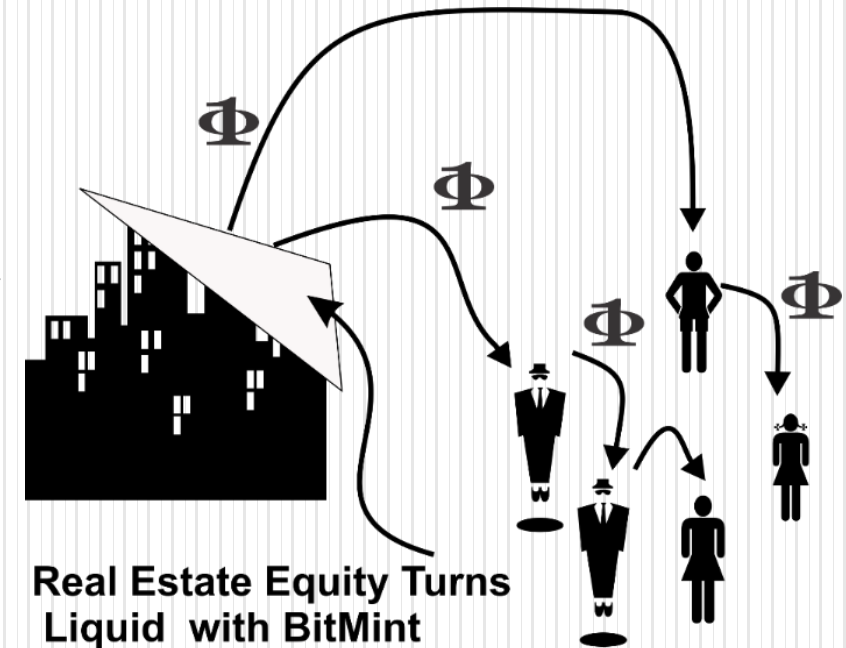
BitMint enables the process of digitally evidencing ownership of a real estate asset in a digital claim check form (let's call the "coins").

The coins can move in a frictionless mode from one to another, which opens the option to real estate merchantability among the stakeholders.

In other words, a building, for example, can be divided into small portions.

In that manner the owner of a real estate asset can raise money from the public by offering ownership stakes of the real estate.

These real-estate ownership digital claim checks will be freely traded.



**Real Estate Equity Turns
Liquid with BitMint
Tethered Money**

Hybrid coins and upload-able banknotes

will make cash 'fashionable' and modern,
with users having the choice whether to use it as metal coins or plastic banknote,
or to upload its content to their phone or any digital device



Digital version of the (metallic) cash, i.e. digital Hybrid coins will circulate under the civic-led governance and guarantee flow of value between people and businesses, and will ensure:

-
- privately, inclusively, clearly, impartially,
- effortlessly, freely, instantaneously,
- legally, securely, equitably,
- face-to-face and remotely,
- with and without access to the Internet.

**Digital Money
Inside**

Payment continuity is indispensable for national level digital currency.

Off-line payments cash like

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 to execute a transaction within seconds, making the payment final.

A Hard Wallet [HW] solution should be quantum-safe and ensure the following:

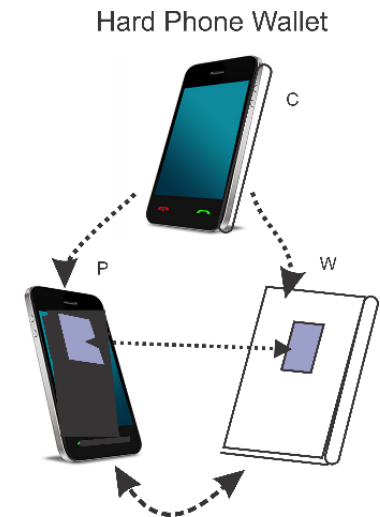
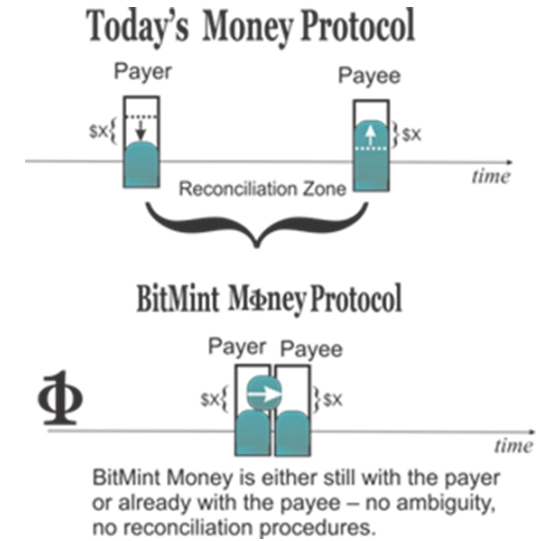
Finality of settlements in the offline mode.

