Hasq Technology as a Platform for National Digital Currency

Hasq Technology Pty Ltd, *2016* (DRAFT v2)

I. Introduction

The concept of money as medium of exchange and common measure of value has been around for thousands of years. While different societies in different times used different natural or artificial objects to represent standard units of value, one of their characteristics remained unchanged – they were physical objects. Even today fiat money physically represented in the form of banknotes and coins is the preferred way of payment in many countries around the world. Cash has also proven to be indispensable for small transactions due to the ease of use. However, despite being proven to work, physical money has deficiencies listed below.

- It's expensive from the government's point of view. Banknotes and coins have to be manufactured with a high degree of protection from forging. Their quality and the quantity in circulation have to be constantly monitored. Specialised equipment is required for counting and handling them. Storing and transporting large amounts of physical money need both high security facilities and vehicles as well as involvement of security personnel.
- It's difficult for a government to control cash involved in criminal activity.
- Cash is the main reason for the existence of certain types of crime (e.g. robberies).
- Cash based economy creates multiple opportunities for tax avoidance.
- Being physical objects, banknotes and coins are easy to lose, misplace or damage. Cash transactions may also attract unwanted attention from general public.

The deficiencies described above seem to be unavoidable and as such are accepted by everyone. However, it's important to understand that they exist only because banknotes and coins are physical objects. The latest advances both in hardware and software technologies make it possible to replace paper money by electronic cash which does not have the deficiencies listed above and which is almost as easy to use as traditional money.

Below we describe how Hasq technology can be used as a basis for creating national electronic currency and what typical transactions may look like. It's worth noting that many technical aspects are omitted for clarity and some concepts may require further development in order to meet future government requirements.

II. Infrastructure

Naturally, electronic money requires technical infrastructure for the system to work. This infrastructure consists of three major components - computer servers, devices for accessing these servers and communication channels.

A Hasq server may work alone, however our technology supports a network of servers, which automatically exchange information and reconfigure/restore the network in case it becomes fragmented or not optimal. Since servers store information about tokens representing money in circulation and transactions, they must be owned by the government. Considering the necessity to balance a transactional load as well as to have redundancy, we estimate that 3-5 servers can satisfy the needs of a few million users. Ideally, servers have to be geographically separated. Usual requirements of a reliable power supply, security etc also apply.

Devices used by the general public to access the servers include public or private computers, mobile devices or any specialised devices developed for this purpose.

The important aspect of any large scale technical system is the cost of deployment and ongoing maintenance. A vast number of computers and mobile devices in private possession as well as the existence of various communication technologies means that neither the government nor the general public needs to spend any funds on buying/upgrading the hardware that's already in place in order to access Hasq servers. The only component that requires upfront government spending is the network of servers itself. However, in terms of their technical abilities, Hasq servers don't need to be different from any other good quality servers used by the government. So the cost of deployment and maintenance of a Hasq network will be comparable with that of a regular computer network consisting of the same number of servers. We believe that at the national level this cost is negligible in comparison with the amount of resources that the proposed system of electronic currency will free up.

III. How it works

A. *Transaction*

Hasq tokens are digital objects that represent money. In Hasq terms a transaction is the transfer of token ownership from a payer to a payee. The infrastructure, set up by the regulatory authority, provides the service of transactions at a basic level. Hasq tokens are operated by this service, but not owned. Each token's transaction is stored in the distributed database as a record in a chain of records corresponding to this token. The records in the chain are linked to each other and every new transaction adds one more record to this chain.

At the lowest level a transaction is the transfer of digital keys (hash function values), necessary to control a token from the previous token's owner to the next. At this level users don't require special devices or trusted applications to complete a transaction.

At a higher level a transaction is represented by a communication session between two applications. In this case users need certified applications running on a computing device. Such an application can be embodied in a smartphone or a smartcard. In the rest of the document we call this application a *wallet device*, by analogy to a wallet that holds banknotes and coins.

Transactions can be categorised into different types depending whether the users have access to the Internet, and whether they have wallet devices.

B. Simple online

A simple online transaction occurs when two users have access to the Internet and allow their wallet devices to communicate with each other in order to transfer the digital keys. The wallet devices immediately finalise the transaction on the servers.

