TDL | Trust in Digital Life

Blockchain: Perspectives on Research, Technology & Policy

A TDL Working Group Publication
March 2017
Version 1.0

EDITORS
Claire Vishik, Ghassan Karame,
Riccardo Masucci, David Goodman

CONTRIBUTORS
Eduard de Jong, Stefan Bumerl,
Michael Huth, Niels Vandezande

Contents

1 Introduction

Blockchain technology has captured the imagination of technologists, investors, and policy makers. Thrown into prominence by the success of Bitcoin, it has created interest in other applications that could be decentralized well as new security models that have been discussed for decades, but mostly as theoretical possibilities. The number of research papers associated with Bitcoin and blockchain has skyrocketed, and a growing number of startups, in the US and elsewhere, have appeared. Open source activities associated with blockchain approaches have become more prominent and now boast the participation of technology giants such as Cisco, IBM and Intel.

Governments have conducted studies of crypto-currencies and blockchain applications. The UK, US and other nations have published reports evaluating technology and regulatory issues in blockchain application areas. The first regulations associated with crypto-currencies have appeared. At the same time, the first non-financial services based on blockchain have made their appearance, with implementations in Estonia and experiments in the Gulf states.

We consider blockchain an important technology direction that requires extensive research. This paper puts this technology in perspective with regard to technical and regulatory priorities in a number of application areas, not limited to finance. We hope the paper when completed will be of use to the technology and regulatory communities as an instrument to build understanding and improve the prioritization of blockchain-related matters.

The paper will also serve as a foundation for future work, highlighting areas that were identified as potential research and policy priorities during the course of the initial discussions at the formation of the TDL Blockchain Working Group.

2
Blockchain technologies, history and other applications

This section describes in a simplified way the foundations of blockchain technologies.

2.1 Definition of Blockchain

According to Wikipedia [1],

> A **block chain** or **blockchain** is a distributed database, introduced in Bitcoin, that maintains a continuously-growing list of data records that each refer to previous items on this list and is thus hardened against tampering and revision

The approach gained prominence following the emergence of Bitcoin, but elements of blockchain have been discussed by researchers for decades. The blockchain consists of blocks that hold time-stamped batches of transactions. Each block contains a hash of the previous block, thus forming a chain that holds a record of prior transactions and provides a level of guarantee for the integrity of the transaction space.

There are at this point a number of diverse applications of blockchain that are discussed in later sections. A prominent application is its use for distributed databases, sometimes called Blockchain 2.0, to separate the class of issues from those associated with Bitcoin systems.

2.2 Open and restricted participation

An important parameter in blockchain systems that extends beyond the technology is the nature of participation: open or restricted. Peer-to-peer is the prevalent model to realise a collaborative system, in which individual, independent operators join up some of their computing resources to provide a service such as file sharing. This model is characterised by openness: anyone can participate without being vetted and with only minimal technical and operational requirements.

Open participation makes a system of collaboration processing nodes vulnerable to two types of attacks. A Sybil attack, where a single operator participates as multiple independent ones and a Byzantine attack, where an operator attempts to disrupt a process, most likely for personal gain.

Restricting participation in a collaborative system to parties who are known as trusted is a way to counteract the threats arising from open participation. However, implementing a mechanism to vet a prospective participant necessitates some form of authority. How such an authority can be implemented within a system that consists of 'peers' is an open issue.

Restrictions can also exist as technical or operational requirements for effective participation; that is, while participation is open in principle, only those with sufficient resources can actually benefit from the services provided by the collaborative system. The miner network in blockchain is an example of where high technical requirements for effective participation have emerged.

2.3 Financial applications – including Bitcoin

2.3.1 Bitcoin

Bitcoin is a decentralized peer-to-peer payment system that was introduced in 2008. Electronic payments are performed by generating transactions that transfer Bitcoin coins (BTCs) among Bitcoin peers. These peers are referenced in each transaction by means of virtual pseudonyms – referred to as Bitcoin addresses. Each address is mapped through a transformation function to a unique public/private key pair.

