Virtual currencies and blockchains: potential impacts on financial market infrastructures and on corporate ownership

Paola Fico

Executive summary

Virtual communities have proliferated in recent years – a phenomenon triggered by technological developments and by the increased use of the internet and it is considered one of the most powerful innovations in finance in 500 years. After an initial enthusiastic phase, a trend change is underway. The most famed virtual currency known as Bitcoin is only six years old, and many of its critics are already declaring it dead. But such dire predictions miss a far more important point: whether bitcoin survives or not, the technology underlying it is here to stay (so called blockchain or public ledger currency platforms). That technology will become ever more influential as developers create newer, better versions and clones.

Part 1 of this paper aims to provide an analysis of this relatively recent phenomenon of virtual currencies to offer a description of its current definitions, its historical background and key attributes. It attempts a comprehensive approach from an economic and regulatory perspective describing advantages and drawbacks of this phenomenon. This part describes the actions taken by competent authorities so far and it shows that virtual currencies and related technology will tend to lead to the emergence of the same kinds of firms, with the same kinds of regulatory and consumer protection issues, as have traditionally existed in the financial services sector.

Part 2 makes a tentative inquiry into how the public ledger currency ecosystem could evolve regardless from the virtual currencies phenomenon. A special attention is paid to the European landscape and to recent initiatives taken by the European Institutions. First of all, it examines the relationship between public ledger currency platforms and the existing financial services sector. Secondly, it identifies the information we would need to determine whether public ledger currency platforms are necessarily a superior technology for delivering financial services. It shows that it is unclear, and unproved, whether these platforms could be more efficient than existing financial services providers.

Part 3 of this paper tries to focus and analyse potential impacts on corporate ownership in case of investments in listed companies realized in blockchains processes.

Part 4, which concludes, poses questions and issues for further consideration.

***

1 The information and views set out in this paper are those of the author and do not reflect the opinion of Borsa Italiana, London Stock Exchange Group
2 http://www.wsj.com/articles/the-revolutionary-power-of-digital-currency-1422035061
PART 1

1.1 The Definition of virtual currencies and its limits

This paper concerns the phenomenon commonly referred to as ‘virtual currencies’ (hereinafter also referred to as VCs) 1. VCs are a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically.

As will become evident, the usage of the term ‘currency’ is misleading for several reasons, including the insinuation that it is therefore exchangeable against other currencies, which may not necessarily be the case. However, this paper will not suggest a different denomination but, to reflect the common public usage of the term, will retain this term throughout the document.

More in detail, a virtual currency can be defined as a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community.

More in detail, three types of virtual currency schemes can be distinguished as follows:

1) **Closed virtual currency schemes.** These schemes have almost no link to the real economy and are sometimes called “in-game only” schemes. Users usually pay a subscription fee and then earn virtual money based on their online performance. The virtual currency can only be spent by purchasing virtual goods and services offered within the virtual community and, at least in theory, it cannot be traded outside the virtual community 4.

---


---

4 There may be exceptions. For instance, e-gold (http://www.e-gold.com/) is a virtual currency scheme, which was founded in 1996 and is operated by Gold & Silver Reserve Inc. trading as e-gold ltd. This currency is 100% backed by physical gold (or silver, platinum and palladium) held in locations around the world, such as London or Zurich. Users opening an e-gold account are actually buying a quantity of gold. The value of the account is linked to the price of gold. The system, which also allows the transfer of money to other users, operates with some companies acting as market makers, buying and selling this virtual currency (i.e. the underlying metal) against other currencies. The US authorities have accused this scheme of violating anti-money laundering regulations. In 2008 the company’s founder and two senior directors agreed to plead guilty to various charges related to money laundering and the operation of an unlicensed money transfer business. In 2009 the company contacted the US Government in order to recover its activity. The dialogue culminated in the development of a Value Access Plan acceptable to both the company and the Government. Once this plan is implemented, the expectation is that users will again have access to the value in their accounts. Example: World of Warcraft (WoW) Gold is a virtual currency used in this well-known online role-playing game designed by Blizzard Entertainment. Players have different options (with different subscription fees) for opening an account and starting to play. WoW Gold is needed as a means of exchange in the game, for instance in order for players to equip themselves well enough to reach higher levels. Players have several opportunities to earn WoW Gold within the game. Buying and selling WoW Gold in the real world is strictly forbidden under the terms and conditions established by Blizzard Entertainment. However, there seems to be a black market for buying and selling WoW Gold outside the virtual currency scheme. If Blizzard Entertainment discovers any illegal exchange, it can suspend or ban a player’s account.
transferring and exchanging money between the different virtual communities. This situation could change if initiatives, such as “Currency Connect” (http://www.currencyconnect.com/) succeed.

2) Virtual currency schemes with unidirectional flow. The virtual currency can be purchased directly using real currency at a specific exchange rate, but it cannot be exchanged back to the original currency. The conversion conditions are established by the scheme owner. Type 2 schemes allow the currency to be used to purchase virtual goods and services, but some may also allow their currencies to be used to purchase real goods and services.

3) Virtual currency schemes with bidirectional flow. Users can buy and sell virtual money according to the exchange rates with their currency. The virtual currency is similar to any other convertible currency with regard to its interoperability with the real world. These schemes allow for the purchase of both virtual and real goods and services.

To sum up, VCs are defined as a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a FC, but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically.

Virtual currency schemes differ from electronic money schemes insofar (see for more details paragraph 1.5) as the currency being used as the unit of account has no physical counterpart with legal tender status. The absence of a distinct legal framework leads to other important differences as well. The difference between electronic money and a virtual currency is that the latter is not necessarily attached to a FC, i.e. it does not have a fixed value in a FC and, furthermore, is not necessarily fixed to be redeemed at par value by an issuer. Electronic money, by contrast, means electronically, including magnetically, stored monetary value as represented by a claim on the issuer, which is issued on receipt of funds. Firstly, traditional financial actors, including central banks, are not involved. The issuer of the currency and scheme owner is usually a non-financial private company. This implies that typical financial sector regulation and supervision arrangements are not applicable. Secondly, the link between virtual currency and traditional currency (i.e. currency with a legal tender status) is not regulated by law, which might be problematic or costly when redeeming funds, if this is even permitted. Lastly, the fact that the currency is denominated differently (i.e. not euro, US dollar, etc.) means that complete control of the virtual currency is given to its issuer, who governs the scheme and manages the supply of money at will.

Moreover, VCs can therefore be characterised along the distinguishing features specified below.

The definition of VC refers to the fact that the value is essentially represented in digital form. This does not exclude the possibility that it may also be physically represented, such as through paper printouts or an engraved metal object. The term ‘digital representation of value’ is close to the monetary concept of a ‘unit of account’ but includes the option to consider VCs as private money or a commodity.

VCs are different from FC issued by central banks or public authorities. Currency issued by a central bank or public authority is considered FC, regardless of its (physical or digital) form.

Example 1: Facebook Credits (FB), Facebook’s virtual currency was introduced in 2009 to allow users to buy virtual goods in any application on the Facebook platform. It was possible to buy this currency using a credit card, PayPal account or a variety of other payment methods. A purchase made using any other currency than US dollars would undergo a conversion into US dollars using a daily exchange rate, before being exchanged for Facebook Credits at the rate of FB 1 = USD 0.10. Users were able to gain additional Facebook Credits through special promotions, for instance if they made online purchases. The terms on the website did not provide for a conversion back to US dollars. Surprisingly, in June 2012 the company announced that it would “update the payments product” and that it would convert all prices and balances that were quoted in Facebook Credits into local currency amounts starting in July 2012.

Example 2: The virtual currency scheme set up by Nintendo, called Nintendo Points, can be redeemed in Nintendo’s shops and in their games. Consumers can purchase points online by using a credit card or in retail stores by purchasing a Nintendo Points Card. The Points cannot be converted back to real money.
VCs can be used as a ‘medium of exchange’ to obtain goods and services from one holder, such as a private person or company, to another. This avoids the inconveniences of a barter system, i.e. the need for a coincidence of wants between the two parties involved in the transaction. How widely a VC scheme is accepted amongst market participants (i.e. its acceptance network) varies from scheme to scheme and could deliberately be designed to be for broader or for more limited use (e.g. for a specific community of individuals).

