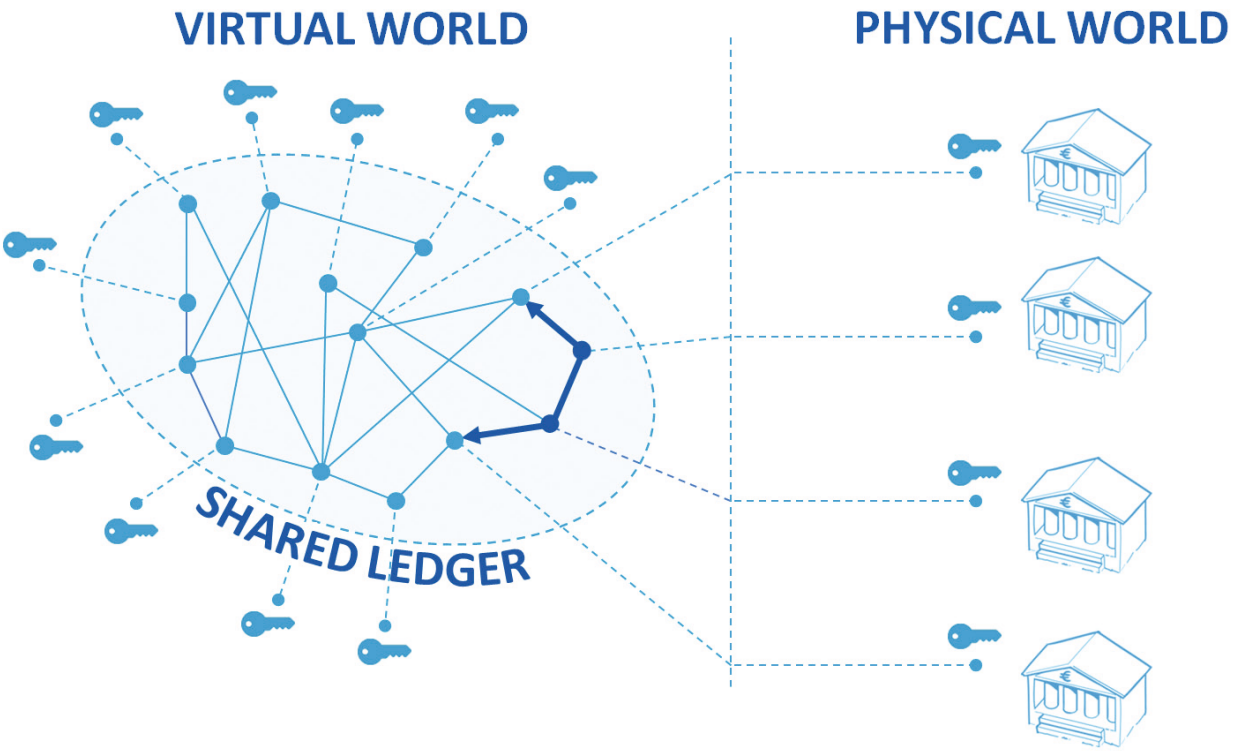
ABE EBA

EURO BANKING ASSOCIATION



Cryptotechnologies, a major IT innovation and catalyst for change:

4 categories, 4 applications and 4 scenarios
An exploration for transaction banking and payments professionals

EBA Working Group on Electronic and Alternative Payments

Version 1.0

11th May 2015

CONTENTS

The information paper is the result of an analysis carried out by the EBA Working Group on Electronic Alternative Payments.

FIGURES AND PICTURES

1. INTRODUCTION AND MANAGEMENT SUMMARY

Major IT innovation: distributed consensus ledgers

Over the past five years, cryptotechnologies have surfaced as major IT innovation with the potential to improve the architecture of systems and processes in a number of digital transaction-based industries. At the core of this invention is the concept of 'distributed consensus ledgers.' These ledgers make it possible to jointly create, evolve and keep track of one repository of transactions or other successive events over a shared network (documenting, for instance, the ownership of value) without maintenance or administration by a central authority. Advances in cryptography, internet performance and computing power are the key enablers of this innovation.

Going beyond bitcoin

Until now, the most salient manifestation of cryptotechnologies has been Bitcoin as a 'cryptocurrency' application. This development bears testimony to the innovative potential of distributed consensus ledgers. Authorities, media and various industry professionals debate its potential, legal implications and chances for survival. Yet, some believe that we have only seen the tip of the iceberg of cryptotechnologies' true potential, which goes far beyond the application of currency and is the focus of the present paper.

The fact that regulatory institutions in Europe, such as the European Banking Authority and the European Central Bank (see section 5. Literature), have issued reports on this topic testifies to the relevance of cryptotechnologies. Similar developments are also taking place outside Europe, the proposed regulation document by the New York State Department of Financial Services being only one example.

Cryptotechnologies for today's practitioners

The Electronic Alternative Payments Working Group (e-APWG) of the Euro Banking Association has identified cryptotechnologies as a subject for further study against the background of evolving financial infrastructures. The present information paper specifically focuses on the practical implications of cryptotechnologies from the perspective of transaction banking and payment professionals for the short to medium term (one to three years).

Four categories of cryptotechnologies

The paper presents an analysis of cryptotechnologies in four relevant application categories. These categories are: 1. currencies, 2. asset registries, 3. application stacks and 4. asset-centric technologies. The paper observes that regulatory and technical maturity issues diminish the *current* utility of three of the four categories (currency, asset registry, application stack). They do, nevertheless, provide compelling future use cases and their developments merit being monitored closely by industry players. As a result, the present information paper focuses on the fourth category: application of asset-centric technologies and its sector-specific use cases. **Figure 1** shows a selection of chronological examples of initiatives that are related to these four different categories.

Four actual use cases for asset-centric technologies that could lead to lower cost, better products and faster time to market

Asset-centric technologies are potentially the most interesting category for the transaction banking and payments domain, both for processes **within** and **between** organisations. Apart from possibly being able to speed up processes and reduce their complexity, cryptotechnology applications in this area can also be integrated with legacy IT, legal frameworks and existing assets (currencies, stock, bonds etc). Therefore, existing financial services could be 'powered by cryptotechnologies' offering financial institutions potentially lower costs, better products and faster time to market. This paper describes four actual use cases: 1. foreign exchange/remittance, 2. real-time payments, 3. documentary trade and 4. asset servicing.

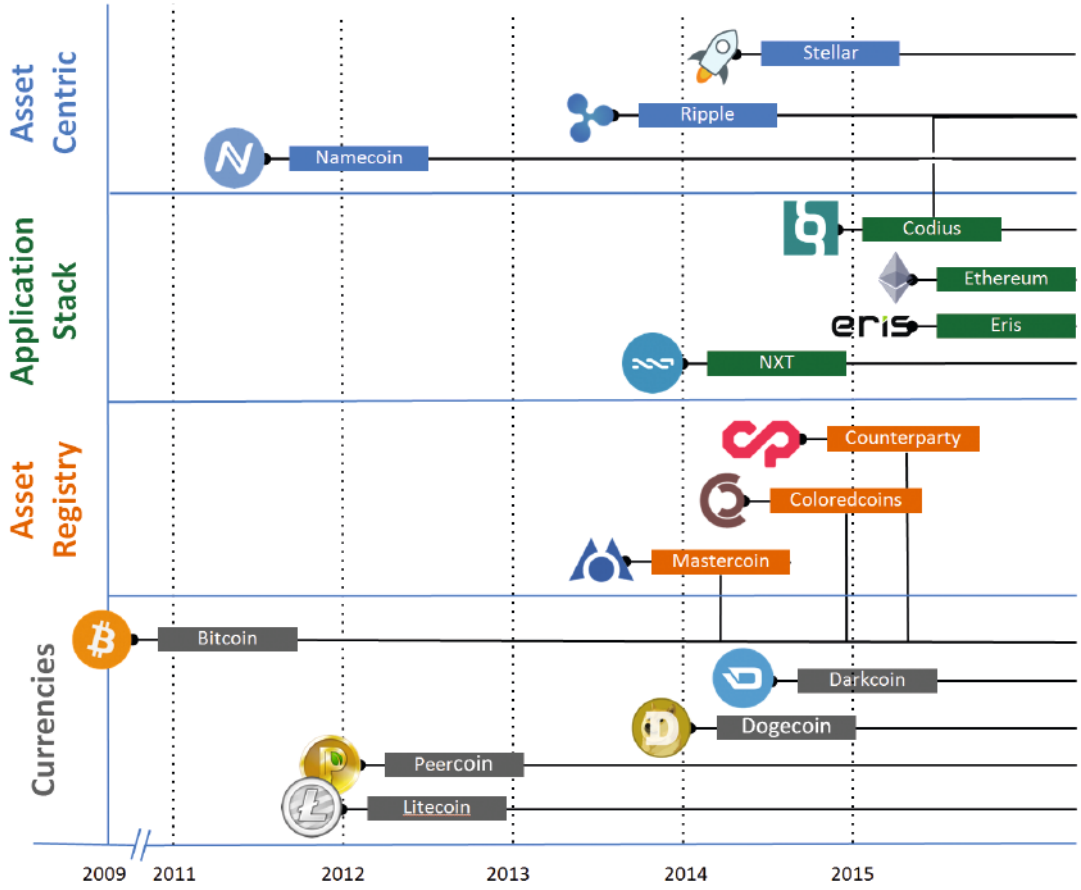


Figure 1: *The four development categories of cryptotechnologies*

Looking forward: industry outlook in four scenarios

Due to the pace of and differing opinions on crypto-technologies, the financial industry has not yet succeeded in developing a unified language and a structure dialogue around cryptotechnologies. This will take time since cryptotechnologies are still in a nascent phase. This paper describes four potential scenarios on how the financial industry and the crypto-technology industry could evolve vis-à-vis each other over time. The scenarios are built around the level of cross-industry cooperation and the actual adoption of cryptotechnologies by the financial industry.