Scalable resistance to tampering.

Defense against counterfeiting.

Double spending prevented.

Creating a trusted off-line payment regimen for as long as the Internet is compromised.





**Do we need decentralized minting for achieving
Decentralized financing?**

Is Bitcoin and alike really decentralized?

Is Bitcoin really private?

Two of the looming issues that threaten Bitcoin..



[i] Quantum cryptanalysis -

Actually, most crypto currencies and crypto assets suffer from

algorithmic singularity vulnerability.

Each crypto coin relies on a publicly exposed complexity-generating algorithm,

serving as a resting target for its attackers.


It is just a question of time for a quantum machine to train its terrific power on that foundational algorithm.

Once compromised the currency collapses.

[ii] Utility disengagement –

means that there is no natural floor and no natural ceiling for the price of Bitcoin, which implies an inherent instability.

IMF: Vulnerable algorithms will need to be transitioned to post-quantum cryptography. Vulnerable applications that rely on public-key cryptography also include popular digital assets such as Bitcoin and Ethereum, as well as password-protected web applications. [Fall 2021]



FT
Opinion Financial Times
December 21 2021
Why bitcoin is worse than a Madoff-style Ponzi scheme
A Ponzi scheme is a zero-sum enterprise. But bitcoin is a negative-sum phenomenon that you can't even pursue a claim against, argues Robert McCauley.

(ii) Mitigating Bitcoin Utility Disengagement

0.01% of Bitcoin holders
control 27% of the supply
By Marco Quiroz-Gutierrez December 2021

Bitcoin Protocol Modification to Secure Stability through Automated Network Dumping Capacity

It is necessary to guard against unbound price hike for keeping bitcoin alive, since there is no natural ceiling for its price.



Exploiting the fact that all the coins are publicly identified, it is possible **to tax them fairly (a percent of each coin's value)** and pass this money to an **Automated Dumping Capacity fund (ADC fund)**

The identity of the owner of the real estate makes no difference. The fund will be owned by the network as a whole. It can be implemented by solving a well-known Bertrand Russell paradox, defining a node in the network as representing the network as a whole.

Having a sizeable, automated dumping capacity fund will also distinguish the currency from any new forks or alternative protocols. It will represent the commitment of the community to the well being of the currency.

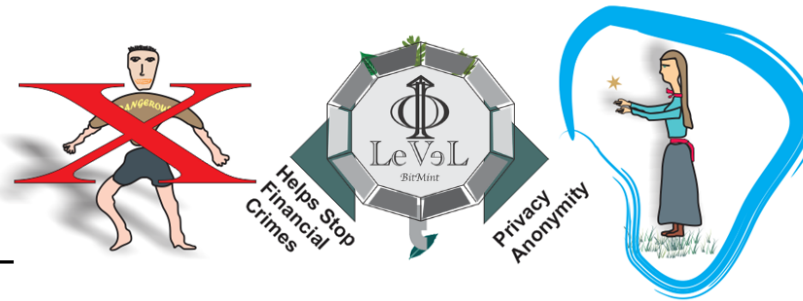
(i) Is public/private key cryptography doomed due to quantum computers' threat?

Well, a crypto saving solution just emerged:

algorithmic mutation

Replacing the resting target crypto coin with a moving target crypto coin;

Building a coin that hinges on ever changing public/private key algorithms, to keep ahead of its predator.



LeVeL can be used with both –

centralized currency (legacy money)

and with

decentralized currency (e.g. Bitcoin, Ether, Diem, Celo etc.).

The *LeVeL* protocol detects counterfeits and prevents double spending of the underlying entity of community value, be it the US Dollar, Euro etc. or be it Bitcoin.

***LeVeL** is adaptable to connectivity failures, IOT payment, and Cross Border transactions.

LeVeL protocol is critical for making all crypto- currencies, stablecoins, and CBDCs sustainable.

Decentralized but with AML.

LeVeL is acronym for:
Legacy
Extended
Value --
Entrusted
Ledger.

Bitcoin legacy of empowering its traders is herewith taken a step further....

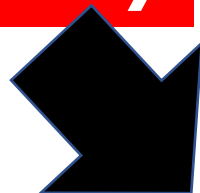
Unlike Bitcoin and alike that in fact are an **algorithmic-centralized currency** that cannot be sued, cannot be held accountable, and cannot exercise acute management intervention when it goes haywire.