VCs can be (i) transferred from one user to another via electronic means, (ii) stored on an electronic device or server and (iii) traded electronically. However, it does not exclude physical transfers, the storage of copies in other forms (e.g. paper, minting and engraving) or that the VC is traded in other ways. Furthermore, the potential function of VCs as a ‘store of value’ (i.e. that the value can be saved and retrieved in the future) does not necessarily imply that the value will remain stable over time and will not be subject to inflation or deflation.

To conclude, the aim of the definition is to distinguish VCs from fiat currency and, in particular, from e-money as digital representation of FC. In economic theory, money performs three different functions: (1) a unit of account, (2) a means of exchange and (3) a store of value. In principle, VCs could potentially fulfil one or more of the functions of money. However, the definition of VC above reflects the fact that these functions are, at least currently, not comparable in terms of quality, and are not always fulfilled at the same time as each other or to the same extent. Furthermore, from a regulatory perspective, inclusion of the term ‘currency’ in the denomination ‘VC’ is misleading as it implies the highest liquidity of the asset, wide or universal acceptance within its geography, as well as exchangeability with other (virtual and fiat) currencies, which may not necessarily be the case for every single VC scheme.

### 1.2 What is a blockchain?

VCs exist purely as entries in an accounting system—a transparent public ledger known as the “blockchain” that records balances and transfers among special bitcoin “addresses”. More in detail, a blockchain is a public register or “distributed ledger” that contains all transactions in the respective virtual currency. At any moment in time the block chain keeps track of who owns how much of the VC. As the word says a block chain is a chain of blocks. The blocks consist of information about several transactions with the virtual currency. Whenever anyone completes a transaction involving a VC this transaction gets logged in a block. Each block contains an identifier of the previous block so that the blocks are linked in a chronological order. Every time a block gets completed a new block is automatically generated. The information contained in a block differs from VC to VC but most seem to contain the following information items: a block number, a 10 time stamp, an identifier of the previous block as a reference, the block’s own identifier, at least one transaction, information about the fees/rewards contained in the block.

Owning VCs doesn’t mean having a digital banknote in a digital pocket; it means having a claim to a bitcoin address, with a secret password, and the right to transfer its balances to someone else.

This ledger is what gives bitcoin its potential to disrupt (or innovate) global finance. In the current monetary system, we entrust banks and other fee-charging intermediaries to act as gatekeepers to nearly every transaction. Those centralized institutions maintain closely guarded in-house ledgers and, with that information, determine whether their customers have enough credit to write checks, buy goods with credit cards or wire money.

With bitcoin, the balances held by every user of the monetary system are instead recorded on a widely distributed, publicly displayed ledger that is kept up-to-date by thousands of independently owned, competing computers known as “miners”.

---

6 Miners essentially take part in a game that consists of solving mathematical problems. Someone wanting to buy, sell or transfer bitcoins automatically broadcasts the relevant information to the network. The system bundles those transactions into blocks and wraps them in a
A key idea here is that data in a blockchain ledger is made irrefutable by the computing consensus that goes into it. A blockchain is distributed across many independent computers rather than residing on a central server. So, unlike bank- or merchant-based data, such information is, in theory, invulnerable to attack or corruption. It is considered impossible for an outsider to hack thousands of computers simultaneously and there are no insiders to manipulate the central server’s software. This, in theory, makes blockchain data reliable and incontrovertible.

This paper is focused on the process of buying financial assets via a virtual currency block chain, leaving aside all the other forms of exploitation of such a technology. This process starts with the user/investor opening an account with a VC exchange and selling fiat currency in exchange for virtual currency units. This can happen in two ways: either online or using a VC ATM. In the case of an online platform there seem to be two different types: one where the platform holds the users/investors’ money at least for a short period of time (‘exchange’) and one where the platform only intermediates between buyers and sellers of VCs (‘trading platform’). This is the start of the users/investors “address” or account in this VC. The transaction is registered in the block chain of that VC as “this address has the right to dispose of this amount of VC now”. Or as two journalists recently described: “Owning bitcoin doesn’t mean having a digital banknote in a digital pocket; it means having a claim to a bitcoin address, with a secret password, and the right to transfer its balances to someone else.” Whenever any transaction is made from now on using the respective account/address, this is registered in the same block chain to keep up to date who owns what.

Depending on which financial asset/security the user/investor wants to buy he/she may need to exchange his/her virtual currency units for another virtual currency. This is currently necessary because not all virtual currencies can be bought using fiat currency. Some can essentially only be bought using another virtual currency (most commonly bitcoin) or if they can be bought directly with fiat currency, fees tend to be higher than when buying bitcoins and then exchanging bitcoins against the other VC. In order to exchange bitcoins for another virtual currency the user/investor may need to use another VC exchange than the one where he/she exchanged fiat currency into bitcoins. This may be necessary because not all VC exchanges offer all VCs.

In order to buy a financial asset the user/investor puts a buy order in the order mask and confirms. The asset/VC exchange normally matches buy and sell orders using a simple priority system: Orders are prioritized first by price (higher/lower bids have greater priority for buy/sell orders), followed by the block height when they’re added (bids in earlier blocks have greater priority), followed by the transaction ID (bids with lower transaction IDs have greater priority). Higher priority orders are filled first.

Once the order is filled the financial asset units are credited directly in the users/investors’ account. Depending on the nature of the financial asset/security, the issuer will distribute revenue/dividends/coupons/interest to every account that holds financial asset units.

The process described above results for example in an individual holding shares in company XYZ in the same way as if an individual buys shares of a company in the traditional way, e.g. via a broker, regulated exchange, clearing house, central securities depository and custodian. Only the intermediaries are different and mostly unregulated. The question is: who plays whose role in the VC world?

The VC exchanges have a similar function as a bank and/or broker: they intermediate in the exchange of different currencies and/or currency units against assets. Some of them even seem to hold client’s money for a short time, acting essentially like a currency exchange.

---

In this arena, another actor can be identified and complicates the final picture: Wallet providers. They can be another service of a VC exchange, a coin developer, or be completely separate of the two. Their function is to store VC units and they offer different degrees of safety and mobility of VC units. Compared to traditional regulated institutions their function is either comparable to safe-deposit box provider or resembles parts of the functions of a payment service provider, i.e. offering a payment or savings account.

The asset exchange provides the same function as a traditional regulated exchange: it matches buyers and sellers of assets. The only difference may lie in the order matching where traditional regulated exchanges offer a variety of order types and VC asset exchanges do not seem to at the moment.

The coin developer is essentially the equivalent of government in creating a new fiat currency and that of a central bank in the sense that some coin developers control the supply of the VC units.

1.3. Reasons for implementing virtual currency schemes

There are several business reasons behind the establishment of virtual currency schemes. They may provide a financial incentive for virtual community users to continue to participate, or create lock-in effects. Moreover, schemes are able to generate revenue for their owners, for instance float revenue. In addition, a virtual currency scheme, by allowing the virtual community owner to control its basic elements (e.g. the creation of money and/or how to allocate funds), provides a high level of flexibility regarding the business model and business strategy for the virtual community. Lastly, a virtual currency scheme may also be implemented in order to compete with traditional currencies, such as the euro or the US dollar.

By implementing a virtual currency scheme focused on the online world (basically for virtual goods and services) a company can generate additional revenue. The use of virtual currencies can help motivate users by simplifying transactions and by preventing them from having to enter their personal payment details every time they want to make a purchase. It can also help lock users in if, for instance, it is possible to earn virtual money by logging in periodically. If users are asked to fill out a survey or to answer other questions in order to earn extra virtual money, users reveal their preferences, thereby providing valuable information for commercial use. Virtual currencies can also be used as an important tool for application developers and advertisers when designing a strategy to reap the benefits of the virtual goods market.

An additional reason for implementing a virtual currency scheme is the possibility, in Type 2 and 3 schemes, to obtain new revenue from the float that results from the time difference between the moment at which money is transferred into the system and the moment at which it is taken out from the system again (either – in Type 3 only – via a currency exchange or – for both types – following the purchase of goods and services from third parties). In addition, scheme owners may also make a breakage profit from money which is not spent or exchanged back after its owners stop being active users.

