INTESA SANPAOLO

International and Regulatory Affairs Dept.

ESMA Call for Evidence
Investment using virtual currency or distributed ledger technology
ESMA/2015/532
July 2015
TRANSPARENCY REGISTER N° 24037141789

Introduction

Intesa Sanpaolo (ISP), one of the largest European banking and financial groups, aims to be at the forefront of financial innovation.

To achieve this objective the Bank set up the Innovation Area, led by the Chief Innovation Officer, with the aim of: 1) Scouting of new trends ideas and new solutions; 2) Supporting innovative enterprises growth (e.g.: equity stakes, seeds financing, etc.); 3) Training on innovation / building innovation culture; 3) Overall coordination and planning of the innovation initiatives undertaken by the Bank.

This Area is performing in depth research on virtual currencies and block-chain technologies. Through its dedicated task force, Intesa Sanpaolo is also implementing cryptofinance projects integrating them with its strategic vision about the evolution of the financial services industry.

Intesa Sanpaolo is grateful to ESMA for the opportunity to contribute with its experience to the analysis ESMA is currently carrying on virtual currencies and the related investing products and platforms.

Key messages

The Bitcoin protocol is a medium to transfer bits of information, based on digital tokens.

Its relative young age and the extreme malleability it has shown so far makes it safe to assume **its potential is far from being fully explored** especially as a mean to transfer rights and value in a very secure way.

For the Bitcoin protocol to function as a mean to manage and transfer rights, each token (or its fractions) need to be **"marked" with a bit of additional information**.

As of today, in the market there are various solutions to implement this functionality: apart from being extremely complex from a technological standpoint, such solutions are typically not interchangeable and in rapid, ongoing evolution. On this subject, ISP suggests the following:

- **ESMA should provide** high level **guidelines and recommendations** about the entwining of tokens and rights, **leaving to the competitive market the selection of the best technical solution**.

It worth noting that the management of tokens entangled with value/rights can be performed with or without intermediaries:

a. Without intermediaries each user holds and manages its tokens with full and incontrovertible autonomy, generally through dedicated software;

b. With intermediaries - custodians - hold and manage tokens on the user's behalf, making the technology accessible to inexperienced users, but introducing a counterparty risk otherwise not encompassed in the system

Therefore, Intesa Sanpaolo suggests that ESMA distinguish between the two solutions and propose guidelines and recommendations posing special attention to the final user's safety.

General observations

Since the Call for Evidence invites stakeholders to provide information on all matters raised in the Call for Evidence, and not just on the specific questions of Annex 1, we would like to start with observations concerning the paper in its general terms.

O 1: "Virtual Currencies": a terminology problem

- We would like to stress that the definition "virtual currency", although now very common, is largely inappropriate when describing Bitcoin and other blockchain-based value transfer systems for the following reasons:
  - First, the key aspects of the modern wave of digital tokens over centralized ledgers is their mix of decentralized and "mathematical" or "cryptographic" based approach: their specific characteristic is not being "virtual", like most of traditional monetary instruments indeed are today, but rather being decentralized, based on distributed consensus and not dependent on a central intermediary or issuer.
  - Second, the vast majority of those value tokens are not, strictly speaking, "currencies". They are not recognized as such by most of the institutions and they do not have at full capacity all the properties traditionally attached to money (means of exchange, store of value, and above all unit of account, a function still not performed even by the most evolved of said systems, the Bitcoin network).
- Considering the two previous points, one could suggest, as a better definition, something like of "limited supply digital entitlement", "digital scarce asset" or "mathematical commodities", rather than "virtual currency". On the other hand, the expression "distributed ledger technology", often used in the Call for Evidence, is accurate and unambiguous, being the exact technical definition of the structure such digital tokens are based upon.
- Even adopting a more accurate linguistic choice, we believe it could be misleading to assume the existence of a vast system of competing and equally powerful distributed ledger technologies for the issuance, the storage and the transmission of limited supply digital tokens. Despite what may be the common perception, distributed ledger solutions are not all equal, and in particular there is a huge difference between Bitcoin and all other solutions. The same way TCP-IP imposed itself as the main protocol in the early days of the creation of internet, and no other (even better) protocol could develop enough network effect to overcome it ever since, so Bitcoin is the first and the most important of "Internet of Value" protocols, and there are high chances that it can establish itself as a global standard, as it leverages at least four powerful network effects: Bitcoin network has by far the largest hashing power (and so the greatest security), the higher capitalization, the largest user (and merchant) adoption, the best and largest developing and maintenance effort around it.
- All that said, it seems like the expression "Virtual Currencies" is now common in institutional analysis about Bitcoin and Bitcoin-like technologies, such as "EBA Opinion on Virtual

Currencies". Therefore, to preserve intelligibility, in the following we will keep referring to distributed ledger technologies and "mathematical commodities" with the "VC" acronym used in the Call for Evidence.