2. FOUR CATEGORIES AND FOUR USE CASES

2.1 Categories of cryptotechnologies and their current relevance for organisations in transaction banking and payments

In broad terms, cryptotechnologies are the combined application of different cryptographic techniques on a decentralised network to create a distributed consensus ledger, which is also known as a blockchain. This distributed consensus ledger presents a singular repository of transactions without the need for centralised control of the ledger itself (a feature referred to as consensus[1]). By means of private/public cryptography, digital assets can be transacted between private/public key holders on the ledger without this taking place under the auspices of any authority.

These digital assets are inextricable to the distributed consensus ledger. The digital assets and their related transactions are respectively created and validated by a process commonly referred to as mining. Mining is done by means of participants in the network providing large amounts of processing power to solve a processing power-intensive mathematical equation. Participants are incentivised to participate based on the fact that being the first to solve the equation allows the participant the right to self-issue a prespecified amount of coins to his/her private address.

The advent of Bitcoin and related cryptotechnologies in 2009 has garnered interest from a myriad of developers. Each group of developers represents a related but different opinion on what the optimal application of distributed consensus ledger technology should be. In combination with the innovative potential of the technology, these different opinions have led to a large amount of differing applications and adaptations of the above-mentioned technology.

For the benefit of the transaction banking and payments industry, an analysis of the current application landscape has been conducted as a basis for the present paper. In this context, the categorisation of cryptotechnology-related applications into 'currencies', 'asset registry', 'application stack' and 'asset-centric technology' has been considered particularly helpful (although other categorisations exist). This categorisation has also prepared the ground for further analysis of cryptotechnology-related applications with a view to identifying potential use cases for PSPs[2].

2.1.1 Currencies

Cryptotechnologies applied in Bitcoin, Litecoin, Peercoin and Dogecoin focus on creating so-called currencies and an associated transfer mechanism. Their applications range from speculations, online and POS transacting and the storage of value (see **Figure 2**). In that respect, the applications are similar to today's fiat currencies, but without the institutional framework (e.g. regulation, legislation, oversight), so it would therefore be more accurate to refer to them as digital assets.

The innovative nature of these applications do provide consumers with certain functions that address key consumer and merchant requirements, namely with regard to reach, conversion and cost. This is reflected in the growing rate of interest and usage these applications enjoy among consumers and merchants globally across multiple channels while their relative market penetration till remains very small. Also, the technological scalability of these applications for a retail transaction environment is still being debated. However, given the potential of cryptocurrencies and the rapidly changing landscape of providers, collective insights and regulatory opinions, it is pertinent for PSPs to stay aware of functional, technical and legal developments in this sphere. An understanding of the currency applications is essential for gaining more advanced knowledge of cryptotechnologies.

[1] Different types of cryptocurrencies make use of different types of mathematical means to achieve consensus. Please refer to the technical primers in the literature section (p. 23).

[2] PSP (Payment Services Provider) is the term commonly used (e.g. in the Payment Services Directive) referring to all parties offering payment services to consumers and commercial clients. PSPs include but are not limited to banks, internet payment gateways and innovative payment platforms.

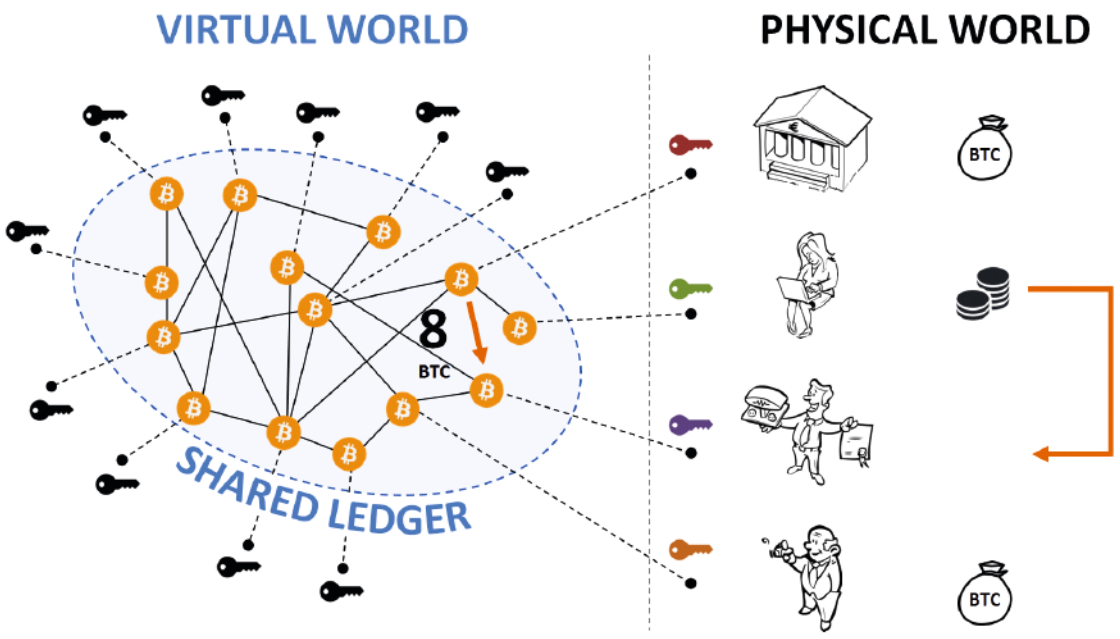


Figure 2: *The currencies category of cryptotechnologies*

Different jurisdictions currently interpret 'cryptocurrencies' in different ways, but draw the same conclusion. The conclusion is that they do not pass the test to become legitimate fiat currencies and do not offer to consumers the same rights and protections of conventional fiat currencies[3]. In light of these currently open questions regarding the appropriateness of cryptocurrencies as core propositions for PSPs, it is not to be expected that this category of "currencies" will gain in major relevance in terms of its practical application in the short term, i.e. within the next one to three years. It is therefore not discussed further in this document.

2.1.2 Asset registry

Asset registries use public ledgers to register assets other than the 'coins' these public ledgers use. By including very small transactions with a reference to an existing asset (e.g. stocks, vehicles, buildings, domain names), the ownership of that particular asset is publicly registered without the need for a central authority. The owner of the private key to that public record is then the owner of that asset. Asset registries have a potential for reduction of governance and auditing cost.

This type of application is commonly referred to as 'Bitcoin 2.0'. Examples are Mastercoin, Coloredcoin, Namecoin and Counterparty.

[3] Readers who wish to know more about the technical properties and legal aspects of cryptocurrencies can refer to the literature section (especially 5.1 and 5.6) of this document. The *Definition* section of the European Banking Authority's *Opinion on 'virtual currencies'* particularly deals with this point. A country-by-country jurisdictional breakdown is also available from the Library of Congress's Global Legal Research Center.

