Fiat Digital Cash and Financial Crime
- an opportunity for law enforcement agencies to 'follow the money'?

Introduction

Money, bank accounts and payment systems lubricate today's complex economies, providing an ever more convenient set of choices for paying, being paid and borrowing money.

Unfortunately, these same systems also unwittingly lubricate and facilitate financial crime, whether it is laundering the proceeds of drug running or using prepaid debit cards to prepare for terrorist attacks.

Governments and the financial services sector work together through the Financial Action Task Force (FATF) (http://www.fatf-gafi.org) to mitigate the extent to which it is possible for criminals to misuse financial instruments and the banking system. This work stretches back to the 1980s and has produced a series of recommendations that continue to inform relevant rules and regulations in FATF member states.

Any new payment system is highly likely to be exploited by criminals. It is therefore incumbent on any new system to show that it will be no worse – and might hopefully be better – at preventing financial crime.

Fiat digital cash

A class of new payment systems being investigated by Central Banks and others around the world is fiat digital cash. Fiat digital cash products would be quite different from cryptocurrencies, as the digital cash would be denominated in nation state fiat currencies and collateralised or backed by the currency issuer. Each issuer would be regulated in the state within which the currency would be issued and might often be the Central Bank or Mint in that territory.

Fiat digital cash designs broadly fit into one of two categories – account-based or token-based.

Account-based digital cash

Account-based designs would be technically very similar to existing services such as PayPal, Alipay or Venmo. There would be an accounting suite that held balances for all currency holders and a 'payment' would be the debiting of one of these accounts matched by the crediting of another.

Critics of account-based approaches to fiat digital cash argue that they fail two of the key defining features of physical cash and are therefore likely to be rejected by consumers as firstly, not being 'cash' and secondly as not offering much benefit over existing payment choices.

The first feature they lack is that they are not bearer instruments. It is the account holder that enjoys the benefit of the value and any recipient has also to be an account holder to receive value. In the context of global tourism and trade, the need to go through an account opening procedure in order to receive something calling itself cash feels not only impractical but also like a contradiction in terms.

The second feature they lack is privacy and anonymity. When I throw coins into a charity collection bucket I enjoy complete anonymity. When I pay with physical cash in a store for goods I can again choose whether or not to tell the retailer who I am. An account-based approach to digital cash would come with an entity that ran the accounting suite. The risk to the system user would be that this entity, running its business to meet its own corporate objectives, would monitor behaviour and limit the anonymity of the payments across its platform.

Token-based digital cash

Token-based digital cash designs work by creating small digital data files that play the role of 'coins'. These coins would exist outside of any customer accounting framework and can therefore be designed to mimic both the bearer nature of physical cash and be able to provide much of the anonymity and privacy that physical cash users enjoy today.

Critics of token-based digital cash claim that the financial crime risks of such designs are too great and that they should not therefore be launched. While they may bring benefits, such as improving financial inclusion, facilitating the Internet of Things, reducing costs in commerce and trade, these benefits are unproven, the existing world of payments works well enough and therefore the balance of the argument falls against their implementation.

AML/CFT strategies today

Today's Anti-Money Laundering (ALM) and Countering the Financing of Terrorism (CFT) strategies are naturally based on the world of banking and payment systems as it has evolved to date.

It is taken as a given that it is unfeasible to comprehensively track physical cash – it is only possible to attempt to find and/or intercept it – and that the key areas for focus should be the control of account holding, the controls over inter-account transfer and the control of the interface between physical cash and the banking system.

Looked through this lens, it is unsurprising that token-based digital cash solutions look risky! There is no account to open or monitor and, once digital cash becomes embedded in the digital economy, little need for those engaged in financial crime to interact with the banking system. You would simply exchange your digital coins to achieve a value transfer.

This thinking is rooted in the notion that the AML/CFT strategies for token-based digital cash would rely on the constructs used for today's world of notes, coin and the banking and payment systems.

Token-based digital cash is however a completely new concept. It makes sense, therefore, to analyse different specific token-based digital cash designs to see what AML/CFT mitigations they offer, before reaching any final conclusions on the risks they pose.

The Tibado design for token-based digital cash

Each and every new payment system design should be examined on its merits. The authors of this paper are the co-inventors of the Tibado design (https://www.tibado.com) for token-based fiat digital cash. The rest of this note discusses how the Tibado design allows for the creation of a set of extremely powerful AML/CFT mitigation strategies. These strategies are rooted in the specific way the Tibado design works.

We argue that the mitigation strategies available to law enforcement agencies from a Tibado implementation would be inherently safer than those available in physical cash, bank accounts and bank payment cards. This is because, as the digital cash flows through the economy, law enforcement agencies will be able to do exactly what they are unable to do with physical cash – follow the money.

Tibado - digital 'coins' and a central database for each currency

The Tibado design centres on the creation, in a secure environment, of small digital files that act as 'coins' in a particular currency. Each coin has a unique serial number, a currency code and amount field, a time stamp marking their moment of creation and is protected by cryptographic keys that mitigate forgery risk.

Each currency is controlled and managed independently, so that, for example, a USD digital coin could not be turned into a GBP coin.