In general, the motivation for setting up Type 3 schemes may differ from the incentives for the other schemes; of particular interest are the schemes designed to compete against real currencies as a medium of exchange. For the time being, the most prominent case is Bitcoin which, according to its creators and supporters, should overcome the limitations of traditional currencies that result from the monopolistic supply and management by central banks.

---

8 Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective, Gareth William Peters, Efthathios Panayi and Ariane Chapelle, University College London - Department of Statistical Science, University College London - Financial Computing and Analytics Group, Department of Computer Science and University College London - Department of Computer Science (2015)

Autonomics: An Autonomous and Intelligent Economic Platform and Next Generation Money Tool, Benjamin A. Munro and Julia McLachlan (2015);

Crumbling of the Bitcoin Cookie, Sharan Bathija, University of Sydney (2015)
1.4 A short historical review of money

It is difficult to establish the precise origins of monetary societies. It seems that payments using some form of money were being made as early as 2200 BC. Nevertheless, the format of money has changed considerably since then. Early money was usually commodity money, that is, an object which had intrinsic value (e.g. cattle, seeds, etc., and later, gold and silver, for instance). Around the eighteenth century, “commodity-backed” money started to be used, which consisted of items representing the underlying commodity (e.g. gold certificates). These pieces of paper were not intrinsically valuable, but they could be exchanged for a fixed quantity of the underlying commodity. The main advantages of this system were the portability of the money and that larger amounts of money could be transferred.

Modern economies are typically based on “fiat” money, which is similar to commodity-backed money in its appearance, but radically different in concept, as it can no longer be redeemed for a commodity. Fiat money is any legal tender designated and issued by a central authority. People are willing to accept it in exchange for goods and services simply because they trust this central authority. Trust is therefore a crucial element of any fiat money system. Regardless of the form of money, it is traditionally associated with three different functions:

• **Medium of exchange**: money is used as an intermediary in trade to avoid the inconveniences of a barter system, i.e. the need for a coincidence of wants between the two parties involved in the transaction.

• **Unit of account**: money acts as a standard numerical unit for the measurement of value and costs of goods, services, assets and liabilities.

• **Store of value**: money can be saved and retrieved in the future.

Money is a social institution: a tool created and marked by society’s evolution, which has exhibited a great capacity to evolve and adapt to the character of the times. It is not surprising that money has been affected by recent technological developments and especially by the widespread use of the internet.

Since its establishment in the 1980s and following the creation of the World Wide Web in the mid-1990s, access to and use of the internet has grown dramatically.

The impact has been so significant that it could reasonably be considered a structural change in social behaviour, affecting the way people live, interact with each other, gather information and, of course, the way they pay. In connection with the high penetration of the internet, there has also been a proliferation of virtual communities in recent years. A virtual community is to be understood as a place within cyberspace where individuals interact and follow mutual interests or goals. Social networking is probably the most omnipresent type of virtual community (e.g. Facebook, MySpace, Twitter), but there are other prominent communities, such as those that share knowledge (e.g. Wikipedia), those that create a virtual world (e.g. Second Life) or those that aim to create an online environment for gambling (e.g. Online Vegas Casino).

In some cases, these virtual communities have created and circulated their own digital currency for exchanging the goods and services they offer, thereby creating a new form of digital money. The existence of competing currencies is not new, as local, unregulated currency communities existed long before the digital age. These schemes can have positive aspects if they contribute to financial innovation and provide additional payment alternatives to consumers.

Bitcoin’s unidentified creator—a person or persons operating under the pseudonym of Satoshi Nakamoto—has provided a novel solution to a problem that has dogged societies for centuries: the distrust among strangers in commercial transactions with one another. In any exchange, how could someone feel secure unless there is a face-to-face handover of physical currency or some other valuable good?

When banks were invented in Florence in the late 1400s, a centralized solution emerged: People didn’t have to worry about trusting strangers anymore; they could just trust their banks to absorb the credit risk.
Using internal ledgers to keep track of everyone’s balances, banks became the middlemen through which exchanges could now occur.

Banking unleashed the Renaissance, the Industrial Revolution and the modern age. But a new problem arose: As the world’s monetary intermediaries, banks became powerful—perhaps overly powerful—repositories of information and influence. The financial system was and remains vulnerable to bank failures, as we were painfully reminded during the financial crisis of September 2008. One month after that meltdown, Satoshi Nakamoto released the initial document describing bitcoin. For the first time, people had a decentralized solution to the financial-trust problem. Here was a new form of currency that could be transferred online without involving fee-imposing, third-party institutions.

However, it is clear that they can also pose risks for their users, especially in view of the current lack of regulation.

In essence, virtual currencies act as a medium of exchange and as a unit of account within a particular virtual community. The question then arises as to whether they also fulfill the “store of value” function in terms of being reliable and safe, or whether they pose a risk not only for their users but also for the wider economy9.

1.5 Virtual currency schemes and electronic money

Virtual currency schemes can be considered to be a specific type of electronic money, basically used for transactions in the online world. However, a clear distinction should be made between virtual currency schemes and electronic money.

According to the Electronic Money Directive (2009/110/EC), “electronic money” is monetary value as represented by a claim on the issuer which is: stored electronically; issued on receipt of funds of an amount not less in value than the monetary value issued; and accepted as a means of payment by undertakings other than the issuer. Although some of these criteria are also met by virtual currencies, there is one important difference.

In electronic money schemes the link between the electronic money and the traditional money format is preserved and has a legal foundation, as the stored funds are expressed in the same unit of account (e.g. US dollars, euro, etc.). In virtual currency schemes the unit of account is changed into a virtual one (e.g. Linden Dollars, Bitcoins). This is not a minor issue, specifically in Type 3 schemes. Firstly, these schemes rely on a specific exchange rate that may fluctuate, since the value of the virtual currency is usually based on its own demand and supply. Secondly, to some extent the conversion blurs the link to traditional currency, which might be problematic when retrieving funds, if this is even permitted. Lastly, the fact that the currency is denominated differently (i.e. not in euro, US dollar, etc.) and that the funds do not need to be redeemed at par value means that complete control of the virtual currency is left to its issuer, which is usually a non-financial company.

Moreover, electronic money schemes are regulated and electronic money institutions that issue means of payment in the form of electronic money are subject to prudential supervisory requirements. This is not the case for virtual currency schemes.

Consequently, the risks faced by each type of money are different. Electronic money is primarily subject to the operational risk associated with potential disruptions to the system on which the electronic money is stored. Virtual currencies are not only affected by credit, liquidity and operational risk without any kind of underlying legal framework, these schemes are also subject to legal uncertainty and fraud risk, as a result of their lack of regulation and public oversight.

9 Is Bitcoin Money?: Implications for Bitcoin Derivatives Regulation and Security Interest Treatment of Bitcoins Under Article 9 of the Uniform Commercial Code, John Michael Grant, New York University (NYU), School of Law, Students (2015)
1.6 Post trading arrangements in virtual currency schemes

Just like in the real economy, in a virtual economy there are a wide range of economic actors who engage in transactions that have to be settled. These transactions have two settlement components: a) the delivery of (usually virtual, but potentially also real) goods and services; and b) the transfer of funds.

A “payment system” can be defined as a set of instruments, procedures, and rules for the transfer of funds among system participants. It is typically based on an agreement between the participant in the system and the system operator, and the transfer of funds is conducted using an agreed technical infrastructure\(^\text{10}\). In essence, virtual currency schemes work much like retail payment systems, except for the fact that financial intermediaries are not usually involved in the payment process. Virtual currency schemes demonstrate three main elements or processes of a retail payment system. A payment instrument is

a) used as the means of authorising and submitting the payment.

b) Processing and clearing involves a payment instruction being exchanged between the creditor and the debtor concerned.

c) Debits and credits are settled in the user’s account.