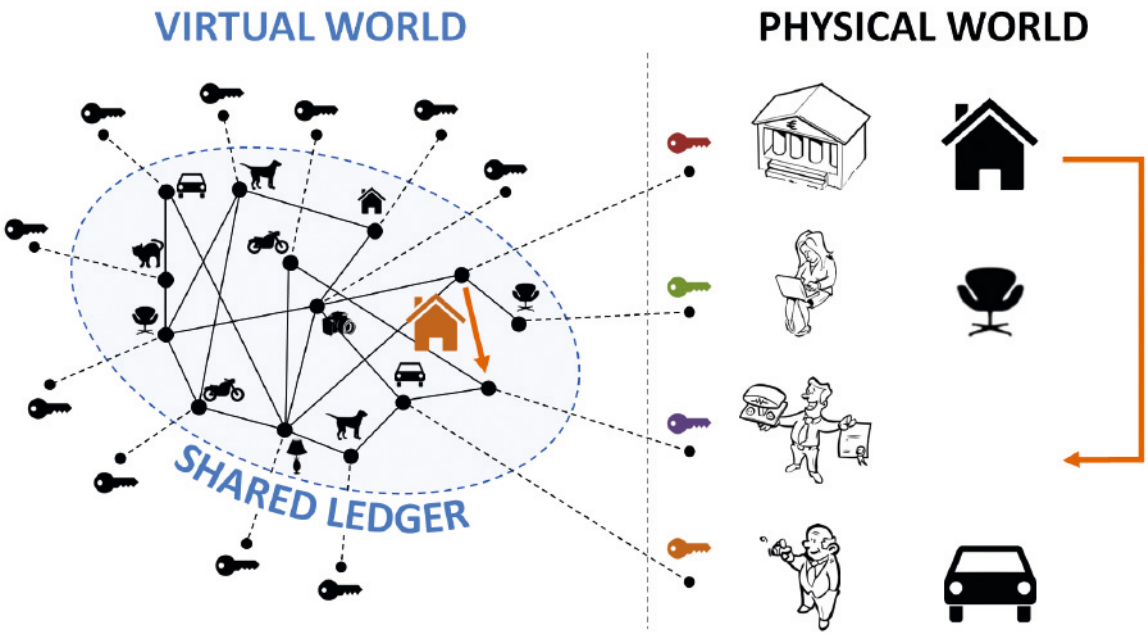


Figure 3: *The asset registry category of cryptotechnologies*

The current technique in which asset registries are realised involves including additional data (i.e. data that is not exclusively meant for transaction validation purposes) in the blockchain[4]. These potentially large amounts of additional data not only affect the underlying network performance in a potentially negative way, additional processing power is also required in order to validate the transactions. This phenomenon of 'blockchain bloat', in combination with the large amounts of transactional data that the financial sector generates, raises concerns with regard to the scalability of applications falling under this category. As a result, one could conclude for the time being that the asset-centric category presently cannot be considered as other than of limited utility for the banking industry.

On the other hand, Factom, a technology that is currently in development, is aimed at addressing these abovementioned issues by using cryptography to pre-process the data before it is written to the blockchain. If the promised efficiencies materialise, then this proposed development, which would support propositions that create and maintain trust warrant careful observation of developments going forward. As applications such as Factom are still under development and recognising the abovementioned technical issues, this category will not be elaborated upon any further in this document.

2.1.3 Application stacks

Applications stacks such as NXT, Ethereum and Eris can be distinguished based on their focus. They are the result of the continuous search for 'non-currency' applications of blockchain technologies.

[4] Cawrey, D. 2014. Why New Forms of Spam Could Bloat Bitcoin's Block Chain. [Online]: http://www.coindesk.com/new-forms-spam-bloat-bitcoins-block-chain/ [Retrieved 15 April 2015].

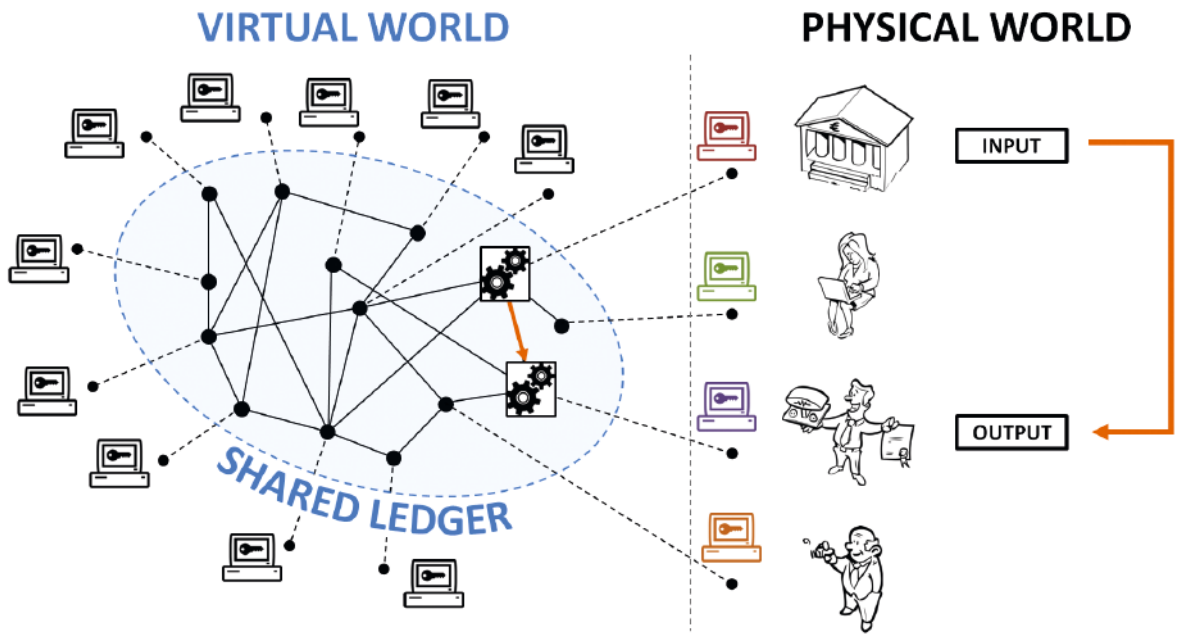


Figure 4: *The application stack category of cryptotechnologies*

The main focus of any application stack is on becoming a platform for the development and execution of complete applications[5] on top of decentralised networks (see **Figure 4**). A close analogy would be to describe application stacks as decentralised versions of what we currently call 'cloud services' as delivered, in non-cryptotechnology environments, by companies such as Amazon and Microsoft.

This technology could hold attractive opportunities for any party involved with payments, especially in relation to the creation of product offerings and the customisability/granularity of these offerings. However, to date, this technology is perceived as immature for banking grade applications and some of these much-anticipated applications have not yet been launched. It is for these reasons that this category will not be discussed further in this document although developments in this category merit ongoing attention.

2.1.4 Asset-centric technologies

Asset-centric technologies such as Ripple, Stellar and Hyperledger focus on the exchange of digital representations of existing assets (e.g. currencies, metals, stock, bonds etc.) in combination with a shared ledger but not on a public leger. Trust is organised between participants directly, so not through a blockchain and mining as is the case with bitcoin.

Key to this approach is that participants in the network commit to 'publishing' digital assets on the network, e.g. in USD, RMB, Gold, Bitcoin. At the same time, some of these participants are responsible for converting these assets (i.e. acting as 'gateways' bridging the gap between the physical and the virtual world). In order to exchange one digital asset for another, the function of the so-called 'market maker' is needed.

In the example in **Figure 5**, a market maker would most likely be a high-volume foreign exchange trading institution.

[5] Readers who are interested in knowing more about these so-called DApps (Distributed Applications) and DAO (Distributed Autonomous Organisations) can refer to a list of technical primers in the literature section (p. 23).

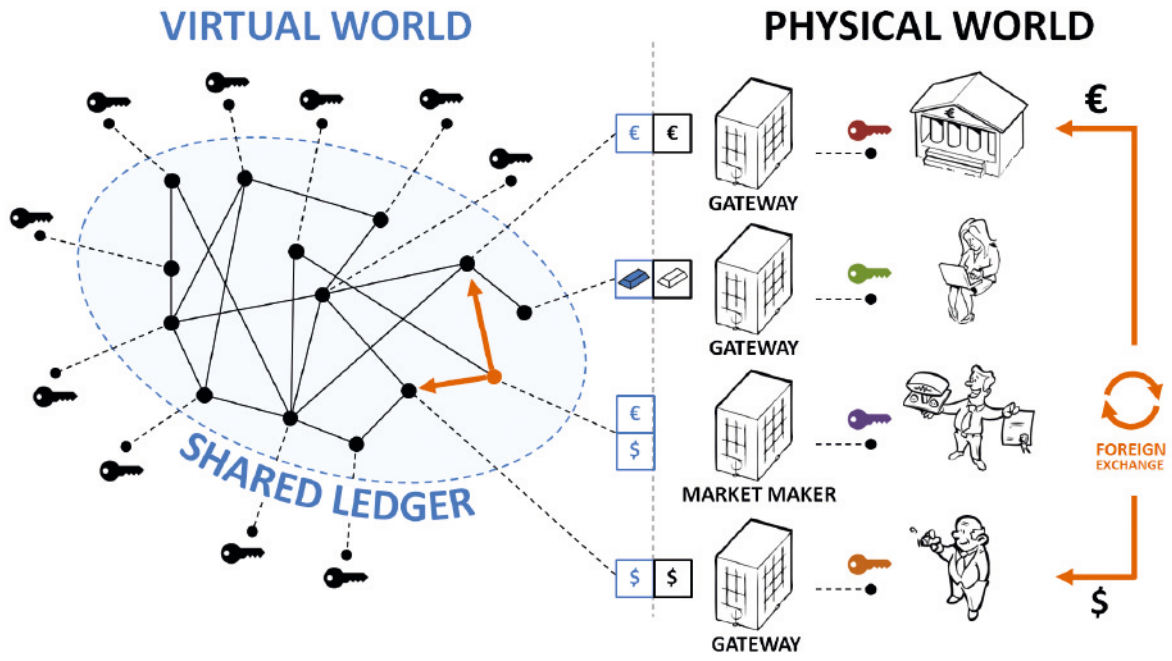


Figure 5: *The asset-centric category of cryptotechnologies*

Exclusive exchange agreements between nodes of these networks can be created. In other words, a PSP can participate in the network with trusted partners on an exclusive basis without risking exposure to the activities of unscrupulous third parties.

