Assessment of Mojaloop

Developed by the Bill & Melinda Gates Foundation

By Nick Brown

Founder of Clear Purchase, Inc.
and technical expert in Financial Infrastructure Systems

June 2018

Summary

Clear Purchase is building a new payment system for developing countries, and is interested in the potential benefit of working with initiatives like Mojaloop, developed by the Bill & Melinda Gates Foundation (BMGF).

We detail in this document the reasoning behind our reluctant decision to decline the adoption of Mojaloop into our secure payment system, and also argue everyone else do the same.

Summary of Clear Purchase

Clear Purchase is central to the movement that will break the poverty trap for the poorest 3 Billion people on this planet. We are looking to create a truly cashless economy where even the tiniest transaction can be done electronically.

Our role in this movement is to build a new Payment Hub that connects everyone together, so that anyone can transact with anyone else regardless of where they have an account.

This is similar to the VISA model, where each connected system offers our services to their customers and we facilitate transactions between systems. Includes: sending of funds, payroll, automatic bill payments, micro-lending, and most importantly tiny purchases.
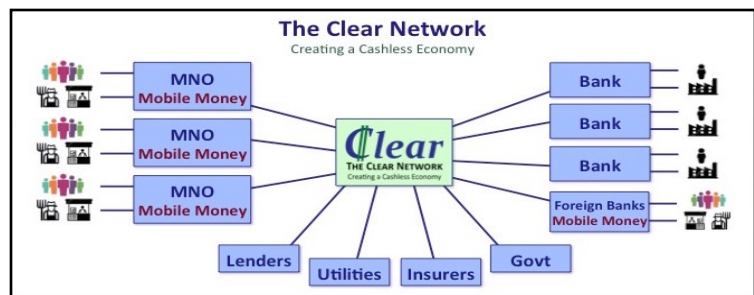

Mojaloop is an Interface

If Mojaloop is loaded onto the systems of two different companies, it would become an interface between the two systems, used to process financial transaction between them.

Clear Purchase adoption of Mojaloop

Mojaloop would be the interface on each end of a connection from a Mobile Money Operator to our Hub.

If every system connected this way:
- Simplify connection process.
- Simplify management of each connection.
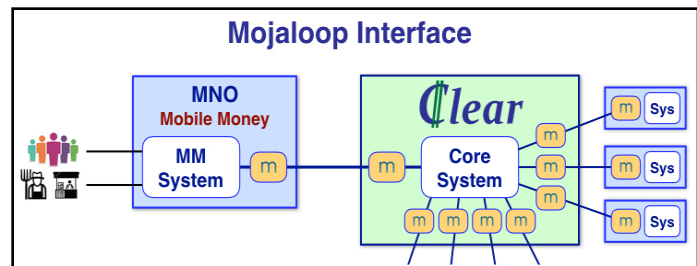
Decision to Decline: Mojaloop is Open Source

The Payment Industry is not the right industry for 'Open Source'. There is over $20B of payment fraud per year, and a Mojaloop system would be too tempting and easy a target.

We will not be adopting Mojaloop because of data security concerns.

Warning: If financial service providers adopt a Mojaloop based system, the inevitable disastrous results could set back the entire Financial Inclusion initiative for years.

Introduction to the Payment Infrastructure Industry

In order to understand the reasoning behind this assessment of Mojaloop as a product/service within the Payment Infrastructure industry, it is important to have a basic understanding of this unique and incredibly complex industry.

The real-time processing of payments between systems is fraught with hazards both accidental and intentional, with massive financial consequences. There are so many pitfalls that are easy to fall into unless you know what to look for, every one affecting people's money.

The central focus of this industry is to continually work on maximizing: *availability*, *reliability* and *security*.

Example of complexity of this industry: VISA issues mandates of changes to be adopted across all players involved in processing credit/debit card transactions. They allow 6 years for these mandates to be applied - it takes that long!

Fraud in the Payment Industry

Fraud is by far the biggest concern in this industry.

Globally, credit/debit card fraud is in excess of $20B per year. This does not include the cost of fraud detection, fraud prevention and fraud management. This is a lucrative market for those committing fraud, who have the resources to spend vast amounts on finding new ways to commit fraud, and reach into new markets.