The Decentralized Math Digital Currency [LeVeL] collect all the great innovations introduced by cryptocurrencies, bitcoin and alike bitcoin and reassemble them in a better way.

This LeVeL protocol or alike, that resists its most powerful attackers with the power of ad-hoc randomness, is **necessary for crypto-currencies, for stable coins**, and for **CBDC** – for those central banks that still wish to be hinged on public/private key infrastructure...

Although eventually, most central banks will adopt **The Quantum-Random money**, which by definition is Cryptanalytic Resistant money, that is minted from a well-guarded Physical Embodiment (Money-Rock or alike), decentralized distributed, and delivering Fair Money, contributing to a more fair world.

Not necessarily



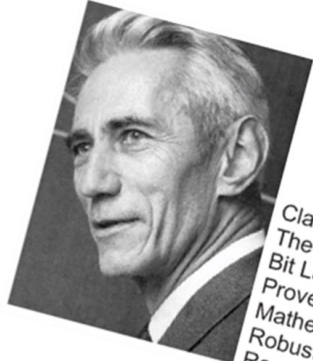
Some people define CBDC **as a cryptocurrency equivalent** of digital and fiat money, having the same technological infrastructure with crypto assets but at the same time backed by the central banking regulator.

Quantum Considerations

The Impact of Quantum Computing on Payment and Money Technology

- Modern cryptography (symmetric and asymmetric) is a financial titan, shaping up the global financial landscape.
- Quantum computing is a technological titan shaping up life in cyber space.
- These two titans clash. How to keep global finance in good order?

Battle royal between Quantum and Crypto



Claude Shannon
The Father of
Bit Languages,
Proved the
Mathematical
Robustness of
Random Bit Series

Quantum-random money The ONLY known manner

To preserve the achievements
of digital currency:

- frictionless transactions
- ease of storage
- tethering of money to its intended purpose

—all while:

- safeguarding privacy, and
- re-establishing the social bond between two strangers participating in a monetary exchange.

Quantum randomness will power the cyber space and it is rising to become the foundational pillar of all digital transactions.

Bitcoin and most of its imitators rely on the mathematical strength of an algorithm known as ECDSA.

ECDSA has been in the crosshair of cryptanalytic shops for a long time.

Some might have already cracked it, and hide this fact.

Quantum computers already crack it in theory, with practice to follow soon.

COVID-19 has accelerated the digitization of financial services, which means more and more bits are being used.....

Data can be read, stolen, without leaving any trace.

BE AWARE of the logic that guided the designers of the Titanic: who needs life boats on an unsinkable ship?



Quantum vs. Crypto

The third decade of the 21st century will witness the **battle** royal between Crypto and Quantum, between the technology that relies on mathematical complexity and the technology that dissolves it.



World Economic Forum (Nov 2021): Regardless of whether the implementation of the CBDC system will be using a DLT- or non DLT-based solution, it will involve cryptographic primitives for protecting the confidentiality and integrity of the data being stored and transmitted. Therefore, **the threat of emerging quantum computers should be taken into account when choosing the cryptographic techniques used in the CBDC system.**

[Ref #7]

Unfortunately, **crypto-based** digital currencies will not save the day. The threat is real.



BREAKING
DEFENSE

from large-scale quantum computers.”

The potential of quantum computing as a change agent was a topic of discussion at AFCEA’s TechNet Cyber earlier this month in Baltimore.

IBM

“I think it is a true statement that eventually quantum will be able to make or break every known encryption in a matter of seconds,” said IBM CIO Fletcher Previn during a session on emerging technologies. “It’s a completely different approach to computing than counting, which is the basis of all current computing. It’s possible we’ve been programming computers the wrong way for the last X number of years. Quantum is a much closer approximation to how nature figures things out.”

IMF:

“Vulnerable algorithms will need to be transitioned to post-quantum cryptography.”

Will adding more complexity mitigate the threat? The answer is:  **NO!**

The so called ‘Quantum resistant algorithms’ are governed by the premise of increased algorithmic complexity, aiming to put so much computational burden on the cryptanalyst that supposing even a quantum computer will fall short.

This strategy is blind -- we don't know the computational power of quantum computers developed behind a veil of secrecy, and hence our defense may be insufficient.

It’s scary, then.....



A completely different approach is required right away!