Asset-centric technologies enable novel efficiencies (e.g. real-time processes) in different areas, such as foreign exchange/remittances, documentary trade, inter-PSP transactions and asset servicing. Innovative vendors are currently developing software that they market as supporting banks and other organisations in leveraging the opportunities for cost reduction, better products and faster time to market that come with reaping these efficiencies.

As outlined in the three preceding sections, the regulatory and technical maturity issues that still affect the 'currency', 'asset registry' and 'application-stack' categories of crypto-technology applications have delisted them from further analysis in this paper.

The remainder of this document will focus on outlining, for this fourth 'asset-centric' category, specific use cases with a view to illustrating the potential applicability of cryptotechnologies to four PSP relevant applications, namely: 1. foreign exchange and remittances, 2. real-time payments, 3. documentary trade and 4. asset servicing.

2.2 The four use cases of asset-centric cryptotechnologies

The potential use cases for 'asset-centric' applications are expected to focus on two waves of innovation. The first wave will concentrate on deeper automation of existing processes. The second will arise from new innovations based on the application of the exclusive features of cryptotechnologies. The use cases in this section primarily refer to the first wave of innovation, because this could have impact within the short to medium term (one to three year).

2.2.1 Foreign exchange and remittance

Foreign exchange (Forex) transactions and remittances can be improved in terms of speed and efficiency through asset-centric cryptotechnologies, potentially forming an alternative for today's involvement of the various PSPs and clearing and settlement mechanisms.

Today, a small European bank that offers Forex transactions to the US sends its customer's funds to a larger bank that has the means to maintain a nostro account with another bank in the US. The US-based bank receives the funds and sends them onward to the receiving party's bank of choice. Each link in this chain of intermediation adds risk as well as extra time and cost to the process. This complexity and the related risk increase with the execution of Forex transactions between less traded currency pairs. The situation is similar for remittance transactions involving an under-banked society on the receiving side with the additional complexity of physical banking infrastructures such as ATMs and branches not being widely available.

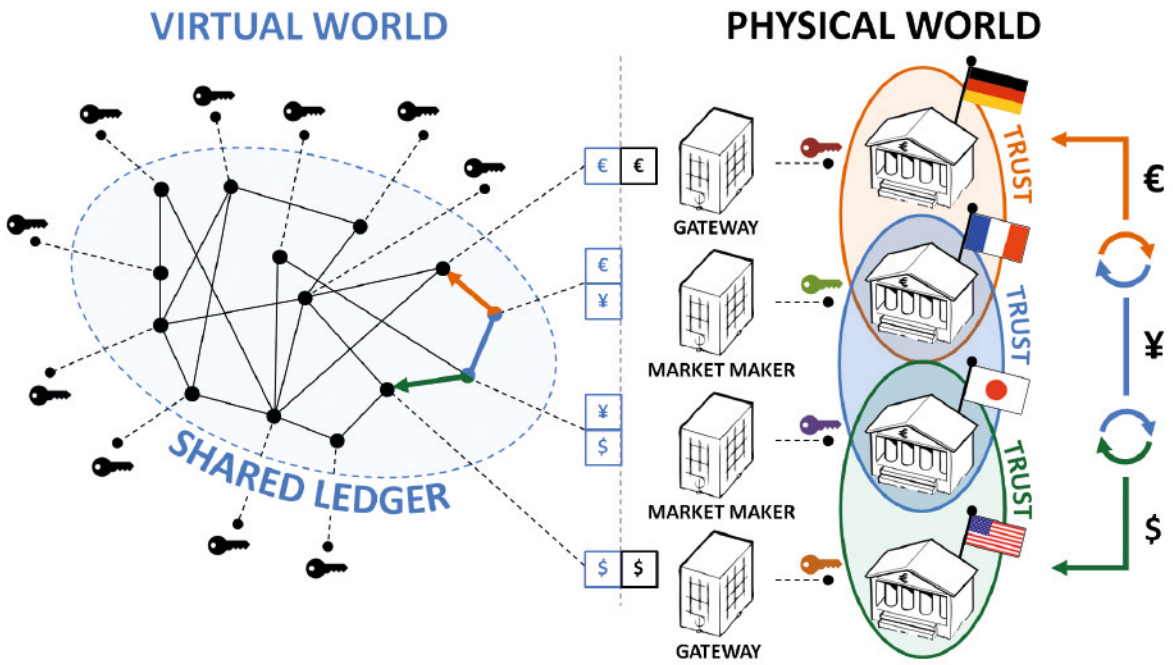


Figure 6: *Foreign exchange and remittance via an asset-centric network*

When performing Forex on a distributed consensus ledger, PSPs in different jurisdictions can act as (or use an existing) gateway to this ledger. The gateway 'publishes' the digital asset and has to hold the asset as collateral in the fiat currency or securities system. Once gateways (PSPs) have set up bilateral trust, they can trade in real time between each other. They can also use so-called 'market makers', which are trade assets, in order to provide market liquidity where needed. As such, they provide the 'bridge' for (some of the) transactions on the network.

In the Forex and remittance sphere, such an approach would offer three key benefits to all parties involved:

1. Positions of the participating PSPs in the various asset classes vis-à-vis each other are maintained in real time.

2. Technical on-boarding across jurisdictions could potentially be cheaper. However, the necessary trust between the contracting parties must be created and/or maintained, as is commonplace today.

3. Lower expenses would be required for the maintenance, governance, security and auditing of such a network when compared to the cost arising in current networks – while achieving similar levels of trust.

Fidor Bank's use of Ripple

Since 2014, Fidor Bank from Germany has been offering to its customers instant Euro/USD FX transactions at low cost by implementing an open-source, internet-based settlement technology from Ripple Labs.

In addition to the potential benefits of a distributed consensus ledger discussed in the abovementioned section, this technology also offers the following features:

- **Trust lines**: For practical and legal reasons, the type of open participation provided by networks such as Bitcoin is often not seen as a suitable option for PSPs. The Ripple framework addresses this issue by allowing PSPs to create exclusive trading relationships with other PSPs. For instance, Fidor has a trust relationship with a US-based PSP. Another nascent consensus-based application called Hyperledger addresses this issue by creating exclusive exchange pools with customised rules.

- **Market maker participation**: Although liabilities can be exchanged between PSPs, one currency-denoted liability still needs to be exchanged for another. In the Ripple framework, FX exchange traders are added to a network as a third party. So if Fidor sends a Euro transaction to its US counterparty, the transaction is relayed through an FX trader that is willing to exchange the EUR amount of Fidor for a USD amount to be credited to the beneficiary institution. PSPs can also add FX traders to their trusted network so they only have to transact with trusted parties.

- **An intermediary asset**: Liquidity is essential in transaction networks. In conventional Forex markets, direct demand between currency pairs is mandatory for the execution of a transaction. This is problematic for transactions involving infrequently-traded currency pairs. Ripple makes use of an intermediary asset that can be used in these types of transactions. Because of the use of an intermediary currency, there only needs to be liquidity in the market between the two currencies and the intermediary asset for the trade to become executable. The network has a smart transactional routing feature to ensure that this extra step adds no complexity for the transacting parties.

- **KYC/AML compliance:** FX propositions using Asset Centric Cryptotechnology solutions are subject to the same AML/KYC requirements as apply to existing FX solutions.

- **Remittance**: In the context of cryptotechnologies, facilitating remittance transactions becomes an issue of basic network access. 37coins has developed a novel means of making the Bitcoin network accessible to phones that only have a text (sms) functionality by sending a text message to a local smartphone that triggers the runing of the 37coins gateway application. A similar construction could be used to support remittance functionality.