The target of fraud is nearly always the weakest link in the chain. For credit/debit cards, this would be the merchant's systems. Unfortunately, most merchants when hacked do not even know it has happened and therefore don't take any action to address it.

Example of importance: Many years ago I was a member of the Associated Standards Committee's X9/F6 working group, which was responsible for writing national (ANSI) and international (ISO) standards for data security in the financial services industry. This was a tiny group of experts (around 15 people) representing each the different industry players mentioned below. We were focused on data at rest and data in motion', and were planning 5 - 10 years ahead.

Different Players

There are many different players in this industry, each with their own perspective and priority.

- **ATM/POS Device Manufacturers**: They manufacture and selling physical devices that can process different types of financial transactions. Their priority is selling a reliable device that is easy to manage with the appropriate level of security necessary.

- **Financial Institutions (FI)**: Their priority is to manage the accounts of their customers, and providing them with a range of financial services. They also manage ATM and POS networks to process transactions for their customers, connecting their systems to one or more Payment Hub's. 24 hour availability of these services is a priority. Because of the costs involved, only the biggest run their own systems, the rest outsourcing this to companies like Fiserv here in the US. Initially *Banks*, now includes *Mobile Money* operators.

- **Merchants**: Their primary focus is to make sales, and would like to accept any kind of payment their customers might want to use. They will most likely have POS devices, a web site, and possibly other digital sales platform. Only the largest have their own system for payments, the rest outsource this to their *Merchant Bank* or a *Gateway*.

- **Gateways**: They provide a means for smaller merchants to easily accept payments, especially online.

- **Payment Hubs**: They connect FIs and some huge Merchants together, as well as to other Payment Hubs. Their core service is to process transactions between systems, and their highest priority to be running and able to process transactions at all times. Often called *Interchanges* or *Payment Switches*.

- **Payment Software Vendors**: There are very few companies that offer payment processing software to FIs, big merchants and payment hubs. The biggest is Base24 produced by ACI (Nasdaq: ACIW). Their top priority is to provide reliable and secure software, customer enhancements, and 24 hour support.

Resistance to Change

This entire industry is resistant to change, and for very good reasons. Once a company installs a payment system, there is little upside and massive downside in switching to a new system.

It is important to understand this characteristic of the industry, as the Adopters will be facing huge challenges to get started and into each market, however once running they will then have minimal competition.

Example: Many years ago while I was working at ACI, they introduced a new product which was considerably superior to the old. Almost all of their customers refused to adopt this new product, even though it was developed by **the** *experts in the industry. The big Banks stuck with their existing systems even thought they were far from perfect - to them the known was safer than the unknown.*

Levels of Expertise

There are varying levels of experience in this industry, and it is important to understand the differences in order to recognize the level necessary to accomplish different aspects of a new system. The focus here is on the technical side.

- **Amateur**: Those without experience on high volume payment infrastructure system.

- **Experienced**: Those who have worked on one of the bigger systems (several million transactions per day), most likely at one of the major Banks or even a payment hub like VISA. They would have an understanding of the monitoring/maintaining of a production system, processing at least a million transactions per day. Would have dealt with a variety of critical errors on the production system, and have a good idea of the priorities the business places on differing aspects of the system.

- **Expert**: Those who understand the entire industry, gaining experience at most types of institution (see player list above), each with their own perspective and priorities. They would understand the reasons why the each type of systems is designed the way it is. Few people reach this level.

Example of contrast between Experienced and Expert: In 1996 when VISA International was building their new Debit Card System, they were struggling badly. They are exceptionally good at running those systems, but did not have the ability to build one from scratch. They realized they needed an expert, so they brought me in to implement their new system, which I did.

Core Requirements of a Payment Method

A payment method covers the entire end-to-end method of making a payment. *For example, a credit card transaction generally involves a merchant, possibly a gateway, a merchant bank, at least one payment hub, and an issuing bank.*

All payment methods must meet certain requirements to function.