Although there are different models that may lead to important variations, the following specific features can typically be observed for payment arrangements within virtual currency schemes:

— **Agents involved:** Virtual currencies are held outside the traditional banking channels. A nonfinancial institution plays the crucial role and there are no other institutions providing payment accounts or payment services, or organisations that operate payment, clearing and settlement services. In this regard, virtual currency schemes work like traditional three-party schemes with a scheme-owned processor. The accounts to be debited and credited are held within this organisation, which is the virtual community operator. Virtual currency payments are therefore handled “in house” and can be classified as a specific type of “on-us” transaction, that is, a transfer of a claim on the virtual currency issuer.

— **Type of transactions:** From a conceptual perspective, payments can be classified as retail payments, i.e. a large number of payments with small values. The payment instrument is typically a virtual credit transfer.

— **Type of settlement:** Payments are usually settled on a gross basis. Each payment instruction is passed on and settled individually across the accounts of the payer and the payee, resulting in a debit and credit entry for every single payment instruction settled. As a general rule, the settlement is in real time, i.e. on a continuous basis throughout an entire day.

1.7 How competent authorities have reacted so far

The reactions from national authorities to the phenomenon vary, partly depending on the part of the world these originate from and on the type of authority. Responses range from warnings about risks, statements and clarifications on the legal status, licensing and supervision of VCS-related activities, or the banning of those.

1.7.1 European Central Bank

ECB published a comprehensive report “Virtual Currency Schemes” in October 2012\(^\text{11}\) – first of its kind by a public authority and a second report “Virtual Currency Schemes—A Further Analysis” in February 2015\(^\text{12}\) –

\(^{10}\) BIS (2001), p. 14, and ECB Glossary of Terms Related to Payment, Clearing and Settlement Systems.


with special focus on relevance for retail payments. The main outcomes of such reports can be summarised as follows: In the current situation, given their small size, virtual currency schemes: (1) Do not currently pose a risk to price or financial stability; (2) Are not (yet) regulated and not closely supervised or overseen by any public authority and this may determine a risk for users; (3) Are a challenge for public authorities, as they can be used by criminals, fraudsters and money launderers to perform their illegal activities; (4) Fall within central banks’ responsibility as a result of characteristics shared with payment systems.

For the time being, for its own tasks in the field of payment systems, the ECB does not see the need to amend or expand the current EU legal framework related to these tasks. The usage of VCs for payments remains limited for now, which implies that there is not yet a material risk for any central bank tasks, including promoting the smooth operation of payment systems. However, a major incident with VCs and a subsequent loss of trust in VCs could also undermine users’ confidence in electronic payment instruments, in e-money and/or in specific payment solutions. The ECB recognises that, besides their drawbacks and disadvantages, VCs could also have some advantages over traditional payment solutions and specifically for payments within virtual communities/closed-loop environments and for cross-border payments. As such, the ECB notes that it is not excluded that a new or improved VCs may be more successful in future. Therefore, the Eurosystem will continue monitoring developments, notably for payments-related aspects of VCs.

1.7.2 European Banking Authority

In September 2013, virtual currencies emerged as one of the many innovations the EBA was monitoring at the time. Following three months of analysis of the potential risks to individuals arising from using VCs, the EBA issued a public warning on 13 December 2013, making consumers aware that they may lose their money on an exchange, that their VC units may be stolen from their digital wallets, that they are not protected when using VCs as a means of payment, that the value of VCs has been very volatile, that transactions in VCs may be misused for criminal activities and that individuals holding VCs may be subject to unforeseen tax liabilities.

In the months following the publication, several of the risks that had been highlighted in the warning started to materialise, as a market-leading exchange (Mt. Gox) had to close due to mismanagement, cyber-attacks and theft of a substantial amount of Bitcoins. As the most popular VC scheme at the time, the value of Bitcoins fluctuated wildly, and several jurisdictions changed the tax status of VCs.

To find a solution to the issue of whether VCs can and ought to be regulated, the EBA carried out additional analysis during the first half of 2014, the results of which are presented in its opinion on virtual currencies published on 4 July 2014.

More than 70 risks were identified across several categories, including risks to users; risks to non-user market participants; risks to financial integrity, such as money laundering and other financial crime; risks to existing payment systems in conventional FCs, and risks to regulatory authorities.

Numerous causal drivers for these risks were identified too, as these indicate the regulatory measures that would be required to mitigate the risks. The risks include the fact that a VC scheme can be created, and then its function subsequently changed, by anyone, and in the case of decentralised schemes, such as Bitcoins, by anyone with a sufficient share of computational power; that payer and payee can remain anonymous; that VC schemes do not respect jurisdictional boundaries and may therefore undermine financial sanctions and seizure of assets; and that market participants lack sound corporate governance arrangements.

In EBA’s view, a regulatory approach that addresses these drivers comprehensively would require a substantial body of regulation, some components of which are untested. It would need to comprise, amongst other elements, governance requirements for several market participants, the segregation of

client accounts, capital requirements and, crucially, the creation of ‘scheme governing authorities’ that are accountable for the integrity of a VC scheme and its key components, including its protocol and transaction ledger.

However, whilst such a ‘long-term’ regime is not in place, some of the more pressing risks identified will need to be mitigated in other ways. As an immediate response, the EBA recommends that national supervisory authorities discourage credit institutions, payment institutions and e-money institutions from buying, holding or selling VCs.

The EBA also recommends that EU legislators consider declaring market participants at the direct interface between conventional and virtual currencies, such as virtual currency exchanges, to become ‘obliged entities’ under the EU Anti Money Laundering Directive and thus subject to its anti-money laundering and counter terrorist financing requirements.

This immediate response will ‘shield’ regulated financial services from VC schemes, and will mitigate those risks that arise from the interaction between VC schemes and regulated financial services. It would not mitigate those risks that arise within, or between, VC schemes themselves.

1.7.3 European Securities Markets Authority

In April 2015 ESMA issues a call for evidence\(^{14}\) after monitoring and analysing virtual currency investment over 6 months, to understand developments in the market, potential benefits or risks for investors, market integrity or financial stability, and to support the functioning of the EU single market.

ESMA declared to have no pre-conceived view as to whether any other regulatory action is needed and, subject to assessing the information received in response to this call for evidence, ESMA said it has no immediate plans to take any.

In seeking to understand investment using virtual currency and distributed ledger technology, ESMA is not expressing any view on the desirability or otherwise of virtual currencies as such or on their use as, for example, means of payment. Although ESMA is aware that many investors seem to consider VCs less as a payment instrument and more as a financial asset.

ESMA is interested in three issues:

a. Investment products which have virtual currency as an underlying: these are ‘traditional’ investments which do not necessarily require the investor to use virtual currency to make the investment, but give the investor exposure to one or more virtual currencies. Examples would be financial instruments such as a collective investment scheme or potentially non-registered derivatives such as options and contracts for difference (CFDs) that use VCs as an underlying or reference to determine the amount payable under the financial instrument or invest in VC related businesses and infrastructure. (‘VC investment products’)

b. Investment in virtual currency based assets/securities, and the transfer of those assets/securities: this would encompass ‘traditional’ financial assets such as shares, funds, etc. that are, however, issued and traded using virtual currency distributed ledger technology. In this case the investor is likely to need to purchase one or more virtual currencies in order to make the investment, the asset/security invested in (which is constituted using the virtual currency and associated technology), and transactions made and recorded through the distributed ledger associated with the currency rather than through ‘traditional’ exchanges, custodians, CSDs or registrars. (‘VC-based assets/securities’)

c. Other uses of the distributed ledger in relation to investment: this would encompass any other use of the ‘blockchain’ technology, which might not be limited to VC investment products or VC-based assets/securities. For example, a distributed ledger technology could be used to record offers, transactions

in or transfers of ownership or other rights in a ‘traditional’ security, whether by ‘traditional’ or new-entrant providers. In this context, the technology might not be dependent on the use of a virtual currency. The latter case is the core object of such a paper.

### 1.7.4 US experience

The U.S. government has taken several steps toward regulating virtual currencies, in general, and Bitcoin, in particular. The most important law leveraged by the government has been the Bank Secrecy Act. In early 2013, FinCEN, the Agency authorized to enforce the Bank Secrecy Act, issued guidance on the applicability of regulations to virtual currencies. Since then, both federal and state authorities have been actively scrutinizing VCs and Bitcoin activities. Notices have been issued and investigations have commenced, and in some instances authorities have arrested individuals and seized assets.

