



RESPONDING TO:

Digital cash in New Zealand

Consultation Paper

1

Submitted by:

BitMint AI-Powered Cyber-Innovation Hub

Contact person:

Amnon Samid

Redacted under 9(2)(a)

25 July 2024

<https://www.bitmintcash.com/>

BitMint's team is building a cohesive innovative ecosystem to democratize access to money and finance and to contribute to economic and financial inclusion by equalizing and connecting people, and creating trust between strangers. Our team is busy in developing new inventions, and is working on creating knowledge platforms to inspire and design the digital money of the future, as part of the battle on human privacy and human dignity in cyber space, which is the battle royal of the evolving century, while being resilient against mis profiling by AI and resistant against quantum computing attacks.





Future of Money Team,

The Reserve Bank of New Zealand – Te Pūtea Matua

Dear colleagues,

We enjoyed reading your **Digital cash in New Zealand [NZ], Consultation Paper**. It's really a very comprehensive analysis, and we applaud you for exploring and actively debating on the issuance of digital version, cash-like, of the New Zealand dollar (NZD), and for such a deep and wide study and analysis that you conducted.

We argue that Digital Cash – if well designed – can support a resilient financial system, that will better serve and protect the NZ financial and monetary stability in the years to come, also against looming threats of AI-Cryptanalysis as well as quantum computers.

It can and should be designed not only to benefit everyone in the country who makes payments, but to keep the NZ at the leading edge of payments innovation.

NZ Exchange Settlement Account System is currently executing digital payments, but digital cash that is value based (a.k.a. token based) can offer more features and added values for the benefit of citizens and merchants.

Currently, physical cash in banknotes and coins is not just the only type of central bank money available to everyone to pay for things, but it is the only manner to enable bilateral payments between parties.

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 the coming revolution, restoring the old way of payment.

We'll be more than happy to introduce to you the **LeVeL-Paying-Field**, that 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.



3

With the LeVeL-Paying-Field the Reserve Bank controls the public ledger (not DLT) that enables two parties to autonomously authenticate and transact with digital cash, without intermediaries, nor a cumbersome consensus mechanism.

The Reserve Bank will be able to see the transactions, but not the value, and also to put a threshold on anonymous transactions, to enable full anonymity of traders up to this threshold (acting autonomously). The Reserve Bank can mandate when ID of payer and/or of payee is required, and has also the power to suspend or “freeze” (suspend) a coin, in case of suspicious transactions, as well as to de-anonymize user/s and coin chain of custody by court order.

The LeVeL-Paying-Field is a universal platform that fits central bank digital cash, as well as stablecoin and asset tokenization, as long as the tokens has unique value and unique identity, like serial number and value of banknotes.

In that sense, it will boost competition and endorse innovation in the payment landscape. It enjoys all benedicts and attributes of decentralised finance and DLTs, without their hurdles and inefficiencies.

Apart from Digital Cash in the form of CBDC, NZD could be issued by the Reserve Bank in a form of digital-claim-check, that is always redeemable against cash, as well as convertible banknotes that could be uploaded to citizens' device and become digital, as well as physical hybrid coins, that contain inside digital cash – it will be pretty much easy to switch between the digital and physical cash as well as bank deposits.





From Your
Wallet
to the
Internet

BitMint®
bitbit Money



Uploadable Banknotes



It will well serve the Reserve Bank in offering citizens and, merchants the benefits of digital cash, while protecting the role of physical cash in New Zealand.

Digital cash could also boost competition in New Zealand's payments landscape by supporting new types of money and payments services from the private sector. New Zealanders will have the choice of who they use to access their digital cash services.

To conclude this part:

The three main attributes of money are:

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

Overlooked are other attributes:

- Money creates a bond between two strangers
- Money is a social lifeline
- Money is universally desirable.

Money could become a powerful agent for social justice and equitable global prosperity. We have to make sure that we do it right! Stable, Versatile, Simple.

