

To The Reserve Bank of New Zealand (RBNZ) or other interested governmental entities.

Regarding the current considerations of the creation of a CBDC (Central Bank Digital Currency) or as it is being called "Digital Cash" system for New Zealand I have felt that I needed to compile this submission as I feel very strongly about such a system.

A digital currency system for New Zealand is needed and presents many significant potential benefits but equally has many significant potential risks.

The sovereignty of New Zealand necessitates the New Zealand dollar be strong, reliable and stable. The possibility of people within NZ starting to use other currencies for every day trading or Dollarization as it is commonly referred to (usually in relation to the \$US gaining prevalence) is a very real risk if NZ does not have digital currency options. Many people across the world are fond of the idea of global unification in many areas including currency for trade however this leads to stagnation a certain amount of friendly push and pull or competition at many different levels including the national is needed to maintain vibrancy and purpose.

Easy, straight forward transactions with as few middle men as possible is only to the greater benefit of the New Zealand economy.

Given the statements above it is my belief that CBDC's present one of the greatest threats to our societies today (potentially greater than the fears some have about AI). The issue is that they are a ticking time bomb due to the principals of "legislative creep", "Power corrupts and absolute power corrupts absolutely" and "any system that can be abused will be abused".

Once a the majority of a society adopts a CBDC everyone is locked into it and the controller of the system (ie governmental entities) can alter laws and/or change the system as they see fit with the general populous unable to do anything. Once a CBDC is well adopted promises that conventional cash won't be done away with are irrelevant. Society must be protected from the potential predations of future less than benevolent governments or even stupid governmental policy (see the collapse of the Argentinian Peso).

Our entire democratic government and legal structure is set up in such a way as to protect against Governmental predation and corruption, but with a CBDC so much power and control over the population is focussed in one location that any kind of dissent can easily be shut down by those in power.

In the consultation paper it is good to see that RBNZ is focussed on the items indicated in Figure 8 (pg 31 - Support the market and Digital Economy as defined in table 3 on page 30 – Screenshots below) and away from the control aspects of digital currencies which many central banks and governments are so keen for.