2.2.2 Real-time payments

Ongoing developments in cryptotechnologies merit close attention in the context of the current European drive towards achieving "instant payments" and in relation to inter-PSP payment systems in general.

One often-cited example is that a distributed consensus ledger could be set up where a central bank acts as the single market maker and as backer of the digital liabilities with fiat currencies. Netting between participating PSPs would then happen on a continuous basis and as a result less funds would have to be cleared eventually. Stepping up the efficiency and frequency of clearing cycles paves the way towards instant payments. The following paragraphs and explanatory section elaborate on how cryptotechnology could potentially be used in this respect.

Today's process is the result of a historical evolution: In cases where a payment is sent from one account at a PSP to another account at the same PSP, the processing and settlement is done on an in-house or intrabank[6] basis. For payments between clients or accounts at the same PSP, this movement of funds results in zero change in the PSP's overall monetary balance.

Many payments between accounts at different PSPs lead to a considerable change in the monetary balance on an interbank basis. Arising from the requirement for PSPs to maintain reserve ratios, this change in monetary balance needs to be managed on a constant basis. International interbank changes in monetary balances due to cross-border payments are cleared in a similar fashion by a monetary authority such as the European Central Bank or the US Federal Reserve Bank for respective Euro/USD Forex transactions.

At a procedural level, this process requires an intricate coordination of resource-intensive steps, especially with regard to the necessary processing capacity and organisational effort involved. Accordingly, these steps are typically not executed at a constant basis, but several times a day in processing cycles. This observation is valid for both clearing and settlement. The outcome of it is that payments are often only credited one or more days after their initiation. This is especially true if cut-off times for same-day processing are not adhered to, if payments need to follow complex routes before reaching their final beneficiary, in the case of cross-currency payments or in case of weekends, holidays and other days that are not interbank business days. The intricacy of the current procedures highlights that international real-time payments constitute a sophisticated challenge to many PSPs.

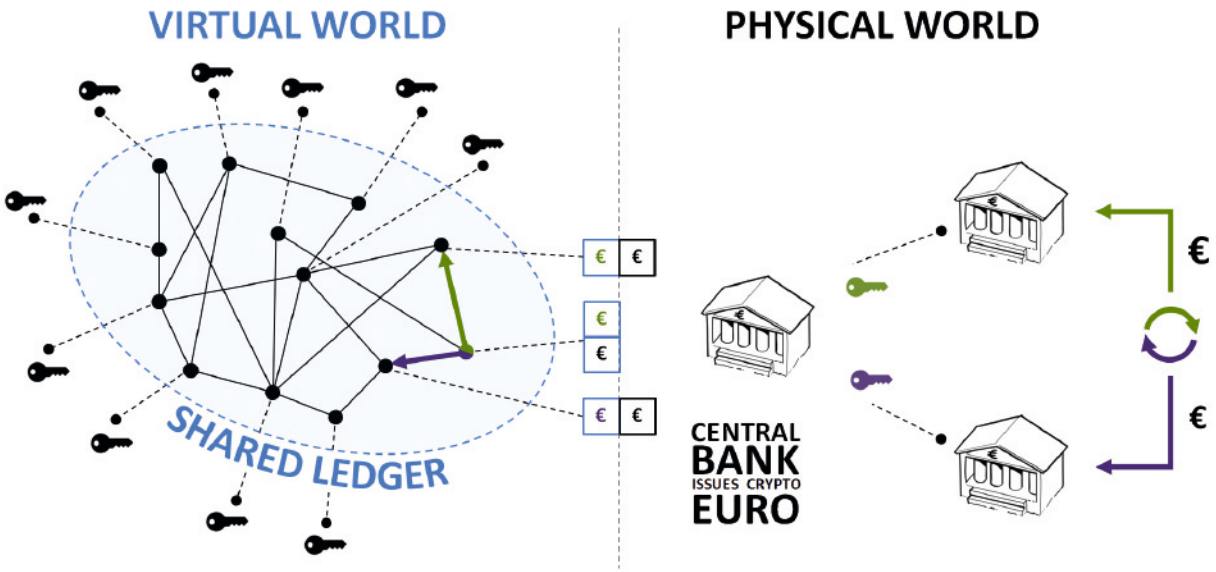


Figure 7: *Real-time payment via a shared consensus ledger*

[6] The widespread adoption of a technology is dependent on how well it meets the needs of the end-user. In keeping with this customer-centric approach, the distinction between inter/intrabank, for the purpose of the paper, is also based on the perception of the average customer. Therefore, if an international affiliate of a local bank is perceived to deliver a service to its customers, the process can still be described as intrabank (this is despite the possible amount of clearing infrastructures). If a service were delivered by means of co-operation between two entities that are distinct and separate in the perception of the customer then this process is an interbank process.

Real-time payments – implementing a cryptotechnology network at an international inter-PSP level

Completing more clearing cycles is often seen as being the key to real-time international payments. One potential future way of meeting this technical challenge is by through the implementation of distributed consensus technology at an inter-PSP level by the PSPs themselves or by their respective automatic clearing houses.

In section 2.2.1, Fidor Bank's use of Ripple for FX transactions was discussed. It was found that one of the advantages of a shared ledger hosted on a decentralised network is constant maintenance of the balances of different asset-related liabilities between transacting parties. This is achieved by means of the combination of trust lines, FX market maker participation, optimised routing, the usage of an intermediary asset as well as the provision of functionality to ensure KYC/AML compliance. This was shown to hold considerable efficiencies in the FX payments sphere. These efficiencies are not of exclusive applicability to the FX transactions but also to single currency interbank/inter-PSP transactions.

If a group of PSPs and their payment infrastructure provider(s) decide to create a trusted cryptotechnology network, leveraging an asset-centric framework (e.g. Ripple), and launch a digital asset that all parties agree upon as being representative of the same liability, then this network could be used for the execution of inter-PSP payments. In such a situation, the earlier efficiencies ascribed to cryptotechnologies could be leveraged to achieve a constantly netted position of inter-PSP balances to the extent that clearing and settlement could be achieved in a very efficient manner.

To achieve this on an international scale would mean the introduction of FX market makers to the trust network to perform exchanges between consumer bank accounts. Central bank participation on the network in a market maker capacity would also be needed between PSPs in different currency jurisdictions. In this way, real-time payments could potentially be achieved on a cost-effective basis.

2.2.3 Documentary trade

While PSPs have adapted their legacy systems by embracing digitisation and automation at an early stage, their updated processes are still very much based on the logic and logistics related to the handling of physical documents (often referred to as dematerialisation). As this paradigm remains at the core of PSP IT infrastructures, many PSPs so far have not been in a position to leverage the full potential of digitisation and automation.

By way of example, documentary trade processes such as open account, letters of credit and consignment are distinct and separate processes at an IT and procedural level in PSPs. This is despite the fact that they all share the following basic components:

- Extension of credit to customer;
- Communication of credit status of customer to vendor;
- Communication channel between banks;
- Communication of goods forwarding/receipt from freight forwarder;
- Execution of the (partial) payment of funds to a vendor when certain criteria are met (e.g. goods have been received or shipped, or a particular date has been reached).

Today's documentary tasks could be further automated with the support of cryptotechnologies. This could be realised through distinct features of cryptography, such as multi-signature wallets and full end-to-end process transparency for all participants (PSPs, vendor, customer). The automation of the process around a 'conditional' payment could be taken to the next level, and related oversight and security costs could be reduced further. Last but not least, more customised and easy-to-use services for corporates could be envisaged.

A side note on addresses and wallets

Cryptographic keys are used to sign cryptotechnology transactions. This is analogous to a signature on a cheque. Ownership of the keys provides access to the 'transaction outputs' (digital assets) stored under the 'address' (account). These keys are also needed to generate 'transaction outputs' (spend the assets). Wallets do not store the assets themselves but they generate, manage and store the needed cryptographic keys.

Added functionality enables some 'addresses' to require extra inputs before the digital assets in them can be accessed. The most common implementation of this functionality is known as 'multi-signature.' This is where more than one signature is needed to access the digital assets. Ownership of these signatures can be granted based on real-world events, such as the receipt of a parcel by a freight-forwarder. Wallets that manage these transactions are commonly referred to as multi-signature wallets.