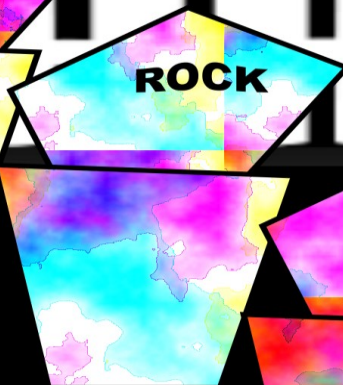
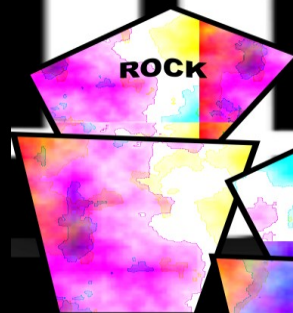
It is based on the emerging technology for high grade, high bit flow of randomness.

A suite of cryptographic products that project security through lavish use of randomness was developed; it is done based on the basis of a painstaking combinatorics analysis proving required degree of secrecy.

Users of Trans-Vernam ciphers can adjust the degree of the projected security, according to the sensitivity of the protected data. If needed, users can assure perfect mathematical secrecy.

When issuing digital currency, You make sure that the seeds of digital currency are not based on digital bits, Because bits can be hacked

Digital Territory



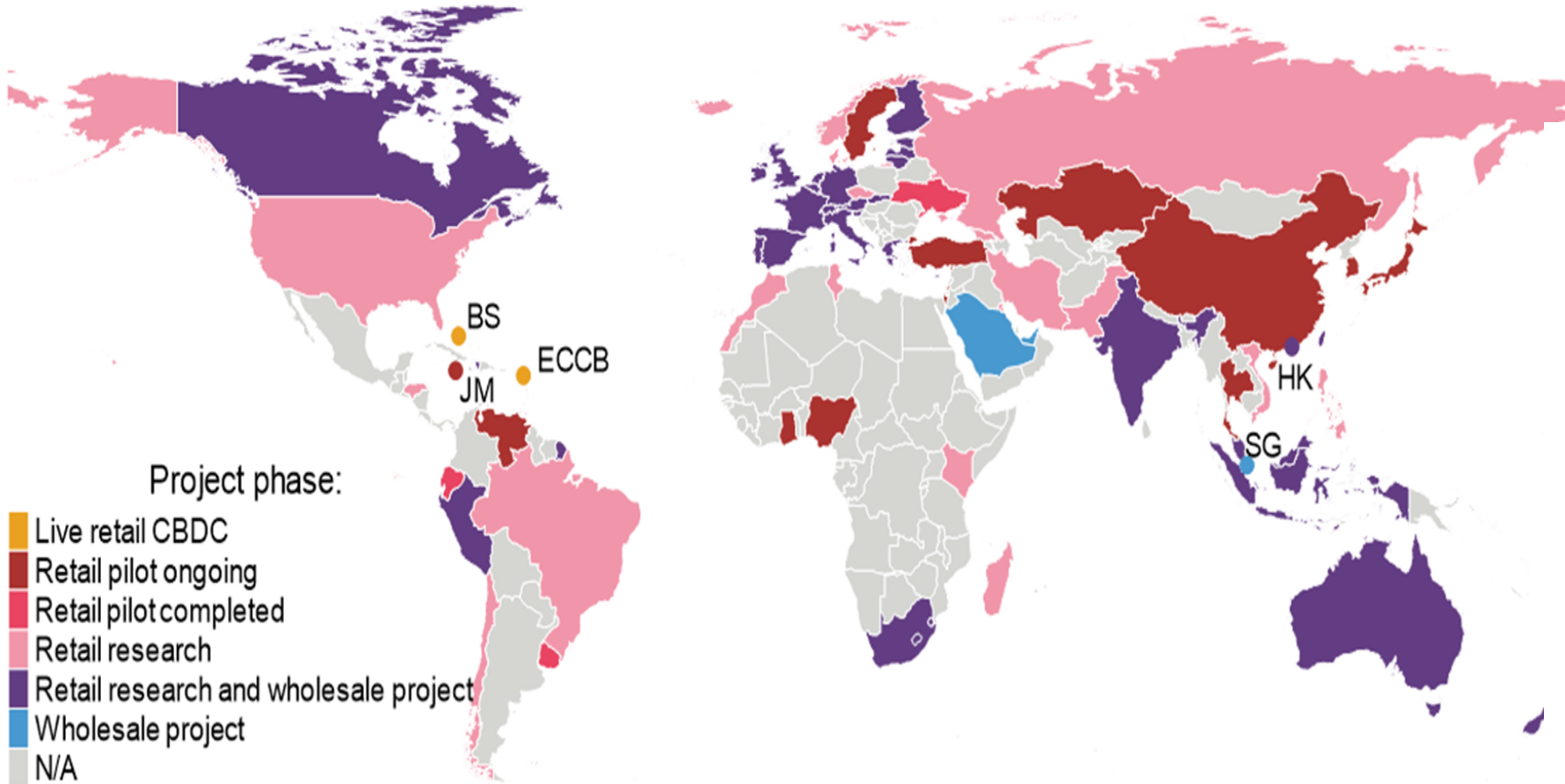
Ref #8

The "Rock of Randomness":
a physical oracle for securing data off the digital grid

