Cross Border Payment

Innovation to make cross-border payments all around the world
easy, fast, secure and competitively priced

Abstract

Innovative well-designed digital currency can bring benefits to wholesale cross-border settlements. They have the potential to revolutionize the FX markets, reducing the dependence of intermediaries, being more efficient, leading to more effective market structures, and opening up competition. And as such, in the future they may substitute (or co-exist with) the SWIFT system. In the meantime, there are several concerns that still suffers from gaps, e.g. inconsistencies and redundancies of regulatory aspects at international levels, as cross-border payments system must be compliant with the rules and regulations of all connected countries, including capital flow management measures, as well as associated technological and financial challenges; information flows between countries should be improved to help authorities counter illicit use of money, including tax evasion. A Superposition Currency Framework for Cross Border Payment can mitigate part of these challenges, adhering to the principles of compliance, and interoperability. A Superposition currency is a Digital Currency that is traded as a temporary currency indeterminate between the payer's currency and the payee's currency. On top of that, we have to realize that the full range of modern cryptographic products, and especially the ones used by wholesale transfer of money, are subject to attack by Quantum computers. This cause must lead to a money language that is being a-priori designed to withstand even the fiercest attack by quantum computers.

Bullet points:

- The large sums of money that flow between global and national banks is a persistent attractive target for electronic thieves.

- Resilient wholesale as well cross-border payment solution should not necessarily rely on validation by backtracking the history of the money which is the tedious effort of reconciliation.

- Moreover, the full range of modern cryptographic products, and especially the ones used by wholesale transfer of money, is subject to attack by Quantum computers.

- The BitMint money language is native to quantum technology, it is being a-priori designed to withstand even the fiercest attack by quantum computers and as such it is a most fitting language for 21st century money.

- The BitMint digital coin carries with it its full chain of custody, so that authorities can trace the whereabouts of the coin since it was minted, and it also creating an accounting Tri-log: bank servers (income books) compared to expense records (or records on the BSN – the Blockchain based Service Network), and both compared to the chain of custody tallied in the BitMint coin (written on the coin itself!). Mistakes are prevented, untoward money routing is exposed.

- On top we propose a Superposition Money Framework 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.

Preface

We propose a generic coin to represent an entity bearing a financial value. We define 'financial value' as an exchange item in a fair transaction where the counterflow is comprised of some measure of goods or services, such that the recipient of the financial value will end up with an asset they can exchange for another measure of goods or services to satisfy their needs.

In other words, abstract and per se as a financial value is, it is acceptable by those who give off products or services, and it is non-vanishing at least for a prescribed span of time, so it is usable by its current owner .

The financial value of the newly designed digital money is a number, but the entity itself that bears this value -- the coin -- has other features.

- It has an identity (like a banknote's serial number),
- it has terms of redemption,
- it has all sorts of data attached to it with the firm grip of modern cryptography.

Such data may be the identity of its current owner, so no thief can pass it around as payment.

It may be the full chain of its custodial history, so that authorities can trace the whereabouts of the coin since it was minted.

It might indicate purpose, say a coin limited to buying foodstuff and unacceptable in a casino.

The new financial language will codify all those terms that become intrinsic features of the coin, all based on its fundamental property of having a distinct unique identity .

The identity of a financial entity of any sort may be linked to a full-blown contract under which it flows. The complete terms of the legal instrument that governs its movement will be nominally recorded, preventing misuse and abuse of allocated funds.

Its custodians will be unable to route money beyond what its tethered features prescribe.

The identity of the coin will include the identity of its mint plus a unique marker to distinguish it from all other coins. The identity will also specify the nature of the coin: positive money, negative money (obligation), etc.

- Security is paramount. A global currency and global framework for financial instruments cannot be dependent on the hope that no one will find a shortcut for hashing or for elliptic curve complexity -- the mathematical foundation of bitcoin. Apart from math insight, quantum computers, by applying brute force approach, will crack all the financial ciphers in use today.

BitMint specify its solutions to be quantum-computing resistant, and security adjustable operated. Namely security of money storage or money transit should be adjustable according to (i) the threat environment and (ii) the amount of money involved.

- The key to the success of the newly designed financial alphabet is its versatility with respect to the full canvass of regulatory regimens. Different countries run their financial matters differently. There is a wide range of philosophies with respect to levels of anonymity, government tracking and visibility, and the rules change from cash to credit to complicated financial instruments. The newly designed financial language will have to be versatile enough to accommodate this variety while insuring global financial flow for the benefit of all.

This is the vision we hold up for the BitMint new financial language: digital money that operates as a globally adhered-to financial railway, respecting fully the financial sovereignty of the participating political entities.

Interoperability: Superposition Currency for Cross Border Payment

This is significant as holders of different coins will require the ability to exchange with one another.

International borders represent two boundaries for two distinct, and often contradictory financial ecosystems. Different currencies, different regulatory climate, political tension, all contribute to harmful friction, at times of paralytic proportions. This friction makes it impractical to pass around small sums of money, and makes it costly to transfer larger sums, not to speak about time loss. In recent years the AML (anti-money laundering) efforts on a global scale built up more friction, posing a big hurdle on the goal for efficient global finance.

Many solutions are focused on proper translation of regulatory environments between the payer and the payee zones. They can be supported by the concept of superposition currency. The term 'superposition' is used in physics to indicate subatomic entities that are in an intermediate state for a short period before they 'collapse' to one of two allowable states.

We borrow this concept to devise a currency that is a superposition between the currency paid by the payer and the currency received by the payee. This super-positioned currency will be short lived and will soon be reduced to one or the other currencies it is a superposition of.

While in a superposition state this currency will be tradable frictionlessly while crossing international borders. This is a mechanism to achieve transaction speed and transaction smoothness by sharing the settlement uncertainties between the payer and the payee.

Much as a “qbit” is a super-positioned bit that accepts values zero or one, so we should use *qmoney* to indicate super-positioned money that can accept a value in either the payer currency or the payee currency.

qmoney may be digitally minted, and digitally traded. The reduction or collapse of the qmoney to regular money is a matter of agreement between the two relevant financial ecosystems.

The basic operation is as follows: the payer uses his currency to buy a certain amount of qmoney. The payer then passes the qmoney to the payee, with all the authentication protocols to insure proper transfer. The payee eventually redeems the qmoney against his own currency.

The advantage of this configuration is *first* in the use of digital money payment technology to affect payment from any spot on the globe to any other spot, and *second* in the ability to separate regulatory settlement from the trade itself. The fast trade happens with this superimposed currency that no trader knows exactly how it would “collapse” to one currency or the other. Both parties share the burden of this uncertainty.

The *third* and powerful advantage of the qmoney solution is its ability to suppress the exploitation of fast, unexpected movements in relative values of two national currencies. Some of the richest people in the world today made their fortune not on building or manufacturing much but on smart and lucky exploitation of currency prices in terms of other national currencies. The betting on such alluring riches, and the fear of commensurate loss, puts a lot of tension on cross border trade. The qmoney solution will calm this tension down, via a smart reduction protocol, namely a good way to resolve the currency uncertainty.