Figure 8: Reserve Bank's preferred design positioning

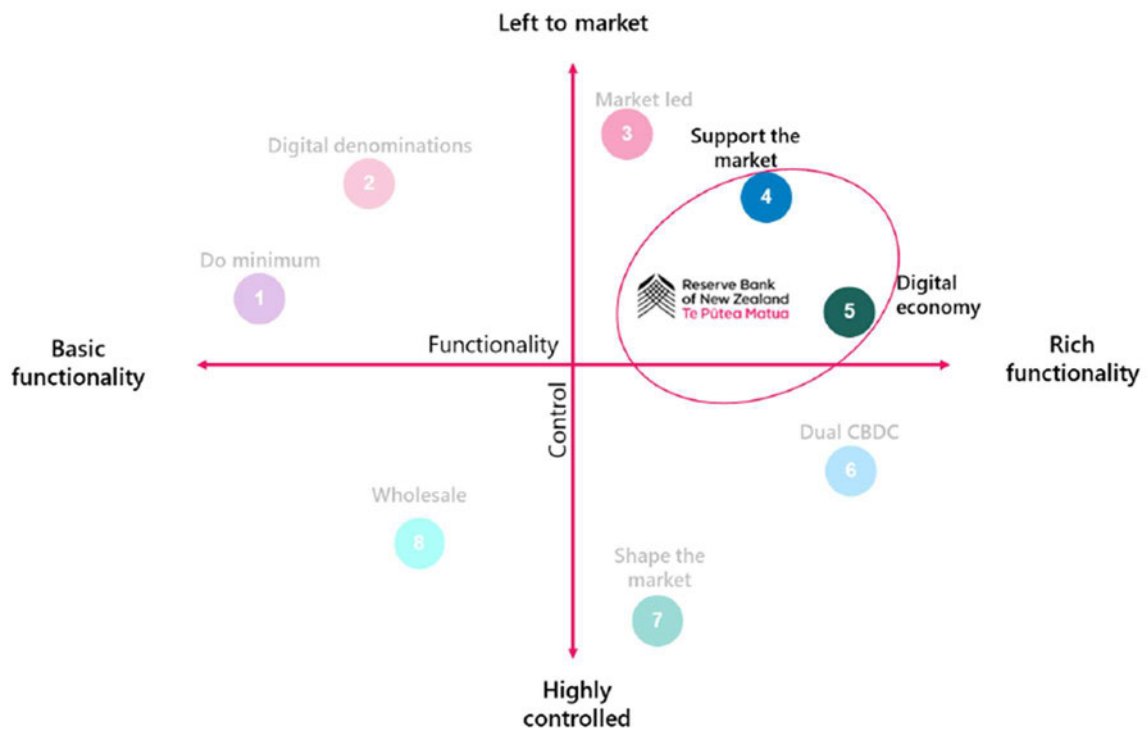


Table 3: Design models for central bank issued digital cash

Model	Description
Do minimum	The simplest possible digital cash model. The Reserve Bank issues only the core systems and functions but keeps flexibility to expand on these functions later. Retail use cases are prioritised, and the ecosystem is less defined.
Digital denominations	A model that replicates the fixed denominations of physical cash \$0.10, \$0.20, \$0.50, \$1, \$2, \$5, \$10, \$20, \$50 and \$100. It would require payments in these denominations and 'change' to be given. It includes offline capability but is less flexible to other innovations.
Market led	The Reserve Bank provides a basic platform and allows it to be widely accessed. Service providers (not the platform) hold and manage user information and transactional activity. There are many roles in the digital cash ecosystem that are left to the market.
Support the market	The Reserve Bank and the market of service providers collaborate to provide tools and functions in the digital cash ecosystem. There is wide access to a feature-rich digital cash platform that provides functions designed to support and accelerate innovate products and services.
Digital economy	The digital cash platform has an open architecture and many features to support all uses. It is highly integrated with other digital economy systems and stakeholders.
Dual CBDC	Service providers hold wholesale digital cash and use it to issue retail stablecoins that are highly innovative.
Shape the market	The digital cash platform and rules are provided by the Reserve Bank in a highly regulated and controlled environment. The rules set out the price arrangements, services (including customer), and user safeguards.
Wholesale	Digital cash acts as an innovation layer on top of existing payment systems to provide enhanced services to financial institutions already in payments systems. This includes a cross-border bridge to support better international transfers.

Also it is good to see the in Figure 1 (pg 7 – screenshot below) the “Private and Secure” items and per the last few paragraphs these are my greatest concern.

Figure 1: Digital cash design features

Issued by the Reserve Bank	Denominated in NZD	Swapped 1:1 with cash and other NZD money	Central bank money held on Reserve Bank balance sheet	Safe from credit risk
Distributed by the private sector	Many service providers offering digital cash services	User chooses their service providers	Payments are made via a Reserve Bank owned digital cash platform	Can be used on a range of devices
Innovative and inclusive payments	Widely available to the NZ public	Can make payments 'offline'	Send and receive payments instantly and at any time	Smart contracts compatible
Private and secure	Reserve Bank will not collect transaction data	Reserve Bank will not limit how digital cash can be used	Safe from cyber-attacks and operationally reliable	Rules on how your information is used by third parties

For the “Private and Secure” features in Figure 1 to be truly achieved and to prevent the removal of these features by future governments there are a number of technical features that are absolutely required and are unachievable without it.

1. The software source of the Digital Cash system must be open source (accessible to anyone).

Widely used open source software is the most stress tested for exploits in the world as anyone can view the code and try to break/hack it. An excellent example of this is Bitcoin. Bitcoin is open source and has existed for over 15 and never been hacked despite hundreds of billions of dollars in value being stored (Only centralised systems such as exchanges or individual wallets, due to poor personal security exposing private, keys have been hacked not the actual bitcoin network).

Many people perceive closed source software to be more secure than open source but due to more limited testing by people fully knowledgeable of the code base this is simply not true. This becomes more and more true the more complex the software is.

To a certain extent closed source software offers a weak form of security called “security through obscurity”. “Security through obscurity” can be easily understood through the analogy – a person says “can’t take my money because I have hidden it” (ie someone searches enough they may find it). The opposite of this is - a person says is my money is in this massive steel vault heavily concreted deeply into the ground – everyone knows where the money is but it is either impossible or impractical to take it.

Being open source allows the New Zealand public to review the code (should they have the knowledge to do so) and ensure that the planned privacy and security features remain in place preventing their quiet removal.

As an open source project in which RBNZ has a significant vested interest it would be the primary driver and facilitator of the Digital Cash system software development but also publically allow for other interested entities to participate in the development potentially reducing the internal development cost to the RBNZ while also allowing for wide ranging and feature addition due to the code contributions from others.