Let's del deeper into the CBDC world –
what is going on and where is it going

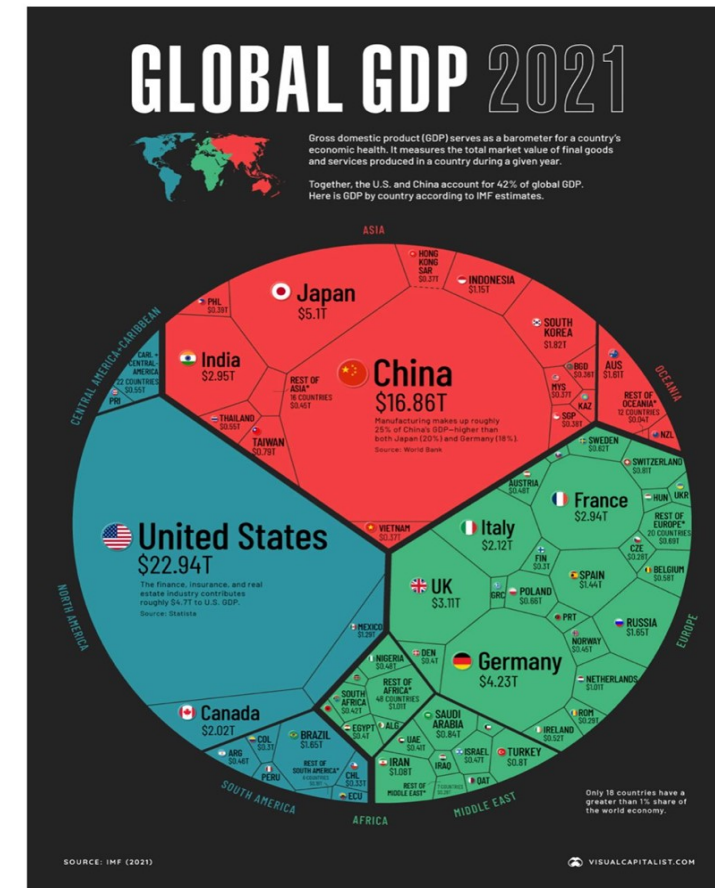
More than 110 countries have carried out CBDC-related work Retail and/or Wholesale to varying degrees

CBDC research and pilots around the world



BS = The Bahamas; ECCB = Eastern Caribbean Central Bank; HK = Hong Kong SAR; JM = Jamaica; SG = Singapore. The use of this map does not constitute, and should not be construed as constituting, an expression of a position by the BIS regarding the legal status of, or sovereignty of any territory or its authorities, to the delimitation of international frontiers and boundaries and/or to the name and designation of any territory, city or area.

Source: R Auer, G Cornelli and J Frost (2020), "Rise of the central bank digital currencies: drivers, approaches and technologies", *BIS working papers*, No 880, August.



Source: IMF 2021

THE RIGHT INFRASTRUCTURE
from which CBDC would be issued and circulated

FEATURES THAT CBDC SHOULD HAVE

CBDC essential doable principles

A strong criteria is required, that would be applied to the proposed CBDC architecture candidates, even if they are proposed by reputable vendors, or companies that are dedicated to digital currency solutions, or the prevailing currency technologies providers, that all wish to exploit their reputation by luring central banks to the digital money options they have expertise in.



CBDC essential doable principles (🌀)

Several of them are **Uncompromisable Requirements**, although unfortunately **MOST** of the retail CBDC pilots that were published does not meet them.

Principle #1:

Opportunity and not offensive

CBDC should significantly offer **improved performance** of the existing functionality on all facets of money, first of all to the people's benefit, and also for the monetary system, and should not represent a defensive reaction to private-sector innovations in money.

It should **rise slowly right next to the full operational tradition system**, and step by step there should be a migration of the operational capabilities from the existing method to the replacing one.

(🌀) for the purpose of full disclosure: BitMint's solutions meets ALL these criteria and principles.