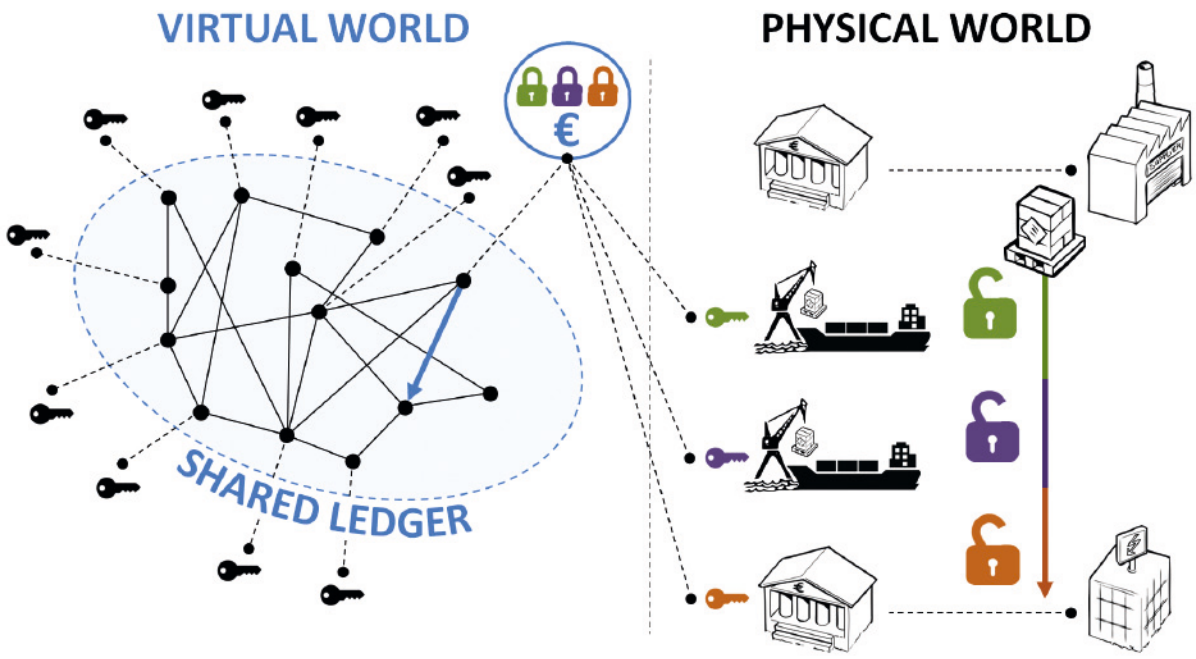


Figure 8: *Documentary trade via a multi-signature wallet*

Figure 8 shows a schematic representation of the use of a shared ledger with transaction automation (through multi-signature) for documentary trade.

Letter of credit example

Letters of credit are often used in international trade when a customer's credit information is not available but a bank with an acceptable credit record is willing to fund the transaction after specific conditions are met. Despite being an international trade mainstay, this is usually a seven-step process with the constant risk of default based on documentary compliance issues.

This process could be made more efficient (refer to **Figure 8**) through the use of a multi-signature wallet (a wallet that only executes a pre-programmed transaction after the application of multiple different cryptographic keys to it). For instance, a customer goes to bank A to request a letter of credit to buy a certain item from a vendor from bank B using a certain freight forwarder that delivers to a specific harbour.

This is a very complex letter of credit but by using a multi-signature wallet the transaction gets executed automatically as soon as the minimum numbers of parties have applied their keys to the wallets. All that is needed is a multi-signature wallet, with the funds for the transaction sponsored by Bank B in the wallet, and the provision of all parties with a key to the wallet, which is created and distributed during the letter of credit creation and is activated by scanning a code on the actual physical parcel.

The described approach holds three distinct benefits for the banking and corporate trading partners involved in this transaction:

- The contract is not easily reversible and its terms are only executed when predefined terms are met, which practically eliminates counterparty risk.
- The transacting parties sign off the transaction on a decentralised basis so no time is spent on additional coordination and transaction execution.
- The standardisation by means of an activated token receipt sign-off procedure rules out the possibility of default because of documentary compliance issues.

2.2.4 Asset servicing

In broad terms, asset servicing for shared consensus ledgers refers to three things:

1. The creation of assets (of all sorts, e.g. currencies, bonds, stocks, precious metals);
2. The enablement of trading between partners such as banks and other trading institutions;
3. The eventual liquidation of an investor's position.

Asset servicing can be seen as 'a layer on top' of the shared ledger and deals with the procedural steps to enable asset trading in a legally conform fashion.

This process is made considerably more complex due to coordination between multiple necessary stakeholders (necessary for safeguards related to bankruptcy and insolvency). These stakeholders are:

- **Securities custodian** – This is a large bank that has an actual license to create certain assets.
- **Currencies custodian** – This is an authority that guarantees that the asset is backed by an actual fiat currency so when an investor liquidates his position there are actual funds at his disposal. A bank connected to a shared consensus ledger could fulfil the role of currencies custodian.
- **Originators** – These are smaller banks/investment companies that act as intermediaries by selling these assets to their customers.
- **Investors** – These are the customers of the originators who buy these assets with the goal of turning a long-term or short-term profit.

Over time, this multi-stakeholder interaction has become overly complex due to legacy, prone to error and expensive based on the fact that the separate parties do not maintain a centralised ledger of positions and multiple coordinated steps need to be taken to execute a single change on the ledger. The lack of a uniform platform for asset servicing also leads to an environment of scattered protocols, several exchange platforms and unreliable workarounds. One standardised network, where assets can be created and traded by creating and changing balances on a shared ledger, could potentially address some of these issues without the disintermediation of any stakeholders.

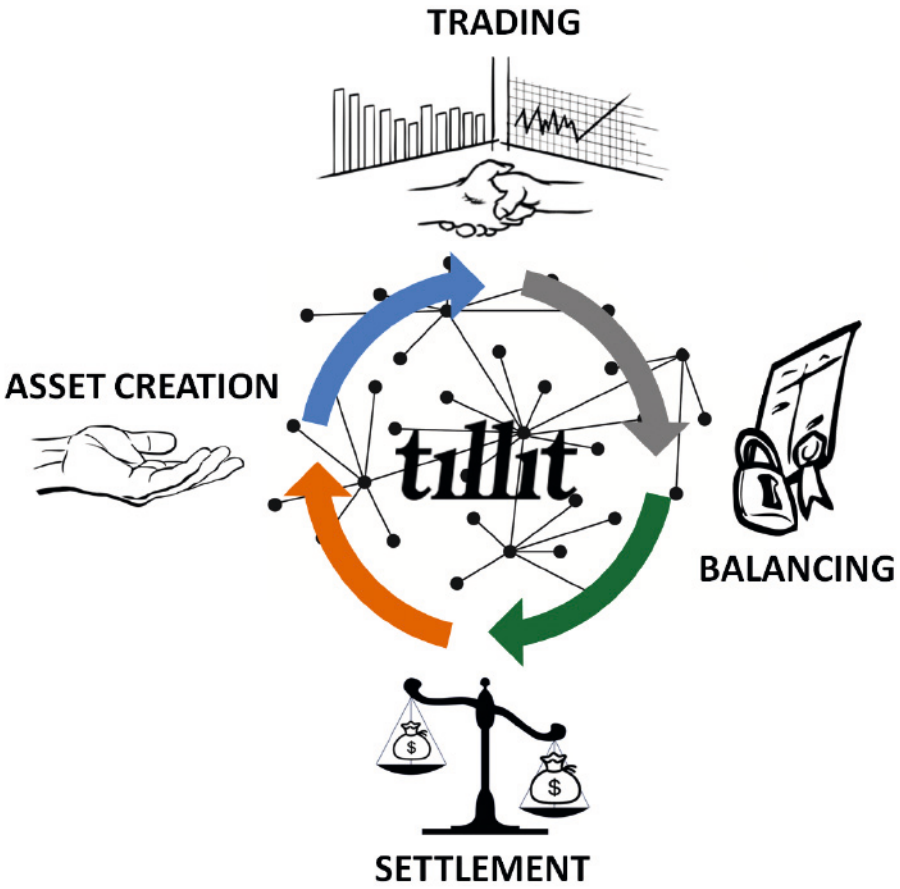


Figure 9: *Asset servicing as layer on top of shared consensus ledgers*

Asset servicing of direct lending assets

We have already discussed the benefits of cryptotechnologies in addressing the general complexities of asset servicing in broader terms. By looking at an application of cryptotechnology by a company called Tillit (see **Figure 9**), which provides asset servicing on top of the Ripple network, the potential benefits can also be observed on a step-by-step basis:

- **Asset creation** – Assets from any asset class (including currencies) can be created on the network with the condition that the trading parties are in agreement and that they are properly backed.
- **Asset trading** – Assets can be traded on the network with a minimal transaction fee in so-called atomic transactions (transactions are either executed or not, so no funds get lost 'in transit'). Enhanced liquidity can also be achieved by means of making use of Ripple's native asset as an intermediary trading asset and combining this with optimised routing of the transactions.
- **Settlement** – The network can also host the currency assets that back the tradable assets. This enables real-time gross settlement (typically refers to an inter-PSP/central bank situation) if an investor wants to liquidate their position.
- **Balance** – Balances are recorded on an undisputable decentralised ledger where positions on the ledger are constantly netted.