These keys are used to transfer the ownership of BTCs among addresses. Peers transfer coins to each other by issuing a transaction. A transaction is formed by digitally signing a hash of the previous transaction where this coin was last spent along with the public key of the future owner and incorporating this signature in the coin. Transactions take as input the references to the output of another transaction which spends the same coins, and outputs the list of addresses which can collect the transferred coins. Any peer can verify the authenticity of a BTC by checking the chain of signatures.

Transactions are included in Bitcoin blocks that are broadcast in the entire network. To prevent double-spending of the same BTC, Bitcoin relies on the assumption that there is synchronous communication along with a hash-based Proof of Work (PoW) concept. More specifically, to generate a block, Bitcoin peers, or miners, must find a nonce value that, when hashed with additional fields (i.e., the Merkle hash of all valid and received transactions, the hash of the previous block and a timestamp), the result is below a given target value.

If such a nonce is found, miners then include it (as well as the additional fields in a new block) thus allowing any entity to verify the PoW. Upon successfully generating a block, a miner is granted a number of BTCs (25 new BTCs after 210,000 blocks. This provides an incentive for miners to continuously support Bitcoin. The resulting block is forwarded to all peers in the network, who can then check its correctness by verifying the hash computation.

If the block is deemed to be *valid*, then peers append it to their previously accepted blocks. Since each block links to the previously generated block, the Bitcoin blockchain grows upon the generation of a new block in the network.

Note that when miners do not share the same view in the network (e.g., due to network partitioning), they might work on different blockchains, thus resulting in *forks* in the blockchain. Block forks are inherently resolved by the Bitcoin system; the longest blockchain will eventually prevail. On rare occasions, Bitcoin developers can force one chain to be adopted at the expense of others.

2.3.2 Ripple

The wide success of Bitcoin has led to a surge of a large number of alternative crypto-currencies. These include Litecoin, Dogecoin, Ripple and others.

Most of these currencies are built on top of the Bitcoin blockchain and try to address some of the shortcomings of Bitcoin. For example, Litecoin primarily differs from Bitcoin by having a smaller block generation time and a larger number of coin bases.

While most of these digital currencies are based on Bitcoin, Ripple has evolved almost completely independently of Bitcoin (and its various forks. Currently, Ripple Labs holds the second highest market cap after Bitcoin and recently finalized the financing of an additional 30 million USD funding round to support its growth and development.

Ripple does not only offer an alternative currency, XRP, but also promises to facilitate the exchange between currencies within its network. Although Ripple is built upon an open source decentralized consensus protocol, the current deployment of Ripple is solely managed by Ripple Labs. In 2015, Ripple claimed to have a total network value of approximately 960 million USD with an average of almost 170 accounts created every day since the launch of the system.

Moreover, there are currently a number of businesses that are built around the Ripple system. For instance, the International Ripple Business Association currently deploys a handful of Ripple gateways, market makers, exchangers and merchants located around the globe.

The Ripple code is open source and available to the public, meaning that anyone can deploy a Ripple instance. Nodes can take up to three different roles in Ripple: users who make/receive payments, *market makers*, who act as trade enablers in the system, and validating servers which execute Ripple's consensus protocol in order to check and validate all transactions taking place in the system.

Ripple users are referenced by means of pseudonyms and are equipped with a public/private key pair. When a user wishes to send a payment to another user, they cryptographically sign the transfer of money denominated in Ripple's own currency or any other currency. For payments made in non-XRP currencies, Ripple has no way to enforce payments, and only records the amounts owed by one entity to another. More specifically, in this case, Ripple implements a distributed credit network system.

A non-XRP payment from A to B is only possible if B is willing to accept an "I Owe You" (IOU transaction from A, i.e., B trusts A and gives enough credit to A. Hence, A can only make a successful IOU payment to B if the payment value falls within the credit balance allocated by B to A. This may be the case, for example, if the participants know each other, or if the involved amounts are rather marginal. Typically, however, such transactions require the involvement of market makers who act as intermediaries. In this case, enough credit should be available throughout the payment path for a successful payment.

2.4 Independent sources of randomness and time

Bitcoin's blockchain (and altcoin blockchains can be used to instantiate a time-dependent randomness generator. In a nutshell, this generator produces values that are unpredictable but publicly re-constructible.