CBDC essential doable principles (🌀) continuation

Principle #2:

In order for Cryptographic Threats to be strictly negligible, CBDC should be based on **Quantum-Cryptanalytic-Resistant architecture**, that offer all the versatility and power of crypto digital currencies, only without the unacceptable risk of currency collapse.

Including a parallel system coming in (like an electric generators in hospitals and other critical infrastructures that start working immediately at electricity shut down) , and on top of that, an in-built system for bouncing back fast and with minimum lasting damage in response to main system being cyber compromised.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.

CBDC essential doable principles (🌀) continuation

Principle #3:

The underlying foundation of a national digital money system should be **well-guarded Physical Embodiment** (Money-Rock), since the seeds of digital currency should not be based on digital bits, as bits can be hacked.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.



CBDC essential doable principles (🌀) continuation

Principle #4:

Being a comprehensive platform for cash, credit and **all financial instruments** to be fit into the same format, to enable **interoperability**, to best serve society.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.



CBDC essential doable principles (🌀) continuation

Principle #5:

Smooth integration with existing and **future local and global** payments channels and networks, whether DLTs or centralized, whether of central banks, commercial banks or current and future financial third parties, public and private.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.

CBDC essential doable principles (🌀) continuation

Principle #6:

One unified framework should enable **retail** as well as **wholesale** payments, while removing existing barriers, settlement risks and superfluous costs/fees, enabling general access.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.



CBDC essential doable principles (🌀) continuation

Principle #7:

Modular architecture, flexible, easy to expand and **support future replacement of specific modules** and easy integration of new innovative technologies.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.

CBDC essential doable principles (🌀) continuation

Principle #8:

Having **legal tender** status and satisfy the distinct properties of cash, including offering **Bilateral Payment Trust**, also between strangers.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.

CBDC essential doable principles (🌀) continuation

Principle #9:

Universal availability and interoperability without restrictions, meeting users' need for secure and **around-the-clock** payment finality capabilities, online and offline.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.



CBDC essential doable principles (🌀) continuation

Principle #10:

Payment continuity is indispensable for national level digital currency, and requires Sustained **Offline Payment** capability for conducting consecutive payments, not linked to any external system/network, providing finality of settlements in the offline mode, not limited in number and volume of transactions.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.



CBDC essential doable principles (🌀) continuation

Principle #11:

Splitable coins, Payable at any desired resolution
micro, nano payments, and continuous payments per service,
with payment finality, while splitting the coins will be
conducted autonomously by user's mobile or by IoT
device, not dependent on any ledger or another intermediary.

Applicable to money in motion and money at rest, creating a
trusted off-line payment regimen, enabling payment continuity
indefinitely from one trusted wallet/device to another.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.



CBDC essential doable principles (🌀) continuation

Principle #12:

Achieving widespread consumer merchant acceptance required great Superior in convenience, speed, efficiency, security, user experience and features than cash pay, mobile payments' Apps, for catering all consumers' changing needs, including under banked, unbanked, non-technology savvy, or those that don't possess smart phones.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.



CBDC essential doable principles (🌀) continuation

Principle #13:

Optionally, serving as Financial management tool

as well as improving the effectiveness of monetary policy transmission channels, while central banks can adapt more efficiently the monetary policy to changing situations, not being dependent on intermediaries to transmit policy decisions to individuals and companies.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.



CBDC essential doable principles (🌀) continuation

Principle #14:

Designed to be able to offer **interest rates**, as well as **positive and negative values** to the digital coins, to serve as a monetary policy tool, with flexibility for changing the policy from time to time, just by "a click of a button", as well as enabling new innovative digitalization technologies and regulations.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.



CBDC essential doable principles (🌀) continuation

Principle #15:

Flip ready from Transactional Privacy to Transactional Transparency. Controlled-Anonymity. Privacy of transactions is a critical aspect of freedom and demanded by the public and should be provided to law abiding citizens.

The basic design should enable the entire range for the choice of issuer, based on regulatory requirements, from fully anonymous and untraceable, until full traceability, and everything in between, including a semi-anonymous solution, and/or enabling digital coins to be passed around cash-like, while maintaining a complete record of chain of custody written on the coin itself (optional), to be read only when warranted by court order.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.



CBDC essential doable principles (🌀) continuation

Principle #16:

Purpose Driven - Tethered-Money

Design should enable an option of the unique Tethered-Money tool, that highlights a very promising possibility unique to identity-bearing digital money, insuring it is used as intended -- not abused, not wasted, while the terms of use or redemption are written on the coin itself (no need for a smart contract on a DLT).