We are working on transforming money towards becoming a tool for a better tomorrow. We'll be more than happy to share from our vast and long experience in this field. For now, please find hereunder brief response to your questions.

We are ready for your call to contribute to the brainstorming process, and more.

With much appreciation.

Amnon Samid

Managing Director



*The following is a brief response to the questions at the consultation paper.
We will be happy to elaborate on each of the topics and others.*

Purpose

1. **Do you have any feedback on the objectives for the digital cash to:**
 - i. **ensure that central money is available to New Zealanders and allow it to be used digitally.**

- Indeed. The main idea of digital cash is to fulfill the vision of restoring the old way of payment with cash and to fit it for the digital age, while enabling bilateral payment that is non-existent today except for discrete passing of cash.

* Digital money can flourish and could be a disaster. It's in the hand of decision makers, starting by choosing the right technology.

- ii. **contribute to the innovation, efficiency and resilience of New Zealand's money and payments landscape.**
- The main challenge is enabling two parties, human or devices, to trade cash-like with no intermediaries and not dependent on a network of validators.
- Second challenge is protecting privacy. It is critical for digital cash in order to obtain public trust, and prevent mis profiling by AI.
- Third challenge is maintaining quantum-grade cyber-security, resiliency and sustainability

5

2. **Do you have any feedback on the digital cash principles of Uniform, Universal, Private, Reliable, and Orderly?**

- The principles are most appropriate. We would recommend a more detailed parameters for obtaining a more effective, reliable and creative digital cash protocol, that is:

- scalable, very efficient and user friendly (not dependent on intermediaries);

- enables more use cases and functionalities and having less environmental foot print – both comparing to ALL current payment rails;

- guarantying much better security, even against the looming quantum threat; and





- enhanced privacy, that is guaranteed by the technology, to prevent data mining and abusing purchase behavior, with 'managed anonymity' (from 100% to zero and anything in between), while not being an enabler for illicit activities.

3. *What are your biggest concerns with digital cash? What design changes, if any, could address your concerns?*

- There is no excuse to pick a digital cash platform to be of reliable long-term service, which has no good answer to the ticking bomb of the **quantum threat** and to the new **AI-cryptanalytics threat**.
- Please note that protecting digital cash against the quantum threat and against the AI-cryptanalysis threat by adding more layers of complexity 'on the go'...is just an illusion!
- **Once a digital-coin framework is put in place, it will be too late to uproot it!**
- We strongly recommend that the Reserve Bank will consider sophisticated technologies that are superior to crypto-based solutions, while cybersecurity up to quantum level, and users' privacy should be the primary concern.
- It is also imperative that the digital cash meets strict **data protection** requirements and adheres to the principle that users retain their data sovereignty.
- You have to design the digital cash to be prepared to mitigate and exploit measures to defend and be ready to AI's risky aspects, such as:
 - AI to break cipher being used in payment rails
 - AI can exploit such invasive privacy violations to learn about us what we wish to keep to ourselves.
 - Exposing payments behavior could be exploited by AI to mis-profiling people.
 - Genetic algorithms build brain-like inference networks that draw clear conclusions from messy payment and expenditure data.
 - Suddenly, **people will get turned down for loans and jobs** that had appeared to be a sure bet. But, unlike the **credit scores** or **social score** of today, where errors can be **complained about and rectified**, - the AI





data-to-conclusion process is not understood by humans and - cannot be appealed by the victims.

- As to use of digital cash in **offline** mode: If you wish to have finality of payment, with no risk of double spending and no risk of **counterfeit** - you **CANNOT** trust ANY cryptographic technique!
- In online payments with digital cash: **Relying on a single key and a single algorithm** (usually, ECC, that most platforms rely on) is like a “stationary target” for cracking. Any weakness of the key can be exploited in any transaction.
- These are the main concerns that - at a first glance - seem **NOT** to be currently well addressed.