Availability

The method of payment must be available whenever a user might want to use it. If a user wishes to use their account to make a purchase and the system is not available, then the user is less likely to trust the system in the future. They may additionally blame their FI and switch to another FI.

Reliability

As we are talking about people's money, it is imperative that no transaction be lost, modified or duplicated. Any failure will likely cause huge loss of trust, the user might stop using the payment method entirely, and word will spread quickly.

Reputation is everything in this industry.

Security

Data Security is the most challenging aspect of any payment model, and is of immense importance (see above). When someone makes a payment, they have the expectation that their personal/account information is secured and cannot be stolen and used against them.

Fraud prevention must be considered at the very design of a payment model, as it can be incredibly difficult, if not impossible, to fix later.

Remember, the weakest point in the transaction chain will be the target of hacking and manipulation.

Example: PayPal never thought about fraud when they designed their system. Once fraud started to occur they scrambled to deal with it. Unfortunately it was too late as their core model leaves itself wide open to certain types of fraud, and they were able to do little about it. Fraud is still a massive problem for PayPal and their customers.

Core Requirements of a Payment Hub

A Payment Hub must meet certain requirements in order to function.

Expectations are much higher than for FIs. If an FI's system fails then it generally only affects them and their customers, and they accept the consequences for their own failures. However, if a Payment Hub fails then it affects all FIs and their customers, and the customers will likely blame their FI.

Important: The FIs are putting their reputation on the line!

System Availability

A Payment Hub must be available **AT ALL TIMES**.

A Payment Hub must declare availability targets, and deliver on those targets. If the Payment Hub cannot deliver availability to the FIs, then the FIs will disconnect.

This is a challenge before the system is even running: the Payment Hub must convince the FIs that they can deliver on these availability targets in order for the FIs to trust them and connect in the first place. This comes down to experience and reputation in the industry, and is improved by large recognized organizations backing it.

Transaction Integrity

This is one of the central roles of a Payment Hub, to ensure integrity of transactions between systems, and identifying corrupted or bogus transactions.

This is a fairly standard aspect of any Payment Hub, often including encryption.

Data Security

The architecture of the payment process across the entire network will determine the security inherent in the system.

Legal & financial liability of each player involved by transaction type must be clearly defined.

Fraud Prevention

The architecture of the Payment Method dictates the types of fraud that are possible. Some fraud is impossible to eliminate (eg. someone claiming they got an empty box), while other types of fraud can be minimized or even eradicated. It is important to remember that those committing fraud will target the weakest link in the transaction chain.

Fraud identification/prevention functionality must be put in place to help identify when fraud is taking place in real-time to stop a fraudulent transaction from completing. While challenging, this is much less expensive than dealing with fraud after it has happened.

Much fraud is never even noticed. However, when it is (generally the user) there must be a means of reporting and managing the fraud.

Example: When I first heard about the new UPI system in India, I looked at their model and immediately identified a major security problem right at the core of their design that would leave themselves wide open to fraud. I pointed this out to a couple of people, and I am now hearing that fraud is indeed starting to happen on their systems.

Dispute Resolution

This is when a user raises a dispute regarding one of their transactions. This can be the result of fraudulent transaction, or a dispute between the parties involved in a legitimate transaction. There must be a clear means for the user to raise a dispute, and expected process the user will follow to resolution.

It is the obligation of the Payment Hub to clearly define processes and responsibilities for all connected organizations. This includes identifying which party involved in a disputed transaction takes financial responsibility for the transaction (dependent on conditions).

Example: PayPal never thought about dispute resolution when they designed their system, and cobbled together a poor system when one was demanded by their users. I may talk negatively in this document about PayPal. The reality is they created an amazing product, building about as good a system as was possible considering the other systems they had to integrate with. They just overlooked a couple of key aspects of their model with some negative result.

Introduction to Mojaloop

Mojaloop was created by the Bill & Melinda Gates Foundation (BMGF), under their Level One Project. BMGF commissioned several quality companies to develop the code under their supervision.

Mojaloop is open source software, intended to allow financial systems to communicate with each other to facilitate financial transactions.

