PAYMIUM

ESMA Call for Evidence - July 2015

The European Securities and Markets Authority (ESMA) has launched a call for evidence on investments using virtual currency or distributed ledger technology.
ESMA is seeking information and views from stakeholders on new developments in how virtual currency technology is used to issue, buy and sell and record ownership of securities. ESMA would like to hear from all those involved: whether from existing financial institutions, new start-ups or their technological advisers, and issuers and investors.
ESMA is interested in how different virtual currencies and the associated blockchain, or distributed ledger, can be used in investments. There are now facilities available to use the blockchain infrastructure as a means of issuing, transacting in and transferring ownership of securities in a way that bypasses the traditional infrastructure for public offer and issuance of securities, trading venues like exchanges and central securities depositaries or other typical means of recording ownership. ESMA would like to find out more about these market developments and in particular to know to what extent the use of the blockchain could enter the financial mainstream, and how it could be used.
All contributions should be submitted online under the heading Your input - Consultations on ESMA's website. The consultation will be open until 21 July 2015.
2015/532 Call for evidence - Investment in using virtual currency or distributed ledger technology.

Foreword about “virtual currency”

In the dictionnary of Computing, the adjective virtual is defined like so:
“1. Common alternative to logical; often used to refer to the artificial objects (like addressable virtual memory larger than physical memory) created by a computer system to help the system control access to shared resources.
2. Simulated; performing the functions of something that isn't really there. An imaginative child's doll may be a virtual playmate.
Opposite of real or physical. “

The world “virtual” is used by the ECB as a substitute for “digital”.
In particular, the use by ECB of the phrase “virtual currency” suggest that some currencies would be real (the Euro for the ECB which is sponsoring the EURO as the sole currency available to Euroepan citizen) while some others, like Bitcoin, would not be real.
In fact, the Euro is largely a digital currency and could therefore be deemed as “virtual” if we were to follow the ECB’s deliberately flawed logic.

Likewise, the use of “crypto-currency” suggest that some currencies would be using more cryptographic processes than others: again the Euro is using cryptography extensively, even more so than Bitcoin. A bank card transaction (in Euro) utilize in fact more cryptographic processes than a bitcoin transaction.

In short, the only distinguishing feature of Bitcoin is the decentralized network architecture enabled by the Bitcoin protocol.

Hence I recommend “decentralized currency” as the correct phrase applicable to Bitcoin while centralized currency” or “fiat currency” can be used to categorize the Euro or other traditionnal currencies.

About decentralization

Evidently, the level of decentralization of the Bitcoin network enabled by the protocol ruling the network participants is constrained by external market factors favoring centralization like the capital intensive nature of professionnal mining. Decentralization, like freedom, does not exist in an absolute form but is relative to a defining context.
The same “relative “ decentralization can be observed on other networks ruled by open source, free software protocols. For instance, it can be argued that the email network (mainly ruled by the SMTP protocol) is dominated today by Google and Microsoft, yet anyone can run his/her own email server to balance the effects of such market concentration.

At the heart of the technological breakthrough achieved by Bticoin is the resolution of the “Byzantine generals problem”: reach a multi-party consensus (between the miners about the state of a shared ledger) without the need for the parties to trust each other.
More precisley, the participants can trust the network as a whole rather than any particular miner.
From a historic perspective, for a long time, banks were suspicious of the Web as an open network enabling online banking services until the development of https and accompanying certificate authorities made it possible to roll out such services.
With Bitcoin, there is no need for certicicate authorities and PKI: unlike the http protocol, the Bitcoin protocol is secure by design and so is the Bitcoin network.

About scalability

Many variants of the Bitcoin protocol have been proposed that weaken the security of the protocol by giving special powers to a central organisation (e.g. Ripple, Inc) or by reducing the protection against centralization (e.g dual-purpose mining in Permacoin).
Some proposals based on Proof of Stake in lieu of Proof of Work reduce drastically yet implicitly the level of security achieved by the network with the explicit objective to reduce its energy consumption.
The multiplication of these variants is a particular case of the Tragedy of the Commons once described by Garett Hardin: I call it the Babel Tower fallacy.
The web would not be what it is today if every company or site had developped its own flavor of the HTTP protocol.
Likewise, the Bitcoin network would not develop its full benefits to the economy if everyone was using his or her own dialect.
The so-called altcoins are a short-sighted way to solve a scalability problem that does not exist yet.
There are much smarter solutions to gradually scale the capacity of the network, notably offchain compensation transactions (happening already), increased block size (debate in progress) and sidechains (work in progress).