How to mitigate? (Hereunder only in bullets point. Elaboration is needed):

- You need to deploy **Quantum-Defensive Strategy [QDS]** for the entire cycle - from **issuing** through **trading** and **redeeming** of digital cash.
- **Cryptographic agility** needs to be embedded into central bank digital currency systems to defend against quantum cyberattacks.
- For mitigating the single algorithm risk - you can make random **mutations** of the key and of the challenge algorithm.
- You need a protocol that is **pattern-less**, enables traders to adjust their privacy, not relying on a static private key, not exposing transaction value, but only coin id, while enabling the authorities to suspend a coin or extract trader’s id and/or chain of custody under court order.
- If you wish to trade (execute payments) with digital cash in fully offline mode - with no Internet at all - (also not for POS) - you need a **physical procedure (not cryptographic!)**, that will authenticate a physical wallet (HardWallet, or HW) that stores the digital cash, and you have to make sure that such a HW is never ever connected to the network.

7



Benefits of digital cash

4. Do you think digital cash can enable longer-term innovation for New Zealanders? And what innovative features in digital cash would you like to see?

Sure. Enabling longer-term innovation should and can be one of the goals of digital cash.

Historically, whenever payment became easier and smoother, commerce flourished and civilization jolted up. It happened when barter was replaced by primitive money, when precious metal became standard money, and then again when pre-minted coins replaced scales.

We have seen the medieval period end and the Renaissance bud up when the first promissory notes became popular and introduced the notion of paper money.

We face an opportunity to cure a fundamental deficiency experienced by money when most of it became computer handled. Money then lost its identity, which was there when money was physical, and it shrunk to be a number only.

This opportunity opened up after the seminal paper of **Nakamoto** (2008), although **Chaum** brought the buds of the revolution already in 1982, and **Samid** filed the first comprehensive digital currency patent in 2007; - it introduced a new financial language that restores identity to digital coins and thereby puts them at par with physical coins as to the inherent advantages held by banknotes and metal coins, while offering cyber-unique advantages for being subject to cryptographic processing.

Hereunder a few examples of innovative features, enabling disruptive use cases and functionalities :

- Designing the digital cash to enable trading with it on a public ledger without exposing to the public the coin value (only the identity, which is separate from the coin value .
- Designing the digital cash to enable traders (or a device) to split each coin to any desired resolution without the network. Each split will have a unique id after they split by the traders, with no need for network connection. This VERY UNIQUE CAPABILITY enables several interesting use cases:



- First of all it is desired for payment in offline mode;
- Second, it enables continuous payments per time or service:

“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 he/she pays attention to you ;

hop into a taxi and pay as you ride for as long as you ride; pay real time with no subscription for charging your electrical vehicle; pay for reading one article in a eNewspaper or per exact time of reading; pay for streaming - as long as you are enjoying the movie, and you stop watching - payment ceased automatically. etc .

** All the above - - without post-accounting, with no next-month-invoice, with no subscription; and with anonymity to boot (optional).

- Demonstrating Purpose-driven money (to avoid misuse of funds), which enables to attach logical rules to the digital cash, such as time-related, or event-driven, or rules of any logical relationship.

- An autonomous public settlement/transaction protocol with digital cash, that is almost not burning the bank’s server, while still the bank not losing control of where the money moves. Verification, Split, Transaction - are all done by the users’ phone.

- A public ledger that is decentralized with no intermediators; not dependent on peer review or validators, and that provides quantum resistant instant settlement with no risk to payee or issuer and with no tradeoffs.

5. Do you think digital cash can improve payment’s reliability in New Zealand? And what reliability features would you like to see?

Reliability and Trust are combined and require Continuity of payment, with no risk or double spending and of bad actors distributing counterfeit digital cash.

The digital cash, if well designed, can grasp the fascinating opportunity to democratize access to finance and to contribute to economic and financial inclusion by equalizing and connecting people, and creating trust between strangers, embracing interoperability, advocating digital





innovation in sovereign money and in non-sovereign digital currency networks.