Their intended market is developing countries, where there is currently little if any interoperability between financial systems. By simplifying the process of connecting systems, they hope to accelerate the path towards fully making digital financial services available to the poor. This is a critical aspect of the global Financial Inclusion initiative.

Overview of Mojaloop

Mojaloop is intended to be used by any Digital Financial Services Provider (DFSP) to talk to another DFSP that also has Mojaloop integrated in their system. The initial focus is Mobile Money Operators, with following adoption by conventional Banks. The intent is for their respective account holders to transact with each other using mobile phones. DFSPs can include other types of financial organizations, for example Micro-Lenders.
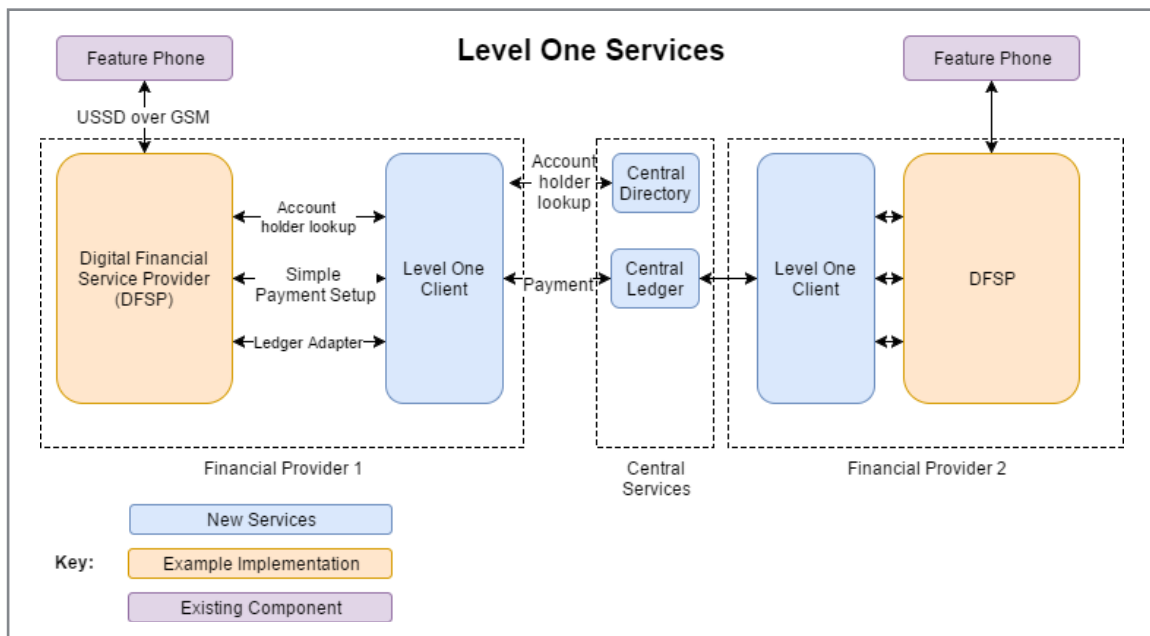
As you can see from the above diagram, Mojaloop (called Level One) would be installed in DFSP systems as an interface to other systems for financial transactions. The Central Directory identifies the destination DFSP for a specific transaction, while the Central Ledger is responsible for clearing and settling the actual sending of funds.

There is also the potential to have shared fraud services to aid in identifying suspicious services.

Designed and built by: Ripple, Dwolla, ModusBox, Software Group and Crosslake Technologies.

Open Source

Mojaloop is open source, available here: https://github.com/mojaloop

BMGF have informed us they are planning to create a new entity into which all the Mojaloop IP will be deposited, with this new entity owning and governing the Mojaloop open source code.

Adopters of Mojaloop

Mojaloop is not intended to be directly adopted by DFSPs. They are looking for other organizations to integrate Mojaloop into their systems, with those organizations selling, installing, and supporting the Mojaloop code. In this document we refer to them as "Adopters".

An Adopter fulfills a couple of key roles:

- **Payment Hub**: Design, build and maintain a payment hub.
- **Payment Software Vendor**: Install, certify and support the interface in each DFSP that connects their system to the Payment Hub.