O 2: Benefits and risks of VC investment products

- To integrate on the question on the benefits and risks of VC based financial assets/securities (Q 8) we would like to comment on the specific topic of benefits and risks of VC investment products.
- We agree that the main benefit of VC investment is that it enables investors to participate in the performance of a market without needing to hold VCs directly, and we would like to elaborate about the main disadvantages of directly holding VCs and about drawbacks in using VC investment products. We identify these disadvantages in 3 major categories: technical difficulty, market difficulty, legal difficulty.
    - Technical difficulty is related to technological entry barriers that the investor has to overcome to directly manage VCs: the choice of a suitable wallet provider, the creation of a personal wallet, the secure storage of private keys or seeds, the monitoring of transactions and the grasp on confirmation mechanisms (unlike with traditional trust-based financial assets, in the case of loss of private keys or seeds of a VC wallets, there is no intermediary able to help recovery, and in the case of fraud or theft no intermediary can cancel or reverse confirmed VC transactions. Intermediaries can be built on top using escrow multi-signature mechanisms.
    - Market difficulty is related to the very early stage of VC markets and their limited liquidity: even the biggest VC market cap, the Bitcoin one, is just over $ 4 billion in its entirety. Obtaining VC in substantial quantities is currently still very difficult, requiring knowledge of many exchanges, strong KYC/AML on a large number of them and the ability to deal with the order books without excessively penalizing the purchase price.
    - Legal difficulty is related to the regulatory complexity related to direct possession of these tokens: a VC investor has to manage tax, legal and fiscal accounting in an ever-changing and often unclear regulatory environment.
- On the other hand, we think that the main drawback in using VC investment products, as opposed to direct VC possession, is the counterparty risk associated with the platform (especially in an environment which is still immature and unclear).

INTESA SANPAOLO

Questions

Q 1: Do you have any further information about any other VC investment product or platform distributing VC investment products, their location or size outstanding/volume?

- Pantera Capital, an investment firm focused exclusively on Bitcoin, other digital currencies and companies in the space, since at least 06/10/2014 has had 3 bitcoin vehicles (CIS) with various exposure to bitcoin for potential investors to the VC: 1x, 0.5x and 0.2x (respectively 0X, 0.5X and 0.8X exposure to US Treasury bills).
- Kraken and Bitfinex, two of the most famous bitcoin exchanges, has recently introduced margin trading. Also OkCoin, one of the biggest exchanges in China with zero trading fees, has (optional) 10x and 20x bitcoin leverage on trading.

Q 2: Do you have any information about the profile of investors investing in VC investment products?

- We believe that the expression "retail investors" in the second half of paragraph n°10 does not fully represent the complexity of users of VC derivatives. We believe that given the heterogeneity of geographies and legislations and the wide "grey zone" in terms of regulatory obligations, it is highly probable that, beyond traditional accredited investors, there is a proportion of non-accredited individual investors that we are currently unable to quantify.

Q 3: Do you have anything to add or suggest a change to the description (paragraphs 15-18) of how virtual currency distributed ledgers work? Please clearly state to which virtual currency you are referring in your answer or whether your answer refers to virtual currencies in general.

- In paragraph n. 15 there are two incorrect sentences:
    - The first is: *"Whenever anyone completes a transaction involving a VC this transaction gets logged in a block".* Here is a more accurate description of the process: whenever a transaction gets completed, the user (or the software he is using) attempts propagation via his connected nodes (which may or may not reject it and may or may not further propagate the transaction). Once the transaction hits one or more miner nodes, miners may decide to include it or not include it, based on its own internal policies and based on the current state of the network (if an influx of transaction with higher fees is available the miner may decide to never include the transaction). Only when one of the miners includes the transaction and finds the solution to a block validation puzzle the transaction is said to be logged in a block. The set of unconfirmed transactions is called "memory pool" or "mempool".
    - The second is: *"Every time a block gets completed a new block is automatically generated."* Even the least powerful miner attempts millions to billions times a second to create a new valid block. The super large majority of attempts fails. Once one of them generates a valid block, it attempts to propagate it to the network, at which point it may get accepted or it may compete with a block found by other miners. Other blocks will be eventually generated through mining, but that's neither automatic nor instantaneous.
- In paragraph n.16 there are 2 potentially misleading sentences:

- The first is: *"When the solution gets broadcasted this validates the transactions contained in the respective block. This normally takes around 10 minutes."* It doesn't take 10 minutes to propagate or to validate a block. Propagation is very fast, up to a few seconds (depending on the network speed), and also validation by nodes needs to happen very fast, in the order of seconds. The 10 minutes interval is only an average that the network targets for the creation of new blocks. Every attempt to form a block has the same probability of success and the number of attempts per second is roughly constant.
- The second is: *"With bitcoin the recommended confirmation time is 6 blocks, i.e. around 1 hour."* Actually, the number of confirmations required is not fixed: it is dependent on the amount being transferred and the risk people are willing to take also varies. For instance merchants accepting Bitcoin for small purchases may want to wait 0 (unconfirmed insecure) or 1 confirmation, while transferring relevant Bitcoin amount (worth millions of Euro) may warrant 30 confirmations or more.

- We would like to stress the relevance of the first sentence in paragraph n.16. The incentive structure (mining rewards and transaction fees) for preserving the network is the key element of the Bitcoin architecture and more generally a vital element of decentralized public ledgers. Without the economic incentives for miner nodes, update and continuous maintenance the architecture will not be sustainable. In the case of the Bitcoin protocol, the assumption stated in this paragraph about the dimensions of the transaction fees ("small") has to be regarded as fundamentally correct with respect to present time, when the main part of the costs of the network are borne by VC holders in the form of "inflation fees", and not on VC users transacting in the form of transaction fees. However, this is going to change inevitably as block rewards gradually decreases by halving every 4 years, leading to two possible scenarios: a) a vast number of transactions included in blocks, each with a relatively small fee, or b) the need for high fees associated with a relatively small number of transactions included in blocks. The likelihood of the latter should not be underestimated, especially given the recognized problems of scalability of the Bitcoin network in its current state[1].
- We would like to point out that, unlike Bitcoin's Proof of Work method (which, as stated in O 1, we regard as the only effective one, at least at the moment, because of the computational power dedicated to it), other decentralized double-spending prevention algorithms, like NXT's Proof of Stake (PoS) presented in paragraph n.17, are still not validated from both a theoretical and an empirical point of view:
  - There is an ongoing debate over the "Nothing at Stake" problem affecting every system which doesn't use any consumption of resources external to the system for the validation[2];
  - Every single existing PoS scheme, NXT included, is actually relying on some kind of centralization in validation checkpoints, in "currency" ownership or in nodes distribution.

[1] https://en.bitcoin.it/wiki/Scalability

[2] https://halshs.archives-ouvertes.fr/halshs-00945053/document http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2393940 https://download.wpsoftware.net/bitcoin/pos.pdf

Q 4: Do you agree with the general investment process in VC based financial assets as described above (paragraphs 19-24)? Please explain where this process could differ for different virtual currencies.