The digital cash is supposed to be one of the most critical components of a national payment system. As such it **MUST** be sustainable and resilient, also against the looming threats of AI and Quantum attacks. (we assume that prevailing payment systems in NZ are not (yet?) immune against AI mis profiling and against future quantum attacks).

Interoperability is also essential for maintaining reliability. In order to avoid furthering payment system fragmentation, it is important to ensure its interoperability with legacy and new payment systems as well as Fast payment systems (FPS) .

Digital cash may become a critical component not just in the context of NZ national payment systems but also in the context of cross-border payment infrastructures.

6. How can digital cash support digital financial inclusion? And what features (technical, governance, standards, etc.) are required to support digital inclusion and financial inclusion?

10

Digital cash, if well designed, can open a fascinating opportunity to equalizing and connecting people, even vulnerable groups such as physically remote populations, old or sick people, non-savvy technology, marginalized communities, and SMEs and creating trust between strangers, embracing interoperability and advocating digital innovation that will increase the overall value and appeal of digital initiatives.

For enhancing financial inclusion, the digital cash should enable secure and instant exchange of value, providing seamless user-friendly payment experience to consumers and merchants, enabling ALL market participants to execute frictionless, precise and real-time transfer of value, like experience with banknotes and coins, enabling the receiver to use the funds immediately.

It requires also for the digital cash to be always accessible.

The above is doable, if well designed, from day one. It requires a financial language that restores identity to digital cash and thereby puts them at par with physical banknotes as to the inherent advantages held by banknotes and metal coins, while offering cyber-unique advantages for being subject to cryptographic processing.





7. *What problem could digital cash help you or your organisation address and what benefit could it bring?*

We are supporting decision makers in digitalizing a country's governance and economy and delivering the promises of a secure (up to being quantum-safe) and most efficient digital transformation in terms of security, social, economic and environmental impacts, geared toward social accountability and financial inclusion.

We can offer the next generation of digital cash, and invaluable guidance for the Reserve Bank, based on vast knowledge and experience that we have acquired in the last 17 years, including from our practical experiments, and to foster and to contribute to your further exploration process and investigation on this topic.

The benefits we expect, include among others:

- Cash-like privacy
- Adjustable anonymity
- Issuer not losing control on where the money moves
- Not being enabler for illicit activities
- Enables to transact with digital cash without burning the bank servers
- Faster transactions
- Higher efficiency
- Less energy consumption (less computing power)
- Better security (up to being quantum resilient)
- Broader adoption and better circulation
- Useful functionalities and use cases, that are impossible today with all prevailing payments systems, including crypto-based, card-based, etc.

In the CBDC project that we conducted with a central bank and a commercial bank, we demonstrated coexistence, interoperability and harmonization of CBDC with the legacy systems.





Future stages of work will continue to refine the design details of digital cash and its ecosystem, including governance arrangements. To assist us we would like feedback from industry or possible partners.

8. Do you have feedback on the design models and the Reserve Bank's preferred approach?

For addressing people's fear of digital cash issued by the Reserve Bank, being used for surveillance and control or harassment purposes, privacy must be guaranteed by technology. Citizens may not trust the current solutions.

Deploying zero-trust architecture for national currency is too risky. Trust can be shifted not removed. Zero Trust systems place trust in an abstract construct which is too sophisticated for most players to fathom. And hence when the trust place is infected and is being violated, the players have no clue.

The solution for digital cash is to place trust in a trust-bearer from which you can remove the trust at will. To do this one has to practice network dynamics in a configuration where trust-claimants compete, and are motivated to stay trust-worthy lest they lose their users.

The digital cash CAN and SHOULD enable private bilateral payments, which will be MORE convenient for users, compared to any other payment rail, without being an enabler for illegal activities.