Opening up Closed Systems

The purpose of Mojaloop is to connect 'Closed' systems together to make them all 'Open'.

A Closed system is easy to build and manage as every aspect of the transaction is controlled by the one organization. Once a Closed system becomes Open, the level of complexity increases by an order of magnitude.

One of the huge challenges in developing countries is it's unlikely the DFSPs will believe the level of complexity until they have experienced it themselves (most likely the hard way).

It is up to the Adopter to take on the role of expert, setting rules and expectations for the DFSPs, and guiding them towards a safe and efficient implementation.

If Clear Purchase Adopted Mojaloop

Mojaloop would be the interface on each end of a connection from a Mobile Money Operator to the Clear Purchase Hub. We would customize the code to fit our specific needs, and then be responsible for installing, monitoring and supporting this modified code.
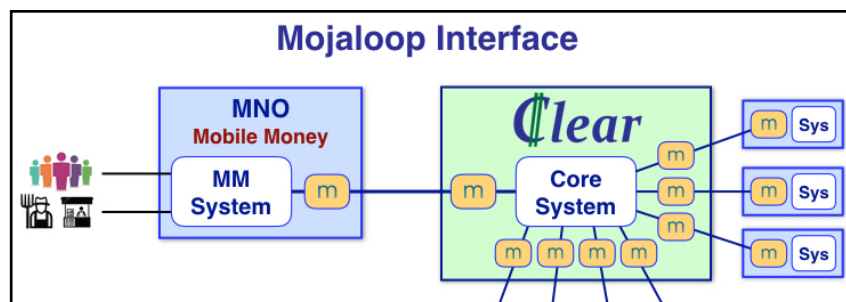
If every system connected this way, it would simplify the connection process for each system as well as the management of each connection.

This would accelerate the expansion of Clear Purchase.

Assessment of Mojaloop

This assessment includes only those aspects of Mojaloop relevant to the decision whether or not to incorporate Mojaloop into the Clear Purchase system.

In general, the work that has been done in the creation of Mojaloop is very impressive. They even encountered a few of the many pitfalls unique to this industry, and dealt with them well.

'Push' Payment Method

Mojaloop is a 'Push' payment method. This is where user A 'pushes' funds to user B, from A's account at DFSP X into B's account at DFSP Y.

Assessment:

Most financial methods here in the West are 'Pull' payment methods, where funds are 'pulled' from a user account. This includes credit/debit cards, checks, and online bill pay. The ACH system here in the US is a both a Push and a Pull method.

Pull methods are inherently risky. For example, when using a credit card you give to the merchant all the information necessary for the merchant to pull funds from your account. This information is shared with several (often around 5) other companies in order to process the transaction. This is the cause of most of the fraud in the West.

Having the basis of a Mojaloop being 'Push' payments is an excellent decision.

Central Directory

This component is responsible for determining the destination of transactions, the core system of a Payment Hub.

A DFSP will send a message to the Central Directory with a destination account identifier, which will respond with the destination DFSP that manages that account. For example, User A with account at DFSP X wants to send funds to User B. DFSP sends message to Central Directory with User B's account identifier. The Central Directory responds with DFSP Y, where User B has the account identified by the account identifier.

Here in the West: Credit/debit cards identify the issuer using the initial few numbers of the card number (the Prefix). Checks use the Routing Code.

Assessment:

This is a security disaster waiting to happen. If hacked into, it would be incredibly easy to commit whole-sale fraud.

Most of those involved in the developing of Mojaloop know this is only intended as a place holder, which the **Adopters would replace or massively rewrite**.

This will become the central service managed by the Adopters, and it is imperative they have experts in this industry to design, build and manage it.

Central Ledger

This component is responsible for clearing and settling the actual sending of funds. It is intended to be real time from one DFSP to another, with same-day settlement.

Assessment

Each country has regulations around the sending of funds, and most have built their own national infrastructure for doing this, for example here in the US it is the ACH system. There are also some international settlement organizations, like Switch. There are also new 'instant' funds settlement systems like Ripple.

The process of becoming an approved 'settler' of funds in a country is onerous, so the recommendation is an Adopter would utilize one or more of these existing systems for settlement.