From information gathering to analysis

This concludes the section on the different categorisations of cryptotechnologies and the different applications of asset-centric cryptotechnologies. Due to the pace and differing opinions on cryptotechnology-related developments, the transaction banking and payments industry has not been able to develop a unified cognitive framework surrounding these developments. The illustration of banking- and PSP-specific use cases is a starting point for the generation of a better understanding of cryptotechnologies and their applications. The expansion of this understanding through further analysis of cryptotechnology-related developments, the evolution of regulation in this area and the conclusions that banks and other organisations may draw based on their analysis and regulatory monitoring, will impact their decision-making and lead to the unfolding of different industry scenarios. Four plausible industry scenarios are described in the following section.

3. THE FOUR INDUSTRY CRYPTOSCENARIOS

In this section, the potential relationships between the banking industry at large and cryptotechnologies will be discussed as a basis for projecting plausible options for the banking industry's future positioning towards cryptotechnology. Four key scenarios have been identified in this context and will be exposed in connection with their relevant drivers and sub-drivers.

Cooperation, adoption and their respective sub-drivers (communication and regulation) will prove to be decisive factors in whether the banking industry and cryptotechnologies develop together or in parallel (refer to **Figure 10**).

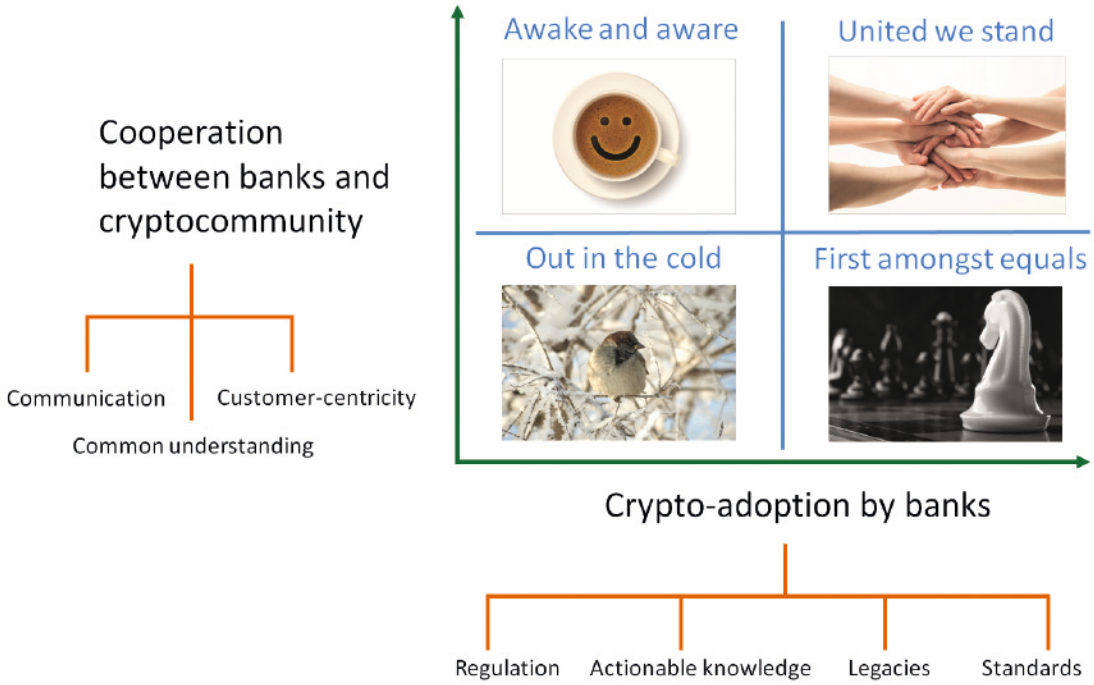


Figure 10: *The levels of cooperation and crypto-adoption and the resultant scenarios*

Due to the interest from the international software development community, venture capital funding and the broad set of possibilities that distributed consensus ledgers offer, cryptotechnologies are by no means just a passing trend. Although it is difficult to predict the exact shape and form that cryptotechnologies will eventually take as well as the areas where they will have an impact and the importance of that impact, one can be assured of ongoing developments in this sphere.

3.1 Drivers and their sub-drivers

The interaction of two variables, namely the level of cooperation (between PSPs and the cryptotechnology community and between PSPs themselves) as well as the level of adoption of cryptotechnology by PSPs, will be the main drivers of cryptoscenarios as they relate to these two sets of market participants into the future. Common understanding and regulation respectively are the most influential sub-drivers. The choice of drivers and sub-drivers has been based on the same concerns, considerations and industry dynamics[7] that were at play when voice over internet protocol (VoIP) applications such as Skype were regarded as a disruptive technology around the year 2005.

[7] Darlington, R. 2005. A guide to voice over internet protocol. [Online]: http://www.rogerdarlington.me.uk/VoIP.html [Retrieved 15 April 2015].

3.1.1 Cooperation and common understanding

Apart from the perceived benefits related to the adoption of cryptotechnologies at an intra-PSP level, the successful implementation of cryptotechnologies is also dependent on outcomes that are more achievable on a cooperative, inter-PSP basis. For instance, a critical mass of participating banks would be needed to ensure interoperability. The requisite amount of market makers and processing power providers are needed to provide liquidity and ensure the scalability of the ledger. Standardisation of communication, identification processes and general rulebook maintenance would possibly be better administered under the auspices of a supranational authority. For the sake of clarity, the minimal requisite amount of inter-PSP cooperation is assumed when applicable to a scenario.

Another type of cooperation, the cooperation between the cryptotechnology community and banks, will not only influence the success of one cryptotechnology implementation but will impact the very level of innovation of cryptotechnologies that PSPs will have access to. Cryptotechnology is a nascent development with innovation in this sector not necessarily coming from a selection of top vendors as with more mature technologies. To be aware of the newest innovations in the sector, cooperation with upcoming vendors, developers and thought leaders is therefore warranted.

Whether it is between PSPs themselves or between PSPs and the cryptocommunity, common understanding is a prerequisite for cooperation. At the PSP level, common understanding would be generated by collective analysis and understanding of cryptocurrencies' capabilities and applications. At the PSP/cryptocommunity level, common understanding would require broad-based knowledge generation on the possibilities of cryptotechnologies to the point where PSPs can also participate, as thought-leading players, in the cryptotechnology sphere on an innovative basis.

3.1.2 Adoption and regulation

For a bank, adopting cryptotechnology does not necessarily equate to an internal implementation of cryptotechnologies. Due to their involvement and experience in the interbank transactional sphere, payment infrastructure providers are especially well suited to provide asset-centric cryptotechnology services in that space. In a circumstance, for example, where a country's central bank decides to issue crypto-euro or crypto-sterling, then the banks in the country could also be said to have adopted cryptotechnologies on a vicarious basis.

Regulation that is specific enough to give proper guidance to all parties but that does not stifle innovation would be seen as a prerequisite for the adoption of cryptotechnology by banks, vicariously or otherwise. The provision of informed analysis to lawmakers/regulators for issuing quality legislation can be interpreted as an industry-wide responsibility.

3.2 The four cryptoscenarios

3.2.1 "Out in the cold" – the creation of a separate cryptoconomy

In this scenario, low levels of cooperation and adoption by PSPs will lead to a positioning of cryptotechnologies (including any future developments in this area) in parallel with PSPs, which will result in the development of a so-called cryptoconomy. Current revenue drivers such as remittances and foreign exchange services are likely to be challenged by cryptotechnology firms during the first wave of innovation.

The application of decentralised trust is most obvious in payments, but essentially any process that currently relies on a centralised ledger of accounts combined with rule-driven changes could potentially be automated and delivered at a fraction of the current cost in an easily governable and auditable manner. Property record keeping, contract execution, escrow, factoring and arguably the management of an individual's share portfolio are prime examples of this. The second wave of innovation could lead to an increase of alternative service offerings in these areas by cryptotechnology firms.

In the 'Out in the cold' scenario, each major change in regulation will also have an inverse effect on revenue streams due to the fact that cryptotechnologies are perceived to be better positioned to take advantage of external changes.

3.2.2 "First amongst equals" – an approach where individual PSPs strive to position themselves as developers of cryptotechnology applications

In this scenario, individual PSPs decide to adopt cryptotechnologies, but due to organisational, cultural and strategic differences, they do not wish to collaborate with the cryptotechnology community or, indeed, with other PSPs. This may leave these PSPs in the situation of reinventing the wheel at a large expense to themselves. In this scenario, the PSP would also have less access to information about the most recent developments and given the limited resources of their individual innovation departments vis-à-vis an international open source network they would most likely find themselves in a (fast) follower position by default.