- As stated in O 1, outside the case of centralized fiduciary digital titles, there is no real interchangeability between protocols operating independently from the Bitcoin block chain and protocols leveraging the Bitcoin block chain. PoW effectiveness of independent block chains is proved to be very low at the moment (very low hashing power), and such is the security of these systems. Viable alternatives to PoW are still theoretically and empirically unproven (cf. Q 3). We would therefore suggest focusing the analysis on systems leveraging the Bitcoin block chain security, even in the case of VS-based asset/securities, also called "cryptosecurity"[3]. Currently, we can identify three main technical strategies to issue and transfer asset/securities leveraging the Bitcoin block chain: colored coins, counterparty protocol (with omni-protocol/mastercoin), and sidechains.
    - Colored Coins[4] are a set of methods for representing and managing real world assets on top of the Bitcoin block chain, by using actual bitcoin transactions. These assets inherit the same intrinsic security of underlying "white" bitcoins. The main advantage of this methods are: the absence of any intermediate currency between bitcoins and assets; a very simple, dedicated core protocol, directly based on Bitcoin, easy to assess with regards to security and correctness; a straightforward compatibility with many of the advanced or upcoming Bitcoin features, such as multi-signature, contracts and payment channels. On the other hand, these methods appear to have scalability limitations and may 'bloat' the blockchain if used more widely. Transactions depend on underlying Bitcoin transactions and inherit its transaction fee costs and its confirmation time.
    - In some ways similar to Colored Coins, Counterparty[5] and Mastercoin/Omni[6] protocols allow for a method for representing and managing real world assets on top of the Bitcoin block chain. They also promise to allow P2P trading of assets in a decentralized fashion, as well as smart contracts and oracle feed services. Both suffer from the limitations of Colored Coins and some more, like the need for a specific native "middle-coin" to use the protocol. Mastercoin has been rebranded Omni after bad reception and many technical woes, but still benefits from the fact that some interesting experimental services have been based or still are based on it (Maindsafe, Tether, Factom). Counterparty has been the subject of much attention for news about a possible use by Overstock[7] for the issuance of crypto-securities, but there seems to be no follow up.
    - Sidechains[8] are fairly different from Colored Coins: Sidechains rely on Bitcoin block chain security, but users transaction are not on the Bitcoin block chain, they are instead on a separate block chain which is "merge mined", a process that allows the separate chain to be secured by Bitcoin miners. This method appears to have better scalability properties than the alternatives and allow for more innovation.
- However, many project for asset/securities on distributed ledgers independent from Bitcoin are noteworthy, even just for innovative ideas and experiments that they enable, if not for

[3] https://www.o.info/How_to_issue_a_cryptosecurity
[4] http://developers.coloredcoins.io/hc/en-us/articles/203062871-ColoredCoins-Presentation
[5] http://counterparty.io/docs/about_counterparty/
[6] https://github.com/OmniLayer/spec
[7] http://www.coindesk.com/overstock-hires-counterparty-developers-build-cryptosecurity-stock-exchange/
[8] https://github.com/ElementsProject/elementsproject.github.io

the real possibility to use them in production environments. For instance, Ethereum[9]'s team is trying to decentralize computation and create a universal platform for user generated contracts and applications: the code of smart contracts is directly stored in the Ethereum's blockchain and a digital token called Ether is used to pay transaction fees and contract execution fees.

- The process description in the paper assumes an asset exchange separated from the VC platform. That could be the case in some application, but we think that many of the advantages of VC-based asset/securities are related to the possibility of directly using the underlying technology to exchange two kinds of assets, or bitcoins with assets, in a trustless, secure and automatic way (atomic swaps).
- Even if the scenario described in paragraph n. 20 is definitely the most common right now, there is often no intrinsic reason why the user/investor should go through a VC exchange in order to acquire VCs, before he can buy VC-based assets/securities. The need for an intermediate VC between fiat money and VC-based assets/securities is usually due to two reasons: it could be a technical requirement for the use of certain platforms (like with Counterparty's XCP, Ripple's XRP, Omni's MSC; although the actual technical need for these intermediate coins is doubtful: in many cases they are thought to be just attempts to somehow monetize founder's efforts), or it could be a way to engage in anonymous or anyway unofficial asset/security markets, where fiat payment could result problematic. If we imagine a technical solution without intermediate coins (Colored Coins implementations, Sidechain assets, etc.) and we leave out legal considerations (the legal challenges a "fiat vs. VC-based assets" exchange would face are not so different to those now faced by "fiat vs. VC" exchange), direct purchase of VC-based assets/securities with fiat currency is a straightforward possibility[10].
- Moreover, paragraph n.20 states that VC purchases happen in two ways: either online or using a VC ATM. There is indeed also the option of a direct vis-a-vis purchases via cash, using direct communication with a vendor, or public forums, or tools like Mycelium Local Trader[11] and its alternatives. One cannot exclude a development of these p2p exchange tools in order to make possible, in the near future, even the direct vis-a-vis exchange of cash against VC-based assets/securities.

Q 5: Which VC based financial assets exist other than the broad categories mentioned (paragraph 24)?