Funds Transfers & Purchases

Mojaloop is most suited for sending of funds from one user's account to another. This is the simplest type of transaction to facilitate.

A purchase is massively more complex as it is a two-directional transaction with people waiting for it to complete.

Assessment

To have real impact in developing countries, this model must be expanded to accommodate tiny purchases. Mojaloop's suggested flow is mediocre at best, though it is possible to use their foundational structure as a starting point. The onus will be on the ***Adopter to flesh this out so that it facilitates purchases safely and efficiently***.

Transaction Fees

This is left up to the Adopter, as it should be.

Assessment

My biggest concern is the ability to profitably facilitate tiny transactions, especially purchases. The fee charged must be small enough to allow for the transaction, while generating sufficient revenue to make this a viable proposition to all the parties involved.

If the Adopter does not see a viable business model for 20 cent purchases, they will likely limit their business to funds transfers, which are generally less frequent and higher amounts (e.g. bills, loan repayment, sending funds to family member).

The World Bank have set a target fee of 3% or lower for international remittances.

Example here in the US: For credit card transactions most merchants are charged a fee of around 2.5 - 3%, though the biggest are charged 1.5 - 2%. There is also a minimum transaction fee of 20 - 35 cents, which is inconsequential here in the US but would be prohibitive for tiny transactions in developing countries.

Major Concern: Open Source

The strength of 'open source' is the diverse community of users, that share each of their own experiences through an iterative development process. This community can quickly identify bugs and share fixes. In addition, new features can be developed by one user and quickly shared and adopted by others.

A weakness of open source is not all users in the community have the necessary expertise to fully understand potential pitfalls. Nonetheless, where the creative license is broad, the project may benefit from multiple points of view. However, when the project objectives are highly defined from the beginning and the cost of failure is also high, an open source, trial and error, development approach can lead to catastrophe.

Encouraging amateurs to enter the Payment Industry

The payment industry is not the right industry for open source code. This is an industry that requires huge expertise to venture into with any hope of achieving a secure reliable offering.

As open source, those with insufficient relevant experience will believe Mojaloop is a complete and secure system. They are unlikely to add sufficient functionality to create a complete reliable system, and will almost certainly fail to include sufficient security measures.

This is an industry with over $20B of fraud per year, the weakest link in the transaction chain being the target. A Mojaloop system will be much too tempting a target. By adopting an open source development process, Mojaloop is guaranteed to be the weakest link – and because of its central role in the chain of transactions, it will cause the whole system to collapse. A single breach could affect every connected DFSP and all their account holders.

The risks are multiplied as criminal actors could insert security holes directly into the open source code, with it being introduced quickly into almost every system that uses Mojaloop.

Open source code installed onto DFSP servers

If a big Bank here in the US were presented with "we would like to put some open source code onto your servers, which will have direct access to your customers accounts" they would justifiably be horrified and refuse.

The problem occurs with DFSPs who are not Banks, who may not have the depth of experience to fully understand the risks involved in processing financial transactions between systems. They may not recognize the implications of open source code and allow the implementation of Mojaloop onto their servers.

Experts would avoid Mojaloop

Any expert in this industry would recognize the risks inherent in open source code and develop the interface component of their system themselves. Only those with insufficient experience in the industry would consider adopting Mojaloop.

It is important to remember that a potential Adopter fills the role of payment hub as well as payment software vendor, and must find experts in both.

Devastating Prediction

With a fairly high level of confidence, based on my depth of understanding of the payment infrastructure industry, I am making the following prediction:

1. A *Company* without experts will adopt Mojaloop thinking it is a complete and secure system. Their '*Solution*' will be missing important functionality, especially around security.

2. Governments and others are likely to push for the adoption of this *Solution*., especially with promotion by the highly respected BMGF.

3. Some Mobile Money providers in a country will connect to this *Solution*, quite possibly under pressure from the government, micro lenders, or others. They will not have sufficient understanding of the risks of interoperability to appropriately analyze this *Solution*, under the reasonable assumption the *Company* does. Conventional Banks will likely delay until the *Solution* has proven itself.