The framework should enable the central bank easily provide liquidity directly to households even if they don't possess bank account, in what is known as “helicopter money”: With the tethering capabilities, this helicopter money could be "purpose-driven" and eliminate hoarding and misuse.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.



CBDC essential doable principles (🌀) continuation

Principle #17:

Creating Novel Payment Options. Serving Micro service economy.

The infrastructure should provide:

- (i) Real-Time Payments with or without privacy, large and small transactions;
- (ii) Pay-as-you-Go replacing the unfair subscription regimen where light users over pay and heavy users underpay;
- (iii) Micro-Services Economy: IoT (Internet of Things) devices pay each other autonomously.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.



CBDC essential doable principles (🌀) continuation

Principle #18:

Payment continuity anytime, anywhere for ALL,
including creating a trusted off-line payment regimen
even as long as the Internet is compromised,
with Finality of settlements.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.

CBDC essential doable principles (🌀) continuation

Principle #19:

The framework should improve overall costs of issuing money and executing payments, while **reducing ecological footprint** of the monetary and payment systems.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.

CBDC essential doable principles (🌀) continuation

Principle #20:

Fair and Efficient Taxation.

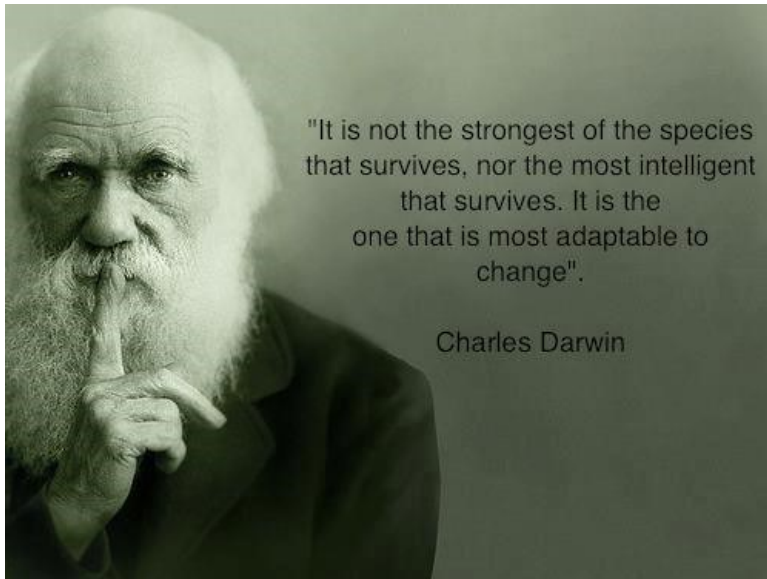
Taxation and funding of governments must be evasion-resistant. Well-designed CBDC can lead to fair and efficient taxation.

Optional, but designed as a prime feature: taxing CBDC money in strict proportion to wealth, even without identifying the tax payer, as an add-on, or as a simplifying replacement for income tax.

(🌀) for the purpose of full disclosure: BitMint meets ALL these criteria and principles.



These are the essentials that were invented and developed already, although being ignored by those that prefer to remain in their 'comfort zone'.



If YOU are curious, innovative, open minded, and wish to leave a mark, You'll find what and how to contribute to these challenges and take them further.



Even before you graduate, start thinking on the overall scope and challenges and you will find it fascinating.

Summary



Its about time for leading to the era of money innovation.

I encourage you to jump on our bandwagon that leads to a new global financial landscape.

Privacy for the powerful and same for the powerless;

Security for the sophisticated class, as well as to the innocent class.

This is part of the Quantum Smart Money vision, which not only introduces a new level of quantum security, but enables much broader and more diverse functionality than any crypto-minted digital money solution.

This prospective empowerment of the global individual citizen comes about just when the vision of Web 3.0 is picking up steam.

Perfect timing.



Digital innovation must rely on basic values.

Users' centric solutions, expressing usability and purpose, are in place.

Digital currencies may not only be reshaping the world of finance, but they will also be driving the emergence of a fair and inclusive global digital finance with increasing spillover effects on many areas of sustainable development across the world.

Specific use cases were created, are all-encompassing for individuals, communities, organizations, industries and governments, taking into consideration security, privacy, technology, developing financial, legal and regulatory models incorporating social aspects.



Beyond the hype....



Are cryptocurrencies ready for Mainstream Business?