More in detail, the SEC’s Office of Investor Education and Advocacy issued an investor alert to warn individual investors about fraudulent investment schemes that may involve Bitcoin and other virtual currencies (SEC pub 153 Ponzi schemes Using virtual Currencies).

In such an alert, SEC expressed concerns that the rising use of virtual currencies in the global marketplace may entice fraudsters to lure investors into Ponzi and other schemes in which these currencies are used to facilitate fraudulent, or simply fabricated, investments or transactions. The fraud may also involve an unregistered offering or trading platform. SEC pointed out that these schemes often promise high returns for getting in on the ground floor of a growing Internet phenomenon.

Fraudsters may also be attracted to using virtual currencies to perpetrate their frauds because transactions in virtual currencies supposedly have greater privacy benefits and less regulatory oversight than transactions in conventional currencies. SEC concluded that any investment in securities in the United States remains subject to the jurisdiction of the SEC regardless of whether the investment is made in U.S. dollars or a virtual currency. In particular, individuals selling investments are typically subject to federal or state licensing requirements.

A 2015 Congressional Research Service (CRS) report, “Bitcoin: Questions, Answers and Analysis of Legal Issues,” provides key background information as well as an overview of major issues. The CRS report notes that, given the powers articulated in the U.S. Constitution, specifically the authority “to coin money” and “regulate the value thereof,” the responsibility to oversee digital currency falls upon Congress. As of now, Congressional actions remain in the exploratory phase, with the Senate Finance Committee having only recently asked the Government Accountability Office (GAO) to review tax requirements and compliance risks. The tax code lacks clarity on how such currency should be treated: Is it digital currency, property, barter or foreign currency? Early concerns have focused more on tackling consumer protection issues than tax ambiguities, and as a result, the GAO recommended increased inclusion of the Consumer Financial Protection Bureau in questions related to Bitcoin. Federal banking regulators have yet to issue guidance or regulations governing how banks are to deal with bitcoins. In a February 2014 statement, Federal Reserve Chair Janet Yellen said: “Bitcoin is a payment innovation that’s taking place outside the banking industry…. There’s no intersection at all, in any way, between Bitcoin and banks that the Federal Reserve has the ability to supervise and regulate.” According to the CRS report, other legal issues with Bitcoin include: (1) Counterfeiting criminal statutes: It is illegal to counterfeit both U.S. and foreign currency, but current monetary laws do not mention digital currency. Given that Bitcoin is a peer-to-peer transaction without any formal involvement by a regulatory body or a government, it is unclear if there is a role or responsibility for the U.S. legal system to intervene if counterfeiting occurred in such a situation; (2) Federal tax laws: To

---


16 http://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf
date, the IRS has done little to address the tax implications of virtual currencies. Instead, the IRS has focused on public education by issuing guidelines indicating that for now, virtual currency will be treated as property for tax purposes, and within that framework, all corresponding tax laws apply; (3) Federal anti-money laundering laws: To fight illegal and terrorist-related financial transactions, the Bank Secrecy Act (BSA) requires financial institutions to keep records. This allows suspicious withdrawals and transactions to be tracked. These requirements would conceivably be placed on any business that engages in the exchange of bitcoins for U.S. or foreign currency.

While VCs are under scrutiny, the regulatory interest (and support) for its underneath technology is growing in governmental institutions an financial actors for its legal implications and potential developments.

On June 3, 2015 Vermont Governor Peter Shumlin signed into law “No. 51. An act relating to promoting economic development. (S.138),” which contained “Sec. A.3. Study and Report; Blockchain Technology.” This mandates that a report be written by January 15, 2016, which has “… finding(s) and recommendations on the potential opportunities and risks of creating a presumption of validity for electronic facts and records that employ blockchain technology.”

There was also an amendment by Senator Balint which appears to be Vermont’s roadmap if there are favorable findings in the report due early next year. On April 8, Amendment to S.138 added in a third reading “Sec. 47. 9 V.S.A. Chapter 2: Electronic Verification Of Facts And Records: § 11. Blockchain Enabling.” It states in part that: “Blockchain technology shall be a recognized practice for the verification of a fact or record, and those facts or records established through a valid blockchain technology process shall have a presumption of validity for matters to be determined subject to, or in accordance with, the laws of the State of Vermont.”

1.8 The dimension of the phenomenon

All of the existing and publicly available statistical information is gathered by VCs stakeholders or operators of web pages connected with them and is thus unverified.

At the time of writing, there are a large number of decentralised VCs, namely around 500 VCs with a total market capitalisation of about €3.3 billion. The majority of VCs have insignificant market capitalisation, i.e. below €1 million. Only 21 VCs exceed this figure, and only the top eight are above €10 million.

The significance of VCs could be estimated by comparing their market capitalisation with money supply for currencies as euro (€5,493,000,000,000), US dollar (€1,952,504,690,000), Australian dollar (€184,161,000,000) or even Bolivian boliviano (€5,286,504,000), which at the time of writing was closest to the market capitalisation of Bitcoin.

According to bitcoincharts.com, only 9% of (Bitcoin) exchange transactions are against euro; most exchange transactions are against Chinese renminbi (31%) and US dollar (25%), while other currencies, including British pound sterling and Swedish krona, are traded to a much smaller extent.

---


PART 2

The public ledger ecosystem, its future developments and its interactions with the “real” financial sector

VCs and its technology may represent a challenge for the current financial and payment systems and its traditional operators. However, this shared assumption is – somehow - counterbalanced by the current trend of digitalisation – the development of new models and approaches through technology and the internet.

Indeed, this trend has been recently seen by European Institutions as a particular opportunity to integrate markets and solve a number of residual concerns in these sectors.

In the context of the recent European Commission’s plan to realise a fully functional and competitive Single Market for financial services (the so called Capital Market Union)\(^{19}\), digitalization and innovation are considered as key actors, supporting growth in the European economy and represent an important driver of the integration of capital markets.

By stimulating both actual and potential competition, greater integration would motivate providers to create a wider choice for consumers, reduce prices, improve quality and innovate. This initiative is also related to other parallel Commission priorities and work streams such as the Digital Single Market (inducing the review of Contract law relating to tangible goods and digital content), the work on contract-law related obstacles in the insurance sector, the assessment of the potential of the Distance Marketing of Financial Services Directive and the sector inquiry into e-commerce.

As aforesaid, in parallel with such enthusiasm, there is a wide perception that the development of such technology could determine – if not controlled and regulated - 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.

As said in Part 1, there has been an increasing trend recently aimed at distinguishing VCs from the expression “distributed ledger technology” which is accurate and unambiguous, being the exact technical definition of the structure such digital tokens are based upon\(^{20}\). Blockchain can be considered as the “rail to move virtual currencies” and represents a powerful means to transmit information in a legally and enforceable way. This could be the real “financial revolution” rather than VCs *per se*. This is because VCs (and Bitcoin et similia) are often negatively associated with cases ranging from MT Gox to Silk Road: both of these services conflated legacy systems entrusting third parties with private keys.

In a podcast\(^{21}\) realised in summer 2015, global investment research analyst Heath Terry addressed both bitcoin and the blockchain, praising the distributed ledger as a technology that would have "massive implications" for asset and ownership transfer.

"We’re first pitch, first inning in terms of seeing how companies are going to use the technology," Terry said, adding: "It's fascinating in really early stages, but it's hard to see a world where blockchain technology doesn't change the way we think about asset ownership."

Having said that, this paper focuses on the way of VC investing by using the transaction technology to buy, sell, transfer and own financial assets/securities. This means essentially that no third party like a regulated exchange, broker, central securities depository, custodian, etc. normally intermediates between the shareholder and the issuer of the security. VC based financial assets/securities are distributed and traded

\(^{19}\) The CMU is a new frontier of Europe’s single market. Its creation is a key element of the Investment Plan announced by the Juncker Commission in November 2014. For more detail, see: [http://ec.europa.eu/finance/capital-markets-union/index_en.htm](http://ec.europa.eu/finance/capital-markets-union/index_en.htm)

\(^{20}\) Cfr Banca Intesa response to ESMA consultation

using virtual currencies and the associated infrastructure. They cannot be bought from traditional brokers using fiat currency.