C. Limited online

This case describes the situation where the users do not have their wallet devices, but they have access to the Internet via a public (possibly untrusted) computer. Using a web page of one of the servers, the payer initiates the search of their tokens. Then, using the same web page, they generate digital keys for tokens which are to be transferred to the payee. These keys are obtained by the payee who then uses them to finalise the transaction, effectively taking ownership of the tokens. Functionality of limited online transactions is implemented on [*http://tokenswap.com*].

D. Simple offline

Transactions of this type occur when there is no access to the Internet. In this case the payer's and payee's wallet devices communicate in the same manner as in online transaction (no difference from the user perspective), but the finalisation step is deferred.

At the application level each wallet device involved in such a transaction keeps track of the tokens that have changed ownership. Once any of these wallet devices goes online, it finalises the transactions on the server. The technology allows implementation of such a scheme to be secure and not allowing double spending.

E. Limited offline

This case describes a situation when there is no access to the Internet and the payee does not have a wallet device. In this case the user interface of the payer's wallet device asks the payee to enter a passphrase which is later used to generate transactional keys. Then the application constructs the offline transaction in the same way as in the simple offline scenario described above. Once the payer's wallet device goes online, the application transfers accumulated information to the server.

To prevent a possible delay of finalisation, loss or even destruction of the payer's wallet, the application can reserve some amount of money as a guarantee of the transaction, effectively making the transaction conditional to the amount that remains locked for the payer until finalising.

F. "Hold-on" and "backward" transactions

Hasq technology naturally allows for two special types of transactions, which are not supported by cash or any known electronic currency.

1) "Hold-on" transaction: A token can be put into a "hold-on" state. In this state a token does not belong completely to either party of the transaction and cannot be controlled solely by the payer or the payee until an agreement between them is reached. A token can be put into this state by the payer and this can be verified by the payee. Later either party can release the token making the other party the full owner. Such a state allows to split the transaction into two steps: 1) the payer's commitment and 2) finalisation or reverse.

This kind of transaction can be useful in situations where prepayment for goods is required, but there is a risk that the goods may not be delivered. In other words, the payer and the payee do not trust each other. In this situation the payee may start delivering the goods upon the payer beginning a "hold-on" transaction (effectively having already spent the required amount of money). Once the goods are delivered, the payer releases the "hold-on" tokens so that the payee can receive their payment.

2) "Backward" transaction: In a "backward" transaction the keys are passed in the opposite direction, from the payee to the payer, contrary to a typical transaction where the payer passes the keys over to the payee. This type of transaction can be useful when the payee does not have the ability to execute the transaction or willing to remain anonymous.

G. Change in transactions

Similarly to ordinary banknotes, Hasq tokens are not breakable into smaller nominations. However, tokens can be swapped over for other tokens of the same combined value. A set of new tokens can be arranged in a way that allows the correct payment to be made. The rest of the tokens form "change" that stays in the payer's wallet. The exchange operation can be performed immediately using the server or by the deferred offline method described above.

IV. Security considerations

The core engine of Hasq technology is based on the use of hash functions. It does not require public cryptography. Hasq chains are not bound to a particular hash function and any secure hash function can be used (e.g. SHA-2 with 256 or 512 bits). The security of the whole system completely relies on the security of the chosen hash function. One important point to note is that the security of Hasq chains does not depend on the quality of the software supporting it. If the software is buggy or compromised, the system just does not function. Also, there is no point to hack servers because they do not store any secret information. Altering the servers function would just invalidate compromised operations, but would not change the database consistency prior to the break.

Wallet devices required for offline transactions are implemented with partially homomorphic encryption schemes, such as the strong encryption mode of Cryptoleq. Hasq technology is robust. The idea of Hasq chains is simple and can be verified by any person with a basic knowledge of maths and hash functions.

V. Summary: Cash vs Hasq tokens

Feature	**Cash**	**Hasq tokens**
Cost	High[1)]	Low[2)]
Controlling cash involved into criminal activity	Limited[3)]	Advanced[4)]
Tax avoidance / significant transactions	Hidden	Can be detected
Handling banknotes and coins	Required	Not required
Transfer requires a 3rd party	No	No
Number of banknotes or tokens in circulation	Unlimited	Unlimited
”Hold-on” transaction state	Not supported	Supported
”Backward” transaction	Not supported	Supported

[1)] Banknotes and coins require high security printing/minting and storage facilities, handling equipment, and security staff.

[2)] Digital tokens have no associated production or maintenance expenses.

[3)] Criminal intent has to be known before the transaction.

[4)] Tokens can be blocked or invalidated by the governing agency at any time – before or post factum.