Apart from **functional/features/capabilities, speed, user experience limitations** characterizing most leading crypto-based tokens and assets,

There are **four main hurdles/challenges** that should be mitigated, before users (individuals, merchants, organizations, industry, institutes) will be lured to widely use crypto-currencies, stable coins and CBDC for daily transactions:

- (1) To ensure **TRUST** you must ensure that the system works as it was designed and that its integrity remains intact, even if the smartest hacker or quantum computer tries to compromise it.
- (2) Safeguarding **PRIVACY**.
- (3) Re-establishing the **SOCIAL BOND** between two strangers participating in a monetary exchange.
- (4) **PAYMENT CONTINUTITY** should be maintained through periods of failing or disrupted Internet, enabling **OFFLINE PAYMENTS** with finality, cash like, with no connectivity and no mobile phone.

Present:



Web2.0
Crypto1.0



Cryptography

Blockchain

Future:



Web3.0
Crypto2.0



Quantum Randomness



LeVeL: *The Bitcoin Innovation Reassembled*

- Better Privacy
- Quantum Safe
- Accommodates Everyone
- Enables public-private partnerships
- CM = Centrally Minted
- DM = Decentralized Market distribution
- Building Bilateral Payment Trust that is non-existent today, except for discrete passing of cash.

Conclusion (1)

Issuers of digital currencies, whether central banks or public or private issuers, should realize the vulnerabilities of the public/private key architecture, corresponding with the BIS and WEF latest documents,

and to come forth with - -

a Centralized-minted, Decentralized-distributed, Quantum safe, stable, unbreachable anonymity, Socially Responsible Privacy, designed to discriminate between ordinary law-abiding monetary privacy, and criminal and abusive exploitation thereto.

Conclusion (2)

to central bankers the message is even more crucial:

Failure to implement a robust Quantum-Resilient strategy from day one,

NOT as a layer or complexity to be added,

Will not only Compromise citizens data and funds,

but will put the entire national stability at risk.

CBDC architecture * must be

comprehensive and consider the full spectrum of risks,

enabling the full spectrum of features and capabilities,

act as a social lifeline,

being universally desirable and inclusive.

Note: CBDC, if well designed, has so much to offer first of all to the people and also for the monetary system, and should not represent a defensive reaction to private-sector innovations in money. CBDC should significantly improve performance of the existing functionality.



*LeVeL

Closing remark

Money rising to become the most powerful agent for social justice and equitable global prosperity.

Let's do it right!

Stable, Versatile, Simple.

We are working on transforming money towards becoming a tool for a better tomorrow.



Further reading

References

- **Ref. 1:** The book "Tethered Money - managing digital money transactions" (Kindle Ready) elaborates on the possibilities of a cyber-currency that incorporates value and identity as one.
https://www.amazon.com/gp/product/B012FR7I3W/ref=dbs_a_def_rwt_bibl_vppi_i



Ref. 2: Chapter 20 in the "Handbook of Digital Currency", David Lee Kuo Chuen, editor, Elsevier Academic Press, discussing solutions for a global currency, and presenting the InterMint solution to ensure interoperability of CBDC Mints issued by different central banks or other issuers.
<https://www.elsevier.com/books/handbook-of-digital-currency/lee-kuo-chuen/978-0-12-802117-0>

Ref. 3: 2020 IEEE International IOT, Electronics and Mechatronics Conference
<https://ieeexplore.ieee.org/document/9216456>

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



Ref. 4: Oxford Journal of Legal Studies acknowledged the security of quantum digital money, Pages 4, 8, 22-25.
<https://academic.oup.com/ojls/advance-article/doi/10.1093/ojls/ggab019/6284236?guestAccessKey=b48e2e2d-5e5d-44fb-b809-1b6036455210>

Ref. 5: Quantum vs. Crypto: The Battle Royal
<https://lnkd.in/eRA5JHXT>

Ref. 6: World Economic Forum [WEF]: Randomness: The Fix for Today's Broken Security
<https://www.weforum.org/agenda/2017/11/what-a-100-year-old-idea-can-teach-us-about-cybersecurity>

Ref. 7: WEF white paper: The Role of the Public Sector and Public-Private Cooperation in the Era of Digital Currency Growth
<https://www.weforum.org/reports/digital-currency-governance-consortium-white-paper-series/public-private-cooperation> Chapter 8

Ref. 8: MRS [Material Research Society] "Rock of Randomness": a physical oracle for securing data off the digital grid <https://lnkd.in/eK573sja>





This is what we do
at BitMint....

**”The best way to predict the future
is to invent it”**

Alan Kay

And this is what I encourage YOU to do when you pave your way in the world.

Thank you!



Don't limit your imagination for the future with
your current ability and current thinking