DCA

Digitized **C**urrency **A**rchitecture

Exploring practical level applications of Digital Currency Claim-Checks and Tethered Money

BitMint workable solutions with well-defined methodology For retail online & offline, wholesale and cross-border Digital Currency Ready to Deploy with no tradeoffs

ESTABLISHMENT:

- BitMint digital currency solutions fulfills the vision of restoring the old way of payment with Hi-Tech Cash, that is distributed directly to and capable of being owned held and used directly by the general public, enabling instantaneous, final, direct, peer to-peer transactions, with same privacy respecting features of physical cash, for the law-abiding users.
- BitMint specialized in research and developing innovative solutions (more than 30 granted patents) and implementation of digital fiat currency bearer instruments, stored and exchanged online and offline with instant settlement finality, supporting technology vendors since 2011, and working directly with central banks since 2013, to characterize, define, build and test under tough real world conditions general purpose CBDC solutions, proven to be interoperable with existing financial ecosystem.
- BitMint implements digital claim checks of fiat currencies and/or assets, that are centrally-minted and decentralized-exchanged and acts as a de-facto transactable currency, being redemption-ready with a fixed redemption value, while not being vulnerable to a crack in a singular mathematical algorithm (the elliptic curve), offering ultimate privacy to all traders, but renders a claim check unredeemable per a competent court order.
- BitMint digital claim check protocol is most scalable, but is ready to serve small and large payment regimen, locally or remotely, and may be established also on very small scale because it does not require a minimum count of peers' approval, with ready and fast scalability.
- BitMint developed Universal Payment Solution [UPS] that supports a public ledger based easy payment regimen among phones and other computing devices -- at quantum grade security, with cash-like privacy; complemented with robust offline payment capability, and with Internet of Things device-to-device payment. The BitMint UPS is metaverse friendly.
- BitMint UPS is ready to serve small and large payment regimen, locally or remotely. BitMint simply transformed the pre-cyber cash to post-cyber cash.
- Hard Wallet: BitMint provides a low-cost device design, which is a closed enclosure containing digital currency or digital claim-checks (whether minted

 utility@BitMint.com

by BitMint or by any other vendor) and a payment software. One HardWallet is paid from another HardWallet, thereby creating a trusted off-line payment regimen for as long as the Internet and electricity is compromised, up to at least six-consecutive-months period with no need to recharge electricity to the HardWallet. The payer's HardWallet authentication by payee's HardWallet and the payment are executed in a very easy and fast process that does not require technical capabilities, apart from indicating the value to be transferred, while achieving payment finality in the offline mode. The secure software erases all money paid out to prevent double spending, and the HardWallet quantum-grade security protects against all possible attacks. Any tampering attempt of the HardWallet will fail and erase all the e-cash tokens stored in the Wallet.

PROVEN EXPERIENCE:

- BitMint promotes and facilitates the development and deployment of national digital currencies or digital claim-checks for use by the general public that as much as possible replicates and preserves the privacy and minimal transactional data-generating properties such as coins and banknotes to the greatest extent technically, legally and practically possible, as protecting privacy is key for maintaining public trust. All that while maintaining quantum-grade cyber-security, resilience and sustainability.

- **BitMint built and tested solutions in collaboration with a central and commercial bank, fulfills the following REQUIREMENTS**:

(1) Being payable to bearer ;

(2) Being a legal tender, to ensure public access and full usability, including ability to pay by a click of a button by anyone, anywhere, to be accepted by all merchants, both in physical stores and online, as well as person-to-person payments and machine-to-machine automation payments .

(3) Capable of being distributed directly to, and capable of being owned, held, and used directly by, the general public; stored on-chain or off-chain in users' device (e.g., mobile phone, tablet, PC or a physical Wallet), granting users control on their privacy, while minimizing the ability and incentive of illicit activities, enabling moving the digital currency freely with free liquidity 24/7.