When created, a complete copy of the coin is sent to the buyer of the coin. A partial copy of the coin is then placed on the central 'Live Coin Database' (LCD) for that currency. To make a payment, a payer simply remits a copy of a coin to the payee.

It is possible for a coin holder to make and send as many copies of the same coin to as many recipients as they wish. In order to gain assurance that a received coin is unspent, it is therefore incumbent on the recipient to present the coin online to the central database, which confirms it as being spent or unspent. If unspent, the centre enables the payee to refresh, merge, split or retire their coin.

The first successful presenter of a coin back to the central database is assumed to be the rightful owner of that coin. Any subsequent presentations of the same coin are met with a 'coin already spent' error message.

Constructing an AML/CFT strategy for Tibado digital cash

Adopting existing FATF procedures

The first element in a Tibado AML/CFT strategy would be to adopt all existing FATF procedures; to the extent they are relevant. The key area would likely be the interface to the banking system. The depositing of digital cash would trigger suspicious transaction reporting procedures much as happens today for physical cash. Any deposit of digital cash would be electronic and would provide immediate information, with no physical bank teller delays. It would also be possible to create automated suspicious transaction exception handling, which would act to interrogate the attempted deposit before the bank account is credited.

AML/CFT within the Tibado world

Monitoring the Live Coin Database

The next element would focus on the central database for each currency. It would be possible to provide a real-time feed of transactions data from the central database to appropriate government agencies. These agencies would receive a complete, time stamped log of all coin activity, complete with the Internet Protocol (IP) address from which the central database had received each coin message.

Working with Internet Service Providers

The IP addresses that the central database would pass on would often be dynamic and might therefore not reveal the identity of the message sender. With appropriate legal mandates, Law Enforcement agencies could work with both fixed line and mobile Internet service Providers (ISPs) to complete their picture of exactly which device, registered to which user (where possible), had initiated a particular message to the central database.

Applying Machine Learning to the data

Law enforcement agencies would be able to employ machine-learning techniques to focus their attention on suspicious activity – in real time – to aid their work. This is a capability that is unavailable in the world of physical cash.

Whitelisting and Blacklisting IP addresses

The managers of the central database would have the ability to block any IP address they wished from interacting with the LCD. Services that act to hide the identity of the message sender would therefore be denied access to check, refresh, merge, split or retire a coin.

A significant incentive to achieve finality

A coin holder only knows their coin is valid when it is checked by the Live Coin Database (LCD). This provides a significant incentive for early coin redemption, effectively minimising the extent to which coins might be exchanged away from any interaction with the centre.

Would such a system still be credible to users as ‘cash’?

A bearer instrument with no account to open

The notion of ‘bearer’ is different in digital, as compared with physical, cash. This is because it is possible to make an infinite number of copies of any digital ‘coin’, while there is only ever one valid copy of each valid issued banknote or coin.

The Tibado design enables any holder of a coin copy to interact with the LCD and achieve immediate finality by swapping, merging, splitting or retiring the coin. This action achieves effective bearer status and completely decouples, from its past, any subsequent use of the value that the coin had held. We believe this will be perceived by users as being superior to the bearer nature of physical cash, as the risk of forgery is fully mitigated by the interaction with the LCD.

Anonymous and private in everyday use

The AML/CFT approach set out above segregates the knowledge available to different system users. In particular, payees only get to see the IP address presented to their receiving computer system. This, in the context, for example, of a merchant Point of Sale (POS) system would normally be insufficient to identify the sender of the coin. Further, unless the merchant also implemented IP address blocking, there would be nothing to prevent the coin sender from using an address shielding service to hide their identity from the merchant.

So payers would be able to remain anonymous with respect to their purchase activity, while law enforcement agencies would still have clarity on who purchased and redeemed each and every coin.

Conclusion and Recommendations

Token-based fiat digital cash is a completely new form of payment system. As implemented in the Tibado design, it enables an AML/CFT strategy, which would allow law enforcement agencies to 'follow the money' as the digital cash was exchanged through the economy, while still preserving existing procedures for monitoring the interface with the banking sector.

The design enables law-abiding users to see their digital coins as bearer instruments and also gives them the opportunity to interact with privacy and anonymity in their relationships with service providers.

Tibado digital cash can be implemented without the need for an issuing Central Bank or Mint to enter the competitive world of payment systems and retail banking. There would be no need for them to provide any customer accounts – their role would be very similar to their current role in physical cash, except that their costs would be significantly reduced.

We believe that token-based digital cash represents a critical piece of the infrastructure of the emerging digital economy. We further believe that a failure properly to analyse and understand the AML/CFT strengths of at least the Tibado design is preventing society from realising the benefits that fiat digital cash could deliver.

We would like to issue a challenge to banking and payment system experts. Is token-based fiat digital cash really an AML/CFT risk too far? Which of our arguments lack merit and what might be the nature of the real residual risks in a Tibado implementation?

This work would help inform debate with policy makers and lead to a period of experimentation in advance of the launch of a publicly available fiat digital cash service.

Tim Jones CBE and Dr David Everett **June 2018**