Asset registry and Blockchain

There are many ways for financial services to harness the potential of Blockchain technology yet many wonder how to get the most benefits with the least disruption to their organization and processes.
To identify the best use case candidate I would recommend to consider the Blockchain for what it is: a shared, secure ledger offering ubiquitous, open access to data records at the minimum cost.
The Bitcoin blockchain is a new IT infrastructure available for all stakeholders to leverage its potential. By doing so, they will be able to cut down on IT capex and opex while adding new functionnalities to their portfolio of services.

Because the blockchain is not encrypted (contrary to what some ill-informed people might say) and offers a ubiquitous, open access to data, an obvious application is the asset registry that custodians, securities service providers, traders and asset managers rely on to find reliable information about available assets.
A private company stock or a peer-to-peer loan would become much more valuable if an open access asset registry made them available for trading as stocks or bonds via a secure API.

There are at least both technical solutions worth considering, both built on the Bitcoin blockchain: sidecoins, factoids and colored coins.
Let’s describe briefly how the asset management processes unfold with each solution.

Sidecoins

Some bitcoins (say 10 BTC) are transfered to a dedicated sidechain where
each 1/100 000 fraction of a sidecoin represents a unit of a registered asset (say a share of ABC, Inc.). Because ABC, Inc has signed and published the transfer transaction to the “ABC” sidechain as well as its number of outstanding shares (1 million shares in our example), everyone can trust that 1000 satoshis of a sidecoin represent one share of the company.
The requirements set on the ABC sidechain are vastly different from those set on the Bitcoin blockchain with respect to mining, fees and transactions. Mining may not be required because no new coins are generated on the sidechain (all the sidecoins are transfered from the blockchain to the sidechain). There may be no need for mining fees. Transfer of sidecoins must be atomic, i.e not split a company share unless a stock split is decided by the company shareholders as a corporate action. In short, the sidechain will run with a specific protocol and sidechain specific wallets will be used on the sidechain.
Sidechain specific wallets must be aware of some Bitcoin unspent outputs as well as store the sidechain unspent outputs.
The main benefit of the two-way pegg binding the sidechain to the Bitcoin blockchain is to ensure the security of the initial transfer transaction with the perennial Bitcoin blockchain.
Another benefit of using a sidechain for each asset class instance lies in the possibility to store transaction metadata directly in the sidechain, not causing a blockchain bloat.

Colored coins

The colored coin protocol is an application layer built on top of the Bitcoin protocol based on the same principle of using a shared ledger to store records of offchain transactions denominated in a non-bitcoin unit. Typically, a stock issuance, stock transfer of ownership, etc..
Company ABC, Inc would be using directly the Bitcoin blockchain but metadata binding the Blockchain transaction to the offchain transaction would need to be stored in a more suitable yet decentralized network such as Bittorrent.
The data storage network cannot be a private network because that would defeat the purpose of leveraging a shared infrastructure.

The Factom and Conuterparty projects also deserve attention of any organization considering the development of blockchain-based asset management solutions.
For instance, Key Investor Information or Simplified Prospectus documents could be encrypted, stored and retrieved through a Factom server or from a Colored coin client. Each registered document would be stored on a Bittorrent network.
The powerful combination of Bittorent technology for storage and Blockchain technology for secure indexing and timstamping will bring about the most benefits to end users and their financial insitutions.

To sum things up, the design of an open access, secure asset registry based on blockchain technology holds the promise of significant IT cost savings for custodians, investment banks, traders, asset managers and other economic actors of financial markets.
At the same time, such public asset registry would open up new market opportunities for small caps, privately held companies or small to medium size projects that could issue securities (stocks or bonds) with industrial grade trading tools that are currently unavailable due to the absence of an easily accessible registry.

As a first learning step, Paymium recommends that ESMA draft a specification with end users in parallel with the commissioning (agile development, continuous deployment) of a Proof of Concept (PoC) platform allowing professionnal end users to become more familiar with the technology in the context of their day-to-day oeprations. Initially, the PoC could be applied to a single asset class so that first results could be derived early in the specification process.
Paymium, established in 2011 as one of the world's first Bitcoin startup, can bring the experience and Blockchain expertise of its team to new developments applying Blockchain technology to securities services and asset management.

Pierre Noizat
Co-founder and CEO of Paymium

About Paymium

Founded in 2011, Paymium is pioneering the European Bitcoin space, with 60 000 European customers.
Paymium is the company behind the Paymium Bitcoin exchange, offering a secure, reliable, high-performance trading platform in compliance with European regulations.
Paymium also offers merchant solutions to accept payments in Bitcoin with instant conversion to Euro, for European merchants.