(4) Being used for instantaneous, final, direct, peer-to-peer cash like transactions even with no bank account, using a protocol to detect counterfeits and prevent double spending, having all features of physical cash, with no trace of value and identities of payer and payee, securing cash-like payment, that is, a payor and a payee able to execute a payment such that none besides these two is in the know, reconciling with the public interest in countering illegal activities.

(5) To better serve users' privacy only a warrant enables exposing transactions history through chain of custody written on the token and/or via the flow of changed private keys that are connected to the token flow between users .

(6) Presents an innovative payment solution for the Internet of Things (IoT) as part of the industry 4.0; this era requires Machine-to-machine payments (M2M), such as releasing payment for goods received upon arrival without the need for intermediaries; connected devices to do business with one another as autonomous legal agents, such as automatic recharging of cars, automatic order of supply for home or for manufacturing, toll payments, logistical services, deliveries etc. Overcoming restrictions that DLTs, blockchain like, may impose on smooth functionality:

- Coins are splitable without a ledger to enable real time auto payment, continuously – per time or per supply, in any resolution;

- Terms of use (similar to smart contracts on the blockchain or to programmable payments) written on the coin itself.

IMPACT ON THE FINANCIAL SYSTEM

(7) BitMint's digital claim checks are convertible with central bank money on a one-to-one basis, being fully interchangeable yet distinguishable from other forms of electronic currency, and inter-operable with commercial banks and other financial institution and payment provider systems, and generally accepted payments standards and network protocols, as well as other public payments programs.

(8) Systemic Liquidity: The tested BitMint solution does not disrupt or substantially impact the general availability or cost of liquidity for depository institutions, credit unions, or community development financial institutions, or their capacity to extend credit and other financial services to underserved populations.

TECHNOLOGY DESIGN

(9) BitMint fulfills the requirement of the inviting central bank for not deploying blockchain and alike in the minting process, due to its potential impact on resilience, sustainability, speed, as well as usability and macroeconomic and microeconomics aspects.

(10) In parallel, BitMint developed a Universal Payment Solution that supports a public ledger based easy payment regimen among phones and other computing devices -- at quantum grade security, with cash-like privacy; complemented with robust offline payment capability, and with Internet of Things device-to-device payment. The BitMint UPS is metaverse friendly.

(11) The technology that underlines the invited and tested BitMint digital currency is people oriented, Quantum-Cyber resilient, Centralized-Minted [CM] Decentralized-Exchanged [DEX], being Universally Accepted, while achieving:

(i) financial inclusion

(ii) privacy controlled by users

(iii) not being a shelter for illicit activities.

(12) BitMint fulfills the challenge of creating a digital currency that is not dependent on a network of validators for making a payment, although dependent on decentralized Math digital coin, while replacing the old cash with Hi-Tech cash, with the same privacy respecting features of physical cash for the law-abiding users.

PROGRAMMABILITY:

We have to distinguish between programing the transaction (programmable payment) and programmable money. BitMint supports programmable money fulfilled by the Tethered-Money tool, which defines the usage of a specific token or a split of a token, without human intervention to achieve commercial automation.

The BitMint solution enables 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 token itself.

The BitMint framework enables providing liquidity directly to households even if they don't possess a 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.

SECURITY:

The main security concerns that BitMint resolve, relate not only to digital currencies, but to the entire financial and payment protocols, including bank transfers, that are totally dependent on prime cryptography. According to the World Economic Forum, the BIS and the IMF this cryptography is vulnerable; QUOTE from IMF [Fall 2021]: "*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*". BitMint's tested solution deals with this threat by offering quantum-grade

mathematical proven solutions, not being dependent on eroding cryptography that is already recognized to be vulnerable.

PRIVACY:

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.

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

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.

Private bilateral Payment is the coming revolution - Restoring the old way of payment.

BitMint introduces the LeVeL-Paying-Field, enabling Private Bilateral Payment that is homomorphic with cash payment: strictly bilateral. Privacy will reign, benefitting the law-abiding citizens. The Hi-Tec sophistication in BitMint's cyber cash will deny criminals from abusing this precious privacy.