In order to understand how similar or different VC based financial assets/securities and transfers of them are from traditional regulated financial asset transfers, it is essential to understand the parties involved and their functions. This is necessary, because the process of buying, selling or transferring assets via the Bitcoin block chain or another block chain is not completely free of intermediaries either.

The block chain unites the functions of several traditional regulated entities: it is the register of all transactions and hence all balances in the VC, a function that is normally provided by the central bank and banks more in general as well as central securities depositories (CSDs). Furthermore, the block chain clears and settles transactions by enabling confirmation of transactions. For most virtual currencies, transaction as well as clearing and settlement times seem to be much quicker than in the traditional regulated system. Confirmation of a transaction and settlement takes at most a couple of hours and not days. Apart from that, transaction costs can be much lower than the fees charged via traditional payment processing or securities brokerage and settlement.

It is also possible that firms could look for ways of using the technology to provide alternative trading and post-trading services in relation to ‘traditional’ securities, and not just VC-based securities. This could represent a challenge for traditional stock exchanges, especially as regards small medium enterprises and start ups (looking for lower listing and trading fees) and Hi-tech companies. Coin IPOs are commonplace in the crypto world, and after doing just a little research in the field you should realize that some of them are scams.

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.
PART 3

The question of enforceability of ownership rights

Anyway, it is unclear whether and how ownership rights created via a block chain would be enforceable. Essentially, all the block chain records is one address sending a certain amount of VC units to another address. First of all, block chain based digital tokens can be considered “irrevocable and self-enforcing” promises.

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). Legal enforcement, on the other hand, is much more complex to address and it requires to analyse post trading profiles (i.e. safekeeping and settlement arrangements).

As regards safekeeping of VCs, in the absence of a "central register" of investors, information on the holders of virtual currency assets is stored as part of the blockchain. This is not directly comparable to the notary and registration functions performed by CSDs, which are essential to maintain the integrity of the issue. In the case of blockchains, individual "miners" are collectively responsible for validating transaction data but there is no legal entity bearing responsibility for reconciling individual holdings with the number of total assets having been issued, and for managing any potential discrepancies. This could present a serious weakness in terms of investor protection. The "safekeeping" of virtual currency assets is done through accounts maintained in IT servers, without any "depositary" entity being responsible for the central maintenance of these accounts. On this regard, the de-centralization of the ledger can be considered as a strong drawback. However, its fragmentation in numerous servers is, at the same time, its strength as it is difficult (even impossible) that each single block of the chain can be damaged or out of order simultaneously: so the level of business continuity and crisis management could be stronger than the ones which characterized and must be ensured by the traditional trading and post-trading systems.

As far as settlement is concerned, it seems to us that the speed with which transactions can be processed in virtual currency environments is due to absence of (chains of) intermediaries. Transfers occur directly between individual accounts.

But, which is the relevance of such accounts?

In today’s securities markets, securities are held in a "book entry" form. As securities are paperless, either dematerialized or immobilized, they are held through accounts that the intermediaries keep for their portfolios or the portfolios of their clients in the Official Central Securities Depositories (CSDs) or registries. This electronic form of establishing property rights in securities arose as a consequence of globalization of financial markets. Trading, commerce and, generally, free movement of securities can be better achieved throughout the world if securities are allowed to cross borders without any restriction resulting to an expansion of the scope of potential “clients” to participate and invest in global financial markets.

Starting from a very general perspective, when analysing the legal position under national law, in the first place, an important distinction has to be made: under national corporate law and other relevant laws, a securities holder has a specific legal position. However, in some (not all) Member States, this legal position might change depending on whether such securities are credited to a securities account or not. This phenomenon occurs in particular in the context of holding systems which are built on the issuance of a
paper certificate which is subsequently immobilised with the CSD: supposing the investor had the paper certificate physically in his hands or held in segregated safe custody under his name, he would enjoy exactly and purely the full legal position with respect to the securities given by the applicable law (in most countries “ownership” or “property”). In case the paper is delivered into the holding system the legal position would change in many jurisdictions, for example towards a shared property interest in a pool of securities or similar interest, or the equitable interest of a trustor (investor) against the trustee (account provider).

The above raises the question of what is the exact legal position received by an account holder upon credit of securities to its account under national law. The answer is again that there are significant differences depending on the law of the Member States. Under national law, two factors can have influence on the legal position of an account holder when securities are credited to his account: first, the basic legal concept, and, second, the question whether the account holder holds for its own account or for the account of somebody else.

First, the basic legal concept differs considerably between the various Member States: some systems are based on the principles of property law. Others organise the holding and disposition of securities following the concept of fiduciary trust. Second, in some jurisdictions, it makes a difference whether an account holder is the one at the end of the holding chain that holds for its own account or whether the account holder does not hold for its own account but for another person. In such system, this factual difference leads to a completely different analysis regarding the legal position of the account holder. For example, under German law, the “ultimate account holder” has a shared property interest in a pool of securities kept by the CSD, whereas account providers which are also account holders in the holding chain have no proprietary interest in the securities but have merely a role of safe-keeper with actual or deemed possession of the securities. In the UK (England and Wales), the upmost account provider (which is the participant in the CSD in this case) is regarded as trustee having legal ownership of the relevant securities, while the ultimate account holder has the role of a trustor with respect to the securities, disposing of an equitable interest in the securities, as opposed to legal ownership. All entities intervening in the holding chain are themselves trustors as regards their own holding with the upper-tier account provider and trustees with respect to their own account holders22.

In addition, we can distinguish between Transparent systems and non Transparent ones23. In the first ones, the CSD “knows” directly the ultimate shareholders. In case of “indirect” holding systems, i.e. the holding through a chain of intermediaries, an “irregular deposit” is established. This irregular deposit scheme operates more or less as a bank or cash deposit. The intermediary, which is for example the custodian bank, holds in such system its clients’ assets in a commingled manner (and not segregated per client) and is entrusted by its clients to make use of the deposited assets or to redeposit them. In effecting this intermediation status, the depositor sacrifices its ownership right over its assets, which passes to the custodian. Consequently, the custodian becomes in this case the owner of the deposited assets, on the only condition to retain at the depositor’s disposal assets of the same quantity and quality and return them to the depositor upon the latter’s demand. Following this second approach, it could be easily explained why as registered shareholders appear in the registries not the investors themselves, but the intermediaries acting on their behalf. It is the intermediary that acts as the owner of the deposited shares in the context of the

---

22 Second Advice of the Legal Certainty Group “Solutions to Legal Barriers related to Post trading within the EU”, August 2008
irregular deposit, regardless of the fact that it owes a duty to redeliver to the depositor shares of the same quantity and quality upon the latter's request.

The blockchain’s technology functions in a way similar to these established mechanisms as the account in which securities are credited is not a “traditional account” – held by an intermediary or by a regulated entity – but it’s a web account realized via electronic annotations.

So, what is the (legal) value of the registration in the blockchain’s accounts? Is it just a promise (whereas legally enforceable)? Who is the legal shareholder? Is it the investor or the blockchain operator? Who is entitled to vote in the general meeting of the company? When is the property transferred upon the investor? When possession is secure?

Let’s focus on the issue “when is the property transferred” in case of an acquisition made via blockchain.

Both the competing values of possession and market transfer are essential to the functioning of capitalism. On the one hand, owners of property must be secure in their title. On the other hand, markets cannot function efficiently unless buyers can be assured that they are acquiring good title without having to engage in burdensome searches. Conflicts arise when one party, X, purports to transfer property that belongs to an innocent second party, O, to an innocent third party, P. It is clear that the double-dealing X has legal liability to make O and P whole, but such fraudsters tend to leave the jurisdiction, are judgement proof or both. Conveyancing and priority rules, therefore, are needed to decide which of two innocent parties, O and P, shall be recognized as the superior claimant and which bears the loss.

This is true also for transactions realized via blockchains.