Furthermore: Digital cash should comprise on quantum-resistant bits, designed to withstand the most aggressive hackers' attacks, not being affected by quantum computers nor by AI-Cryptanalysis. A feasible solution was demonstrated and successfully tested in a real retail digital currency project.

Online Transaction protocol should NOT rely on a fixed public/private key algorithm and fixed OWF, as it turns it into a resting target for advanced cryptanalysis.

It is advisable to design the digital cash protocol to enable most of the functionalities to be conducted by users' device (mobile phone) instead by issuer server or ledger.

Cutting out network of validators and intermediators, will enable autonomous validation/transaction by payer/payee, ready for enormous number of secure, legal and genuine transactions per second.



9. **What role might your firm or organisation take in the digital cash ecosystem, and what support would you require from the Reserve Bank?**
I.e.

i. **What products and services would you build off the options? What design functionality would you need to support you?**

BitMint's team is dedicated to leading the charge into the post-digital currencies' era with our unparalleled expertise (17+ years into this challenge) and innovative state-of-the-art solutions for the benefit both of people and governments.

We are at the leading edge of the technology, that would integrate seamlessly into the evolving payments infrastructure and be fully interoperable with existing payment rail.

We are willing to join your exploration of privacy-preserving designs for digital cash, by demonstrating the merits of a novel privacy-enhancing technology (The LeVeL-Paying-Field) that could be brought into the design of the digital cash form of NZD.

Having privacy-by-design, technically guaranteed, that can be verified by anybody, without direct oversight of intermediaries or the bank on individual transactions, while being compliance with AML/CFT, implemented into the design, is of utmost importance for ultimately establish trust.

One of the universal platforms that we developed, seem to be a perfect fit for the digital cash narrative, as described in the consultation paper:

The LeVeL-Paying-Field

It is a centrally governed distributed public ledger (not a DLT, although achieving DLTs advantages without its limitations),

which is hinged on the fundamental experience of payor passing a transactable instrument of value to a payee,

with no intermediaries, within a community-sanctioned protocol,

with adjustable privacy guaranteed by technology ,

consistent with oversight accountability, and law enforcement,





as well as enabling scalability and preserving highest security challenges, up to being quantum-resistant.

While the LeVeL privacy is robust, It has a built-in route for law enforcement to catch and prevent criminal activity.

The LeVeL solution is universal and programmable, applies to exchanging any financial instrument (with value and identity), locally and cross border, with the advantages of being quantum-safe, instant, automatic, environmentally friendly, most user friendly.

BitMint protocols may be established also on a very small scale because it does not require a minimum count of peers' approval.

The BitMint **Universal Payment Solutions [UPS]** are ready to serve a small and large payment regimen, locally – retail and wholesale, or remotely (cross border).

We will be happy to offer invaluable guidance and assistance in all project components to ensure the architecture is countering the growing threats posed by AI-Cryptanalysis and by quantum computing, which are the looming threats of any payment and currency system, and especially on digital currencies.

This should be a design choice from day one, since once a digital-cash framework is put in place, it will be too late to uproot it! (protecting digital cash against these threats by adding more layers of complexity 'on the go'...is an illusion!)

Our commitment lies not only in providing cutting-edge technology, but also in accompanying you in all other aspects as well as in every step of the way as you navigate the evolving landscape of digital cash.

We are obliged and have the talent and knowhow and vast experience with comprehensive digital payment solutions that encompass the entire cycle and various methods, features and use cases for conducting a wide range of transactions with digital cash, that **we are willing to share with your Future of Money team.**



ii. What core functionality should be provided by the digital cash platform and what should be provided by the market?

The Reserve bank should create, issue and redeem the digital cash. Transactions should be autonomously conducted by traders, and as required by regulation, with commercial banks or regulated PSP's oversight.