3.2.3 "Awake and aware" – a collaborative approach based on constant dialogue and possible partnerships in selective areas

In this collaborative scenario, PSPs engage in constant dialogue with the cryptotechnology community. Due to the novelty of the technology and the nature of the regulatory and compliance process, full adoption is unlikely to emerge.

The in-house legal counsel of the PSPs will play an important role in this scenario. Not only do the legal teams need to understand what the latest developments in regulations with regard to cryptotechnology could mean for their organisation, they also need to anticipate changes and develop regulatory roadmaps so that PSPs and their cryptographic partners can adapt to the changes in regulations as they develop.

Germany's Fidor bank – awake and aware

Fidor Bank AG from Germany is an example of a bank that leverages the latest regulation to pro-vide cryptotechnology-powered services to its customers.

In Germany, cryptotechnology's digital assets have been identified as *accounting units*. Regulation has allowed Fidor to partner with the value transfer protocol Ripple. Fidor has benefitted from its partnership with Ripple by means of substan-tially lowered foreign exchange costs.

3.2.4 "United we stand" – a collaborative approach based on partnerships between PSPs and the cryptotechnology community embracing a successful integration of processes

In regions where regulation allows for the adoption of cryptotechnologies, PSPs that decide to enter into partnerships with the cryptotechnology community may benefit. These PSPs will not only observe which developments are on the long-term horizon, they are also likely to be better positioned to take advantage of new developments in this sphere when the technology reaches maturity.

Undoubtedly, the cryptotechnology community in turn will benefit from the PSPs' legitimacy and procedural knowledge. Banking customers are likely to benefit from the added reach without the expense of maintaining another financial relationship. The banking interface that customers know can continue to be used.

A value network – a collection of agreements regarding the expected result and each partner's expected contribution – will be a fundamental part of a successful integration. The reason for this is that such an integration would most likely be needed among multiple and diverse partners.

4. CONCLUSION

This information paper has been written with the purpose of informing the members of the EBA Electronic Alternative Payments Working Group, the EBA membership as well as interested stakeholders about the possibilities of cryptotechnologies in the short to medium term (one to three years). This has been achieved by providing an assessment of the generic developments of cryptotechnologies in the most relevant areas. Four categories of cryptotechnologies were identified: 1. currencies, 2. asset registries, 3. application stacks and 4. asset-centric technologies. All are distinct manifestations of cryptotechnology with unique merits and differing levels of current applicability to the transaction banking and payments sector.

Currently, asset-centric developments are potentially the most interesting cryptotechnology-related category for transaction banking and the payments industry. This conclusion has been drawn based on the fact that developments in other areas are still impeded by technological and regulatory challenges, even though these other categories also hold considerable future promise. The industry is therefore advised to stay aware of developments in: 1) reach, conversion and cost advantages of currencies and 2) reductions in auditing and governance expenditures from asset-centric as well as 3) radical innovation from application stack cryptotechnologies.

Asset-centric developments have potential and current applicability regarding today's activities of financial service and payment organisations, because they can operate in an integrated fashion with legacy IT, legal frameworks and existing assets (currencies, stock, bonds etc). The use cases (foreign exchange/ remittance, real-time payments, documentary trade and asset servicing) presented in this paper have showcased cryptotechnologies in a more practical context. The categorisation, in combination with the use cases, should benefit the readers of this paper by providing an explanatory structure geared at increasing understanding of ongoing developments in this area.

Technology does not exist nor does it develop in a vacuum. It is subject to institutional norms and dynamics. Comparably, in history few things happen without precedent. By drawing on these insights it has been possible to create potential cryptoscenarios for the transaction banking and payments industry by identifying drivers that were also relevant to voice over internet protocol (VoIP) around the year 2005. Two drivers, namely cooperation (between organisations in the transaction banking and payments industry themselves and between these organisations and the cryptocommunity) as well as adoption of cryptotechnologies, were identified. The combined outcomes of differing degrees of cooperation and adoption led to four broad and plausible scenarios, which have been detailed in this paper.

Cryptotechnologies are still a nascent area of innovation. Together with emerging and future technical developments in this area, the impact (and speed of impact) of cryptotechnologies on the transaction and payments industry will very much depend on the future cooperation models as well as the adoption of cryptotechnology-fuelled applications by existing or new market players. What can be safely said at this point in time is that cryptotechnologies are an area to be closely monitored and revisited for further analysis.

5. LITERATURE

5.1 Books

Essentials on cryptocurrency technology and its application on a more technical basis and inner workings:

Antonopoulos A.M., 2014. *Mastering Bitcoin*. [e-book]. O'Reilly Media. Available through: Chimera Labs website <http://chimera.labs.oreilly.com/books/1234000001802/index.html>

Thorough description beyond cryptocurrencies covering a wide variety of topics and future applications:

Swan M., 2015. *Blockchain Blueprint for a New Economy*. O'Reilly Media.

Information on how Ripple works and its key features, benefits and applications:

Ripple Labs, 2015. *Ripple Executive Summary*. [online]. Available at: <https://ripple.com/files/ripple_executive_summary.pdf>

Ripple Labs, 2014. *Ripple for financial institutions*. [online]. Available at: <https://ripple.com/files/ripple_deep_dive_for_financial_professionals.pdf>

5.2 Blogs

The executive architect for banking innovation at IBM UK:

Gendal, R., 2015. *Thoughts on the future of finance*. [blog]. Available at: <http://gendal.me>

5.3 Magazine and news sites

Although this list refers to dedicated sources, it should be noted that other more mainstream publications such as *Time*, *The Economist* and *The Wall Street Journal* regularly report on cryptotechnology-related developments.

Magazine and news sites with a good balance between news and commentary:

Bitcoin Magazine, 2015. *Bitcoin and Cryptocurrency News*. [online]. Available at: <https://bitcoinmagazine.com/>

One of the most comprehensive news sites on cryptotechnology developments and detailed analytics in the cryptotechnology market:

Coindesk, 2015. *Bitcoin News, Prices, Charts, Guides & Analysis*. [online]. Available at: <http://www.coindesk.com>

Independent cryptotechnology news source with an informative "For Beginners" section:

The Cointelegraph, 2015. *Bitcoin for Beginners*. [online]. Available at: <http://cointelegraph.com/bitcoin-for-beginners>

5.4 Audio

Around the Coin, 2015. *Podcast about Fintech, Banking and Payments*. [podcast]. Available at: <http://www.aroundthecoin.com/>

Let's Talk Bitcoin, 2015. *Lets Talk Bitcoin*. [podcast]. Available at: <https://letstalkbitcoin.com/>

5.5 Forums

Question and answer formatted forum with a dedicated cryptotechnology section

Quora, 2015. *Cryptocurrencies*. [Q&A forum]. Available at: <http://www.quora.com/Cryptocurrencies>

5.6 Relevant official documentation

European Central Bank, 2012. *Virtual Currency Schemes*. Frankurt am Main: European Central Bank. Available at: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

European Banking Authority, 2014. *EBA Opinion on 'virtual currencies*'. London: European Banking Authority. Available at:
<https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>

New York State Department of Financial Services proposed regulation Title 23 Section 200 of July 2014 on Virtual Currencies. Available at: <http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf>

New York State Department of Financial Services, 2014. *NY DFS releases proposed bitlicense regulatory framework for virtual currency firms*. [Press release]. Available at:
<http://www.dfs.ny.gov/about/press2014/pr1407171.html>

The Law Library of Congress Global Legal Research Center, 2015. Regulation of Bitcoin in Selected Jurisdiction. [online]. Available at: <http://www.loc.gov/law/help/bitcoin-survey/>

5.7 Videos

Financial Times, 2015. *How bitcoin and its blockchain work*. [online video]. Available at:
<https://www.youtube.com/watch?v=f7iXTyHGYX4>

intobitcoin, 2014. *The real value of bitcoin and crypto currency technology*. [online video]. Available at:
<https://www.youtube.com/watch?v=YIVAIuSL9SU>

ABE EBA

EURO BANKING ASSOCIATION

Contact details

For any additional information, please contact:

Daniel Szmukler
Director
d.szmukler@abe-eba.eu

Euro Banking Association (EBA)
40 rue de Courcelles
F - 75008 Paris
TVA (VAT) n°: FR 12337899694

layout: www.quadratpunkt.de
Illustration: © www.innopay.com
photo credit: © www.shutterstock.com
/ Dima Sobko, Antonio-I,
Maryna Pleshkun, vaselenka