Let’s refer to the Italian legal framework where the debate on virtual currencies is well developed24 and authorities have taken a “stay and see” approach25. In case of securities held via a CSD ex art. 80, d. lgs. n. 58/1998, in doctrine and jurisprudence we may identify two different positionings. Some authors believe that,26 the securities entitlement is transferred because of the consensus between the parties, therefore at the “trade date”. The related contract can be categorised as a “contratto consensuale con effetti reali ex art. 1376 c.c.”.

On the contrary, other authors27 believe that the consensus determines an obligation to transfer the security, while the transfer of the property will follow the registration on the account, i.e. at the “actual settlement date”.

24 Bitcoin: la moneta è virtuale, ma l’esenzione Iva è reale (FiscoOggi.it, 26 ottobre 2015); Rapporto UIF 2014: Bitcoin sotto osservazione(Italia Oggi, 14 luglio 2015); FATF: Guidance fora risk-based approach to virtual currencies (June, 26th 2015); Banca d’Italia: “Criptovalute tra opportunità e voglia di regolamentazione” (Forum del Sole 24 Ore, 3 Maggio 2015); Virtual currencies and AML risks, the Italian Supervisors opinions (April 18th, 2015); Bitcoin in crisi? “No”, ci riprovano le startup(Corriere Comunicazioni, 14 aprile 2015); Bitcoin, Jp Morgan recluta cervelli per la sua moneta virtuale (Il Messaggero, 11 marzo 2015); Bitcoin o Blockchain, quale sarà la vera rivoluzione? (linkiesta.it, 10 febbraio 2015); Antiriciclaggio: Bitcoin sconosciute dall’Ulf (Italia Oggi, 7 febbraio 2015); Parere di Bitcoin Foundation Italia su comunicato di Banca D’Italia su Bitcoin e critto valute (3 febbraio 2015); Bitcoin - Bankeitalia: strumenti di pagamento del tutto legali (Italia Oggi, 3 febbraio 2015); Bitcoin da maneggiare con cura (Italia Oggi, 3 febbraio 2015); Bankeitalia lancia l’allarme sul Bitcoin (Il Sole 24 Ore, 1° febbraio 2015); UIF, Unità di Informazione Finanziaria per l’Italia: “Utilizzo anomalo di valute virtuali” (30 gennaio 2015); Quei trecento bonifici segnalati da Bankeitalia che servivano a finanziare la jihad (La Repubblica, 19 gennaio 2015); Bitcoin «europei», congelati anche i conti italiani (Il Corriere della Sera, 7 gennaio 2015); Bitcoin, focus in UK, Usa e Russia (Italia Oggi, 8 dicembre 2014); Trust e bitcoin nel mirino dell’Ulf (Il Sole 24 Ore Plus, 12 luglio 2014); FATF/GAFI: “Valute Virtuali, definizioni chiave e potenziali rischi in ambito antiriciclaggio e finanziamento del terrorismo” (11 luglio 2014); Bitcoin, Guardia di Finanza: “In quei codici si annida il riscaldagio” (La Repubblica, 10 luglio 2014)

http://uiuf.bancaditalia.it/normativa/nom-indicatori-anomalia/Comunicazione_UIF_su_VV.pdf


27 De Gregorio, Delle società e delle associazioni commerciali, artt. 76-250 cod. comm., in Il codice di commercio commentato, a cura di Bologna, Rocca e Vivante, IV, Torino, 1938, 499; Weigmann, voce “Società per azioni” in Dig. Disc. priv., Sez. comm., XIV, Torino, 1997, 366 ss; Oppo,
In case of securities acquired via blockchain, in the first scenario, we may say that the acquisition takes effects as an acquisition made via a traditional trading system. This is because the consensus is expressed by the real shareholders when the order is inserted in the system and the contract arises from the matching in the trading system, via the intermediation of the blockchain. In the second approach, however, there could be big and tricky questions. Which accounts we should consider for the registration? The blockchain’s ones or the accounts of the intermediary where securities are credited at the very end of the process when the investor decides to opt out from the blockchain environment?

In order to meet their accounting and book-keeping requirements, intermediaries keep track of all phases of a transaction, entering records in the customers’ accounts. Under the same obligations, over time the principle has become established (and come to apply generally) whereby the identification of the stocks necessary for ownership of them to be transferred takes place as and when the trade contract is executed, i.e. when the buyer and seller receives the executed trade from the market and/or provides instructions to their settlement agents based on which the agents themselves make arrangements for the stocks to be delivered/collected at the contractual settlement date (which requires the stocks in question to be identified). However, the legal status of the entries made crediting the stocks to, or debiting them from, the customers’ accounts to record the trade being concluded is less dear-cut. They could, for example, be mere accounting records, with a deferred performance obligation (similar to “subject to collection” entries), or as the point in time when the financial instruments involved in the contract are identified.

The method adopted by the majority of intermediaries for their all customers (i.e. institutional as well as retail) and for all centralized trades (i.e. those executed on regulated markets and OTC), based on the provisions of Consob regulations 929/81 and 7679/94, uses the trade date as the point at which the financial instruments involved in the trade are identified (and hence ownership of them transferred).

However, the different purposes of the provisions cited, plus the fact that in theory they apply only to non-institutional clients, does not help in clarifying the legal status of the transfer of ownership.

In this connection, it is sufficient to recall that institutional investors, to which the Consob regulations referred to above have never applied, have always been able to short-sell financial instruments, needing only to ensure that the stocks are available in good time for such trades to be settled. Accordingly, for trades concluded by such parties, it is doubtful that the entries made by the intermediaries in the accounts at the trade date can effectively qualify as the point at which the financial instruments involved in the contract thus concluded are identified.

Lastly, with reference to minor real rights such as usufruct and pledges, the importance which the law (Italian legislative decree 213/98, Article 34; Italian legislative decree 58/98, Article 87) assigns to the point at which these are recorded in the accounts should be noted. For pledges, which are real rights, for instance, the point at which the pledge is recorded in the intermediary’s account is equivalent to delivery, and hence is necessary for the contract to be fulfilled. The real right is only established when it is actually recorded in the account (a point which is therefore equivalent to the actual settlement date).

It in unquestionable that such a contract can be considered as a “vendita di cose determinate solo nel genere” and so the transfer of the property should happen at the time of the “identification” in accordance with article 1378, Civil Code (vendita di cosa determinata solo nel genere) and article 1478, Civil Code which

\[Tramonto\ de\ i\ titoli\ di\ credito\ di\ massa\ ed\ esplosione\ de\ i\ titoli\ di\ legittimazione,\ in\ Riv.\ Dir.\ Civ.\ 1998,\ I,\ p.\ 650;\ Cian,\ Titoli\ dematerializzati\ e\ circolazione\ cartolare,\ Milano,\ 2001,\ p.\ 291\]
sets the obligation upon the seller (in case he’s not the owner) to provide the property to the buyer stating that the acquisition of the property takes effect starting from the moment the seller acquires the property.

The identification is done by the intermediaries which, in compliance with their record keeping obligations, tracks all the phases of the transaction via annotations on the clients accounts. The same activity can be done by the blockchain operator, even if its activity isn’t regulated.

So, in case of an acquisition realised via blockchain, the property is transferred to the real investor at the time of the matching on the exchange by the blockchain operator if we adhere to the “trade date” theory. If, viceversa, we opt for the “actual settlement date” theory we should discuss about the opportunity to recognize relevance with reference to the registration on the accounts of the ledger rather than on the accounts of an intermediary. Otherwise, the consequence is that all the legal effects would happen upon the blockchain operator – at least for a certain time lag.

The challenge of identifying beneficial owners of securities transactions and the exact timetable of the related entitlement is not trivial. For example, it matters in case of insolvency of the ledger or for anti-money laundering purposes in the absence of a central register. The comprehensiveness, reliability and integrity of the information on trade counterparties contained in the blockchain needs to be assessed in this regard, and solutions may need to be developed in the future to allow for a proper verification of beneficial owners' identity for legal and fiscal compliance purposes.

Similar analysis and tentatives to understand how the transfer of ownership via blockchain is legally enforceable have been conducted in the US in respect of the “traditional” Commercial Law28.