Hereunder, examples of use cases for the market (commercial banks, fintech's etc.) to provide, based on the digital cash to be issued by the Reserve Bank:

privacy coin;
coin with expiration time and incentives;
redeemable loyalty token with ID;
positive and negative coins;
Interest bearing coins;
and more.

iii. What key governance measures would you expect the Reserve Bank to provide in the digital cash ecosystem?

A robust regulation and supervision are required for maintaining trust in the financial and monetary system. The Reserve Bank should provide Regulation to balance between fulfilling citizens' expectations from the digital cash to support their welfare and desire for privacy and liberalizations, alongside taking care of financial stability and monetary stability, and between preserving commercial banks' role in the financial system, as well as minimizing the possible exploitation of digital cash for money laundering and other illicit activities .

In order to foster broad adoption and public trust, apart from educating the public BEFORE issuing the digital cash, we recommend that the following principles will be guaranteed by the technology, not just by regulations, that could be changed in the future:

Digital cash will adhere to the principles of responsible and trustworthy public good currency, such as fairness, privacy, accountability and inclusivity.

We strongly believe that cash-like privacy should not be bound to offline payments only, but be extended to online payments with close proximity under a certain threshold. Strong privacy should be a key differentiator of the digital cash. Privacy should be backed by technical assurance.





10. Intermediaries will still own the customer relationship including managing onboarding and AML/CFT requirements. What support or enabling functionality would you require?

The digital cash platform could allow users to exchanging money bilaterally without intermediaries in the transaction process, and without validators, nodes and peer review, as well as to transact with digital cash settlement components.

We assume that it's in the interest of the Reserve Bank to encourage PSPs to compete with each other with added value services based on the digital cash, in order to foster innovation. It's important to provide to the public accessible information what services by PSPs should not be charged.

The selection of technologies for the digital cash components is of major importance. A high focus needs to be on resiliency and scalability and on creating a quantum-safe digital cash, that is not being hinged on vulnerable cryptography, as well as building a solid foundation that will preserve privacy as well as keeping payment behavior unexposed, while offering powerful tools to prevent money laundering and other criminal activities.

Managed issuance

Future stages of work explore the potential impacts of digital cash on the financial system and understand the benefits, costs and risks. To assist with this we would like feedback from industry on the following:

11. Do you expect remuneration to be paid on digital cash holdings?

It is of utmost importance to maintain the free use of the digital cash as a single currency with a legal tender status.

No fees should be applied to funding and defunding of digital cash.

However, digital cash could be designed with an optional procedure to enable remuneration, Interest and being positive or negative (debit).

12. Do you think there should be holding limits for digital cash or other restrictions in how it is issued?

The digital cash, like its name, should be M0; - the most liquid form of money: cash. Restriction or thresholds could be relevant for anonymous transactions or for offline payments (since so far there are NO feasible solutions for offline payment, that can resist fraud and counterfeit).





To conclude -

To foster trust, inclusivity, scalability and broad acceptance of digital cash, it's recommended to combine a conventional data base for centralized minting and redeeming of pattern-devoid digital cash, while transactions being executed peer-to-peer via a public ledger, with no intermediaries and not being dependent on validators, nodes or peers review, eliminating complex consensus mechanisms.

Thus, enhancing all critical elements of a reliable payment system, including decentralization, security, useability and scalability, WITHOUT anyone to come at the expense of weakening another, taking advantage on both centralized and de-centralized protocols' added values, without their faults and deficiencies, being highly scalable by design without facing from a 'single point of failure', and on top of that being resistant against future quantum computing capabilities and against foreseeable threat of AI-cryptanalysis.

The above is doable!

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

Let's do the digital cash right!

Stable, Versatile, Simple.

We share a lot of the Consultation Paper views. Let's work together on designing an effective, reliable and creative digital cash, to offer

- better security,
- more privacy without enabling illicit activities,
- more use cases,
- less environmental foot print,

compared to prevailing payment rails and to crypto-based CBDCs,

towards becoming a tool for a better tomorrow.