4. The *Solution* will test well under a limited series of transactions. It is unlikely they will do sufficient error testing, security testing, volume testing or disaster recovery. Everyone will think it is safe and reliable.

5. A pilot *Solution* will go live in a small market within the country. Volume will be low, the inevitable minor bugs will be fixed, and there is unlikely to be any fraud.

6. The *Solution* will go live nationally to great fanfare. It is likely to work quite well initially while volume is fairly low. Word will spread as people see their friends/neighbors use this new *Solution*, and transaction volumes will increasing quickly.

7. Once volumes reach a certain level **the System will become a target** of the bigger criminal entities. It is unlikely the *System* will be sufficiently secure, and fraud will explode. Small amounts of money will be stolen from huge numbers of poor people.

    a. Unhappy account holders will contact their Mobile Money provider asking where their money is. The fraud management costs will be exceedingly high, far more than the Mobile Money provider makes by providing services to these poor people.

    b. The Mobile Money providers will likely reimburse account holders, especially if the government insists they do so.

    c. The Mobile Money providers, as well as the government, will demand the *Company* fix the *System*, though they will almost certainly be unable to do so. They will likely introduce a fraud detection system that will have little or no effect.

    d. Poor people will blame their Mobile Money provider.

8. At a certain point, the Mobile Money providers will pull the plug, and the *Company* will shut down their *Solution*.

    a. The Mobile Money providers will have accrued huge costs and terrible publicity in this 'experiment'.

    b. Everyone pushing the adoption of this *System* will also be blamed.

    c. Other countries will take notice of the devastating results, and will be much more wary of pushing interoperability.

d. Everyone will have known that Mojaloop was the core of the *Solution*. Other systems that utilize Mojaloop will be forced to remove Mojaloop from their system. The Mojaloop brand will have been damaged potentially beyond repair.

9. At some point, a better *Solution* will be built and presented to Mobile Money providers and governments. However, once burnt twice shy! There will now be huge resistance to any new *Solution*.

10. Interoperability, and the Financial Inclusion movement as a whole, will likely be delayed for years.

Recommendation to BMGF

I previously expressed to BMGF my concerns with the Mojaloop code being open source, including the likely results I have described here. They were not swayed.

Protect the reputation of Mojaloop

To succeed in this industry, the right offering will of necessity be one that exemplifies: reliability, security and ease of implementation.

My recommendation to BMGF is they modify their business model to focus on protecting the reputation of the Mojaloop brand:

- BMGF modifies certain 'open source' aspects of Mojaloop. Specifically, an Adopter cannot advertise that they are using Mojaloop unless approved by BMGF.

- BMGF makes sure all Adopters of Mojaloop have sufficiently experienced technical experts in the industry.

- BMGF certifies and monitors Adopters of Mojaloop to ensure sufficient quality standards are met, allowing them to use the Mojaloop name, providing a level of confidence to the DFSPs.

Conclusions

Great work has been put into Mojaloop, and it has the potential to become the default interface for payment interoperability, accelerating the path towards fully digital financial services being available to the poor across the entire developing world.

Unfortunately, their decision to make Mojaloop open source will encourage the less experienced to venture into an industry they do not fully understand with disastrous results for everyone involved. This will almost certainly destroy the Mojaloop brand, and may even set back the entire Financial Inclusion initiative.

It is with regret that we have decided not to adopt Mojaloop.

About the Author: Nick Brown

Nick is a recognized technical expert in payment infrastructure systems, having worked in almost every aspect of the industry.

This includes:

- Implementation of VISA Debit Card System at VISA.

- Involved in writing national (ANSI) and international (ISO) standards for data security for the financial services industry (ASC's X9/F6 working group).

More recently, Nick has written multiple patents on innovative new payment methods, focussed on reducing the potential for fraud, with two being issued so far.

Nick is now founder of Clear Purchase, which is building new financial infrastructure for developing countries, specifically designed for the poorest people on this planet, with the goal creating a truly cashless economy.

LinkedIn: www.linkedin.com/in/nickbrown1027

Clear Purchase: www.clearpurchase.com