The US various property regimes reflect the familiar tensions between rights of possession and alienation. Although, the term “possession” is commonly used in a way to mean the fact of physical custody of tangible things, jurisprudentially, the legal right to possession can be thought of (for our purposes) as the right of an earlier-in-time claimant to exclude later-in-time claimants from an identifiable object. Indeed the US Commercial law usually reflects the traditional compromise that favors possessory claims. That is, the default rule is that first-in-time claimant prevails over a subsequent transferee. Having said this, it is also true that transferees are protected in favored market transactions. That is, if the transferee can show he satisfies certain conditions, then he will take free and clear of the possessory rights (adverse claim) of the earlier-in-time claimant. These conditions typically require the transferee to meet an appropriate standard of good faith and to give value, but sometimes also require lack of notice, or specific market conditions. In a few cases, however, the Us Commercial Law reverses this rule, adopting a default rule favoring subsequent transferees over prior claimants. For example, rule of Sec. 9-332(a) of the Uniform Commercial Code (hereinafter U.C.C.) provides with respect to money that a transferee of money takes the money free of a security interest unless the transferee acts in collusion with the debtor in violating the rights of the secured party.

Note that while usually a transferee will lose unless he/she can establish that he/she has a favored state of mind (e.g. good faith), in case of money, he/she prevails unless the prior claimant can establish that he/she had an affirmatively disfavored state of mine (i.e. she acts in collusion).

If bitcoin were “money” it would be entitled to the rule of Sec. 9-332(a). Indeed, it could only truly function as money if it were governed by a similar rule which represents one of the hallmarks of money. That is, one reason why you will take a dollar bill as payment is that you can always be sure that no previous claimant

28 Bitcoin and the Uniform Commercial Code, Jeanne L. Schroeder Benjamin N. Cardozo School of Law · Yeshiva University, Jacob Burns Institute for Advanced Legal Studies, August, 2015, Faculty Research Paper No. 458
could try to replevy it from you. This latter is not the current regime that is applicable to bitcoins. Bitcoin transferees, in contrast, must yield to prior perfected security interests.

One of the advantages of using the blockchain protocol for the settlement of financial transactions is that bitcoin is more, not less transparent than conventional payment systems. Hand-to-hand money is rarely traceable. Funds deposited into commingled deposit accounts are not even theoretically. In contrast, bitcoin transactions are infinitely traceable. As described in paragraph 1.2, the defining characteristic of all bitcoin “currencies” is the blockchain which prevents counterfeiting and double spending. Each bitcoin transaction is unique and identifiable and all transfers are recorded. Accordingly, ownership in bitcoin is, therefore, not truly anonymous, but can be pseudonymous. Although the secured party may have difficulty identifying many owners of an encumbered bitcoin, it will always be able to identify the encumbered bitcoin itself. Consequently, if the original debtor defaults on the secured transaction, and the unencumbered bitcoin ever comes into the hands of an identifiable transferee, then the secured party would have the right to “repossess” it. Consequently, one of the advantages of using the blockchain for the transfer of value is that does away with the various (and often complicated) tracing rules which characterized the current post trading systems and diverse legal frameworks that apply to deposit accounts and replace them with the reality of actual tracing.
Conclusions and questions

The main benefits of VC based financial assets and asset transfers seem to be speed and cost. From the perspective of the user/investor, the speed of VC based financial asset transactions is higher than traditional financial asset transfers and takes place within a couple of hours at most. The cost of transactions seems to be currently somewhere around a couple of Euro cents. Both speed and cost of transactions vary between different VCs.

The benefit of cost and speed equally holds for issuers in terms of listing an asset on an asset exchange. In the case of the NXT asset exchange, a listing currently costs 1000 NXT (currently around 10 Euro) one-off plus transaction costs when sending rewards to investors. Especially for small and medium sized companies this could become an attractive source of funding.

A reduction in costs and an increase in transaction speed should in theory be beneficial for the financial system as whole. Speedier transactions should, all else being equal, decrease counterparty risks. A reduction in costs could attract additional market participants, thus reducing entry barriers and contributing to a more complete financial market.

The risks of VC based financial assets/securities for investors consist mainly of the risks associated with virtual currencies in general. Apart from that, investors are subject to exchange rate risk when investing in VC based financial assets/securities. Furthermore, it is unclear how enforceable claims based on VC based financial assets/securities would be in practice for investors. Another risk could be the irreversibility of transactions which is a feature of most VCs. If investors put in a wrong address when sending buy orders they may not be able to get the VC units back. Risks to the financial system could result from risks to price stability, financial stability and payment system stability. However, they would only materialise if transactions and holdings in VCs and VC based financial assets became significantly more widespread and start substituting fiat currency. In that scenario, traditional regulated entities such as clearing houses, central securities depositories and others would face significant risks to their existing business models.

As long as actors in the virtual currency environment remain largely unregulated, there is a risk of regulatory arbitrage and competitive distortions, which might lead some investors, issuers and/or intermediaries to shift their investments to the virtual currency space to benefit from lower costs and fewer regulatory constraints.

Other regulatory risks can be listed:

- The fact that many virtual currency actors are not subject to minimum capital requirements, let alone strict prudential requirements, making an insolvency more likely and potentially more damaging for these firms' clients - i.e. investors;
- Market manipulation is also more likely in connection with the value of virtual currencies. In the absence of a strict framework regulating the entities providing valuations of bitcoins and other virtual currencies, there is a risk that virtual currency indices might be manipulated or distorted in a way that could result in major losses for investors;
- The lack of proper "safekeeping" for virtual currency assets in the absence of real "depositaries". As already explained, the maintenance of accounts holding virtual currency assets is done through IT servers. In order to ensure that virtual currency assets are protected from the risk of loss, errors, and the risk of fraud, guarantees would have to be put in place in case these IT servers are attacked.
or compromised. There are precedents of some companies specialized in the safekeeping of bitcoins having been hacked and having subsequently lost important amounts of bitcoins, for which clients were not compensated.

Against this background, the threat to existing business models of securities, exchanges, CCPs and CSDs, is only secondary, and will probably only materialise if virtual currency players remain largely unregulated, i.e. if regulators allow these players to make use of a lighter regulatory regime to compete with existing securities infrastructure providers. Besides, CSDs and other securities infrastructures can actually benefit from some of the opportunities offered by the increasing popularity of virtual currencies. Indeed, Blockchain has caught the imagination of the financial services industry for its potential to overhaul the sprawling and complicated network of bank payments and settlements. It is seen as a way of instantly updating payment ledgers in multiple locations without a single, centralised authority. Banks, exchanges and settlement houses are exploring ways to harness the much-hyped technology to reshape many of their daily operations, from upgrading old back-office systems and outsourcing billions of dollars in costs to automatic execution of contracts.

For example, as quoted in the press, nine of the largest investment banks, including Goldman Sachs, JPMorgan and Credit Suisse, are planning to develop common standards for blockchain technology in an effort to broaden its use across financial services. The group is looking to channel data, ideas and financial backing to a start-up called R3CEV, a New York-based group of trading and technology executives. Barclays, Commonwealth Bank of Australia, State Street, RBS, BBVA and UBS are also backing the initiative, which intends to be an industry utility to accelerate the acceptance of blockchain.

Visa, Nasdaq, Citi and other industry players invested $30 million in Chain.com, a blockchain developer platform that serves an enterprise market. More in detail, in June 24, 2015 Nasdaq announced its partnership with Chain, to leverage the blockchain platform to facilitate the secure issuance and transfer of shares of privately-held companies. This Nasdaq Private Market project aims to simplify the overwhelming challenges private companies face with manual ledger record-keeping. The new partnership with Chain marks the latest milestone on Nasdaq’s exploratory approach to apply blockchain technology across the company. In NASDAQ’s press releases, it is pointed out: “By using the blockchain to represent securities and manage capitalization tables, stockholders can seamlessly transfer securities between entities, and companies and their affiliates can be provided with a complete historical record of issuance and transfer of their securities. Importantly, the use of a blockchain-based distributed ledger can also offer integrity, auditability, issuance governance and transfer of ownership capabilities”.

Again the issue of relevance of corporate ownership for this phenomenon is just quoted but it need to be further analysed.