- It is likely that VC-based financial assets should, at least in an early phase, mimic as closely as possible the economic and legal rights of existent fiduciary assets, so as to reduce regulatory friction and increase familiarity in investors, but this kind of technology could bring to life new, complex and exotic types of asset/securities. This is still a young sector, in full development right now, and many of the application will become more clear when there will be disclosure of the results of NASDAQ experimentation with the Open Asset protocol, or first application of assed sidechains. With the provision already mentioned in O 1 and in Q 3 about the technical improbability of a functioning, safe and broadly adopted VC-based asset/security platform not leveraging the Bitcoin block chain, in order to examine the current situation, we have to look at decentralized asset exchanges now running over protocols such as NXT, Ripple, Veritaseum[12] and BitShares[13]. On these

[9] https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf
[10] https://www.lamb-cooper.com/qib/
[11] https://mycelium.com/lt/help.html
[12] http://veritaseum.com/

protocols, the main existing different kinds of assets are revenue sharing agreements, tokens representative of voting rights, and tokens representative of liquidation preferences.

Q 6: Do you agree with the analogies to traditional regulated entities as outlined (paragraph 25-32)? Please explain where you have a different opinion, including where the analogies are different for different VCs.

- Comparisons in paragraphs n. 26, 28, and especially 29 and 30 are not trivial, cannot be taken to logical consequences and could be questionable from different points of view. For example, the comparison of a coin developer to a central bank is misleading: the former cannot control the supply anymore after the open source software is gone public and is running on a distributed network of nodes and miners. Neither the developers nor the nodes nor the miners can be compared to central banks without implying a breach in the laws establishing a legal monopoly on money currently applied in almost all jurisdictions.
- Most types of wallet providers, in particular, cannot possibly be compared to safe-deposit box providers or saving accounts, as stated in paragraph n. 27. Indeed, leaving out fiduciary "wallets" as Coinbase which actually store users' bitcoins on their behalf, the vast majority of bitcoin wallets are just software running locally on users' devices, facilitating (and in some cases enhancing) the management of balances and transactions on the block chain. Unlike a safe-deposit box provider, a trustless bitcoin wallet is technically unable to freeze or confiscate users' funds, even under explicit request from legal authorities.
- The question of enforceability of ownership rights created via a block chain is crucial and not trivial. There is a *de facto* "technical enforcement" which holds so far as the security of the block chain is granted (only the owner of the private keys or seeds is technically able to move funds associated with his addresses) and which could be translated to VC-based assets in such case as smart-property[14]. Legal enforcement, on the other hand, is much more complex to address. We think that the definition of ownership rights for block chain based asset is a non-trivial problem, with different solutions for different platforms and technology implementations. We are still living an "infrastructure building" phase and the technological substrate is prone to change and evolution. Therefore, there are still several legal challenges in order to structure and connect traditional legislation regarding ownership and the new systems created with blockchain technologies. It is highly probable that regarding purely bitcoin-based assets there will be an international process of regulatory convergence, partially oriented by the "Bit-License"[15] and other future-oriented regulatory experiments, but there is a whole universe of possible applications of block chain based technologies that will require further work and imagination from the legislators. A specific debate on blockchain-related ownership legal issues was performed in January 2015 at MIT with people from Harvard Law School, the Harvard Berkman Center for Internet and Society and some of the startups working in this area (i.e. Swarm). According to our knowledge, a book about the legal issues related to block chain technologies, including advanced research in ownership rights and in cryptosecurities, will be published by Harvard University Press.

[13] https://bitshares.org/technology/
[14] https://en.bitcoin.it/wiki/Smart_Property
[15] http://www.dfs.ny.gov/legal/regulations/revised_vc_regulation.pdf

Q 7: Do you have more evidence on how widespread ownership of VC based financial assets/securities is? Please mention your sources.

- More information on the structure and dynamics of the bitcoin network and other virtual currencies could be obtained through aggregators like CryptoAsset Charts[16] and Coinist[17]. Nevertheless, the general perception is of a sector still in its embryonic phase. The most used technologies, at the moment, are not well suited to ensure safe, reliable, production-ready distributed asset exchange systems, and most promising technologies (sidechain assets, colored coins) are still not used outside tests and experimentations.

Q 8: Do you agree with the assessment of benefits and risks of VC based financial assets/securities or are there other benefits/risks for investors, for other market participants, and for the financial system as a whole?