INTEROPERABILITY:

Currency solutions hinged on Blockchain and alike are limited in throughput by the need to spread each transaction to a large number of peers. Legacy money solutions are limited by the singularity of the authentication entity. Currently the best throughput is about a couple of thousand of transactions per second. BitMint developed a well-defined methodology to enable an open number of mints to serve the public. All these mints will be connected via an InterMint, that is a network of mints constituted with a public protocol, so any entity can join. This will promote innovation and competition.

STABLECOINS:

BitMint presents a stablecoin solution, with comparative advantages over cryptocurrencies, in terms of privacy, stability, decentralization and solvency. BitMint's stable coins are centrally minted in perfect liquidity (digital claim checks), and decentralized distributed and traded, with a validation mechanism that is not dependent of network of validator nodes. The mint is in charge of the delivery of the coin to trader

1 (the purchaser), and more importantly, in charge of the redemption process -- for the other referential money. Since these stablecoins are pegged 1:1 on a fiat currency, they can coexist with any other currency. They will be passed around from trader to trader. BitMint stablecoins are splitable: a coin will be split as needed, and eventually, it will be returned to the mint for redemption. Trade with such stablecoins will not impact the money supply. They will amount to equivalent forms of liquidity. They should not have a worrisome economic impact. The public will start to pay with these stablecoins, since they offer several advantages, say speed, privacy, instant settlement etc.

CROSS BORDER PAYMENTS:

The BitMint digital currency architecture that was tested by a central bank was designed to serve as retail as well as wholesale and cross border solution, to enable internationalization of the national digital currency.

The BitMint digital coin may be set up to explicitly identify its full chain of custody, so that authorities can trace the whereabouts of the coin since it was minted. This coin-loaded history should fit the accounting books of both the payors and the payees, thereby creating a Tri-Log Accounting, very resilient against fraud and abuse.

ACCOUNTABILITY:

The hallmark of financial institutions throughout the ages was accountability. A public entity stood behind the minted coins, and underwrote all financial instruments. The powers that be at times abused this power, and gave impetus to Bitcoin and its variants that claim to drop the need for trusting a human organization. What Bitcoin et ell achieved is to hide the power that governs the currency. They have no address. 0.01% of Bitcoin traders (who are they?) own almost one third of its wealth. Mining is almost fully restricted to a few hashing powerhouses.

Here is where BitMint distinguishes itself: it utilizes the cryptographic innovations laid out by Bitcoin, uses them for all their remarkable benefit — but at the same time restoring public accountability. Which means that in a democratic society the people are in control.

CONCLUSIONS & RECOMMENDATIONS:

BitMint fulfills the main challenge in front of digital currencies issuers, which is to exploit cyber space to elevate money into a more powerful tool to further benefit society. BitMint projects payment freedom from anywhere to anyplace, enables purpose-targeted payments, effective use of credit, while fiercely maintaining payor-

payee privacy. BitMint serves global financial institutions with its newly designed financial language. BitMint fits into the Internet of Things payment regimen, and BitMint does all that with full public accountability.

BitMint realizes that 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.

BitMint Digital currency architecture fulfills another main challenge of digital currencies' issuer, adopting a comprehensive universal system that will accommodate the entire range of users and features and capabilities, to benefit the society as a whole, while considering the full spectrum of risks, being universally desirable and inclusive.

For that purpose, BitMint developed the Universal Money Language [UML], which is a financial language designed to express all the financial instruments in a format which exploits cryptography, first as a security and a vault, and second as a means to manage, route and use financial instruments in a more refined and more specified way. The BitMint financial language keeps monetary accounting and reporting intact, it simply writes the values and the description of these instruments in a format that allows cryptography to serve as a financial "joy stick."

The BitMint financial language is offered to financial institutions, private and public, as well as central banks, on an international basis.

utility@BitMint.com