2. The NZ Digital Cash system must run in a decentralised manner and not solely on RBNZ or contracted entities servers.

If the Digital Cash system runs only on RBNZ or contracted entities servers regardless of if the system software is open source or not

Anyone with a hardware setup that meets defined requirements as well as a number of other predefined and coded in criteria such as locked up finances of a certain level, should be able to run a full or partial node in the system. These nodes would participate in the processing of transactions with the nodes collectively acting to ensure that everyone remains honest and with locked up finances of the operator at risk in the event of malicious activity as defined by the system's software.

Tiny almost imperceptible transaction fees (\$0.01 or even less) paid to node operators would allow for the funding of node operation which should be minimal and offer an incentive to people to run a node.

Having the Digital cash system operate as a decentralised system would also mean that if system development over time deviated slowly away from the initial design and development principles to the point that a significant enough number of people agreed that it was a problem, it would fairly straight forward for a competing to be setup running a previous or different version of the system but still in \$NZ and so not undermining overall NZ currency sovereignty (though likely with fewer features).

Additionally, a well built, decentralised system provides substantial resistance against malicious cyber-attacks (e.g distributed denial of service or Ddos attacks) which a national currency is potential at risk of if particularly from foreign governmental interests. E.g if NZ had a centralised digital currency then a state sponsored Ddos attack could easily cripple NZ's financial infrastructure. NZ's infrastructure could not compete with a Ddos attack from large countries or multiple smaller ones.

3. The NZ Digital Cash system should allow for competing but interoperable decentralised \$NZ denominated block chain systems (but only decentralised ones) through the implementation of inter blockchain communication or IBC (a well know and proven functionality in crypto currency circles).

The permitting of parallel decentralised systems provides an expanded and or backup financial system in the event of any kind of issue with the official RBNZ supported system.

Permitting such systems would also assist in protecting against governmental predation providing a flight points where people would be able to move their cash to (still in \$NZ) and further from governmental interference (parallel centralised systems would not provide this protection).

IBC functionality would also allow the potential for seamless interaction with other sovereign digital currency systems that also integrated IBC facilitating currency conversion for travellers to or from NZ and even cross border financial transactions (e.g online purchases or international remittances without a middle man).

Also if IBC were established across many sovereign digital currencies would the Bank for international settlements really be needed.

4. On chain governance should be required for system updates and changes with a popular vote by citizens only.

Participation should probably be governed by IRD number and independent of wallet as the system is for NZ which is it's citizenry. Requiring popular acceptance of updates would protect against malicious changes as different knowledgeable, interested parties would be bound to publicise their views for and against to encourage the public to support or object to updates.

5. The 4 items above would protect the long term integrity of the NZ financial system and encourage confidence in the NZ economy for its citizens but not only it's citizens. As RBNZ is well aware all countries reserve banks and many other large international entities commonly keep reserves of other various currencies. A digital cash system with strong protections against governmental predations or stupidity will be extremely attractive to foreign governments.

Given that many central banks are currently planning digital currencies, and that many of those governments are particularly keen on a lot of the more controlling aspects CBDC systems offer, having NZ's digital cash as open and free to use as well as being well protected from the whims of those in power at any particular time is only to the benefit of NZ. It will without a doubt increase the value of the \$NZ in the eyes of large international entities relative to other digital currencies that are not so well protected.

6. I am particularly interested in the claimed offline transaction function described in the Consultation paper as having a solid understanding of the basics of block chain technology I cannot conceive of any way of doing an offline digital currency transaction as there would be no way to verify that a transaction has been processed and transferred and most importantly that the funds have not already been spent offline elsewhere.

Conceivably it might be possible to have transactions verified by software automated phone connection or SMS message but I cannot consider this to be an offline transfer as you are still relying on a mass communication network.

I hope that this submission is found to be helpful. I am quite interested in blockchain and crypto currency and would be interested in participating in the development of a Digital NZ dollar particularly given the points I have made above. A NZ dollar backed (alongside other currencies) stable coin system is also something I have been considering for quite some time.

Unfortunately, I have only very recently become aware of the current RBNZ plans and so have only been able to skim through the consultation paper so as to have time to right this submission.

As an additional point to the itemised points above a well-crafted decentralised NZ digital currency system which incorporated IBC technology would be well placed for implementation as a CBDC for other countries facilitating easy trade and also distributing the software development load as well as system security. Each country would naturally be watching the software development contributions of each other like a hawk ensuring it the system is as robust as possible due to their own self-interest.

Finally I have felt strongly enough about this to write this submission and put my name and contact info to which is something I have always been very reluctant to as I value my privacy when it comes to governmental and corporate interests.

Regards

David Price

Redacted under 9(2)(a)

[Redacted]
[Redacted]
[Redacted]

Avondale
Auckland

Redacted 9(2)(a) [Redacted]
[Redacted]