- In paragraphs n. 34, 35 and 36, the main benefits of VC based financial assets are identified as "speed and cost". This is only partially accurate. In comparison with centralized databases, block chain based financial contracts and assets are not necessarily more efficient in terms of cost and speed: often the opposite is true. Centralized systems can be really instantaneous (instead of 10 minutes average for the first transaction validation) and are much cheaper than distributed ones. This last point is often missed because of lack of understanding of the economic incentives of distributed systems: its huge security cost is usually coved by socialized seigniorage revenues, paid by asset owners through implicit inflation. If and when seigniorage revenues will not be enough to cover the costs the emergence of fee-based transaction will be inevitable. The real advantage of distributed systems is all about their anti-fragility and trust-less capabilities. Where speed and cost seem to be an intrinsic characterization of VC, as in the NXT case, we are not usually really looking at a distributed system of consensus. In those cases high speed and low cost are achieved requiring some degree of trust between different parties.
- There could be other benefits, apart from speed and cost: block chain based digital tokens are "irrevocable and self-enforcing" promises. Their main benefit of VCs is their potential to be independent from central "trusted" issuers, partially of fully decentralized (therefore safe from the failure of a single node or a small group of nodes), cryptographically safe, automated and self-enforcing.
- We agree that the risks of VC-based financial assets/securities for investors consist mainly in the risks associated with underlying VC tokens (cf. O 2). Unless we are considering smart-properties, or self-enforcing titles in smart-contracts, anyway, there is also a substantial counterparty risk related to the issuer: investors could buy, store and transfer tokens representing IOUs or company shares safely on the block chain, but there is no technical assurance that the issuer will respect the rights contractually associated with said IOUs or shares.
- We agree on the assessment of risks of VC based financial assets/securities for current financial and payment system operators: there could be an industry disruption similar to the ones witnessed with the diffusion of mp3 file sharing to the detriment of traditional music records, or with e-mail adoption to the detriment of traditional postal offices. These risks would though only materialize if adoption becomes significantly widespread.

[16] http://www.cryptoassetcharts.info/
[17] https://coinist.co/

- Another potential risk could be identified: that of an infrastructure failure. Block chain protocols are still vulnerable to systemic failure, especially the alternative, untested, non-Bitcoin block chains, which have to prove their stability, security and scalability potential.
- Still another risk, although not specific of VC-based assets/securities (and indeed very common also outside of the VCs space), is that of asset bubbles: as it happened in 2013, the evolving technology of VCs could generate hype cycles and bubbles, and it is impossible to exclude that bubble might be generated for non-bitcoin crypto-asset. Nevertheless, such scenarios did not prevent the long growth run of the block chain technology space, similarly to what has happened with the 2000-01 bubble and crisis that did not stop the evolution of the Internet economy.

Q 9: How is distributed ledger technology being used or likely to be used in relation to the issuance, distribution, trading, recording of transactions and ownership of 'traditional' securities or investment products and why?

- Traditional financial instruments, such as insurance contracts, bond and derivatives could be implemented on distributed ledger technology. Several startups and digital infrastructure projects are now exploring how to implement this form of financial / legal technology. Anyway, none of these efforts have led to definitive, usable and market-ready solutions. The experimentation is just beginning. The concept of "smart contract"[18], although very broad, is one of the most interesting ideas this rising industry is testing (cf Q 10).

Q 10: To what extent is the use of distributed ledger technology in relation to 'traditional' securities or investment products being separated from an associated virtual currency and, if so, how and why?

- A new wave of assets that can be issued, stored and transmitted using distributed ledger technologies could be linked to smart contracts to become carriers for financial contracts, also in case of "traditional" underlying assets. Smart contracts are creating an enormous opportunity to manage high-value information, with potential applications from notary services to voting systems, from insurance to ownership structures. There are significant potential applications in the financial services industry, especially in bond trading and OTC (Over-The-Counter) derivatives. A very interesting application is the field of decentralized prediction markets, of which Augur[19] is an early example. As stated in Q 4, there is no technical need for associated "currencies to use these kinds of asset", even using the term in the broad sense of "liquid, tradable, stable and highly divisible commodities". There could be also many cases in which a smart contract is not associated to a digital asset at all: they could just be self-enforcing computer programs related to financial variables external to the system.

For more information please contact:

Francesca Passamonti	Head of European Regulatory and Public Affairs	Francesca.passamonti@intesasanpaolo.com
Ferdinando Ametrano	Senior Quant Banca IMI	Ferdinando.Ametrano@bancaimi.com
Raffaele Mauro	Innovation manager	Raffaele.Mauro@intesasanpaolo.com

[18] http://szabo.best.vwh.net/smart_contracts_idea.html, http://szabo.best.vwh.net/smart_contracts_2.html

[19] http://www.augur.net/