Several contributions [2,3] already suggest the instantiation of such a time-dependent generator by leveraging the API functionality provided by Bitcoin. Namely, Bitcoin relies on blocks, a hash-based PoW concept, to ensure the security of transactions. On input at time t, the generator outputs the hash of the latest block that has appeared since time t in the Bitcoin blockchain. Clearly, if t is in the future, the generator will output NULL since the hash of a Bitcoin block that would appear in the future cannot be predicted. On the other hand, it is straightforward to fetch the hash of previous Bitcoin blocks whenever t refers to a time in the past. In this way, Bitcoin enables an untrusted party to sample randomness – without being able to predict the outcome ahead of time. Notice that the security of this generator depends on the underlying security of the blockchain. More specifically, if an entity is able to predict the outcome, then they are able to predict a future block hash in the blockchain. Recent studies show that a public randomness beacon – outputting 64 bits of min-entropy every 10 minutes – can be built on top of Bitcoin [4].

2.5 Other blockchain applications

As interest in the technology has increased, blockchain applications have extended beyond Bitcoin and financial systems as well as storage, smart contracts and sources of randomness and time. This section contains information about the most prominent applications and also provides examples of startup companies addressing additional technology-related spaces.

2.5.1 Digital assets

The first prominent application of blockchain included the creation of electronic currencies like Bitcoin or Litecoin. Other digital assets, such as stock and bonds or frequent flyer miles, can be created by adding protocols to crypto-currency implementations. Potentially, digital assets based on blockchain can be created separately from crypto-currencies currently in use.

Digital proxies of real assets represent a parallel application. Several startups focus on scenarios in various contexts; for instance, blockchain-enabled file transfer that could be used as proof of ownership and authenticity over time.

Similarly, blockchain could be used to enforce copyright and support the distribution of copyrighted materials, such as music or movies. Distribution systems can be created where fractional use is supported much better than in traditional systems; for example, the ability to buy one frame or a few bars of music that captured a user's imagination.

2.5.2 **Identity and social networks**

Digital identities can be treated as digital assets and can be created based on blockchain approaches. Social networks based on these identities and other group activities could be put together based on the same framework. Recently, concepts such as Virtual Collective Consciousness (VCC) [5] were proposed to link blockchain technology to the perception of the collective evolution of knowledge as presentedby online group activities. Other efforts focus on identity management, creating approaches to tamper-proof identity practices.

2.5.3 Decentralized File Storage

Blockchain approaches are used to store files in a peer–to–peer rather than centralized fashion (e.g., based on IPFS (InterPlanetary File System).

The blockchain allows different entities, such as banks, governments and industrial players, to efficiently and securely reach consensus on the order of transactions and the correctness of data.

One of the envisioned exploitations of the blockchain lies in the construction of decentralized and authenticated storage systems. The beauty behind this approach is that all data stored in the blockchain is expected to be replicated across a large number of nodes which ensures a high level of reliability.

Authenticated storage refers to a storage system where each entity can prove to another that it had stored a given object. Typical examples are court documents which need to be attested (e.g., that they are issued by a given entity or modifications/updates to legal documents).

Blockchain users are typically equipped with non-repudiable public/private key pairs. Since each transaction confirmed in the blockchain is authenticated, users can prove their ownership of any storage object committed by their transactions.

Similarly, blockchain can also be used to prove data ownership without revealing the actual data. For instance, one can publicly reveal a file digest (e.g., a hash for an object that has been committed in the blockchain and, if conflict arises, the person can prove that they have the data that matches the hash).

This is especially useful for contracts, copyrighted material, patents, etc. For example, one can prove that a specific software revision was developed at any given point in time by time-stamping the hash of the revision tree. BTProof and Proof of Existence already offer such services by leveraging Bitcoin's blockchain.

2.5.4 Smart contracts

Developers can leverage multi-signature transactions in Bitcoin in order to construct smart contracts which refer to binding contracts between two or more parties and are enforced in a decentralized manner by the blockchain without the need for a centralized enforcer.

Multi-signature transactions require $m>1$ correct signatures to be considered valid transactions. Although the primary use of multi-signature transactions is mainly targeted at developing resistance to coin theft, these transactions also support the construction of smart contracts in Bitcoin.

Recent blockchain technologies, such as Ethereum, better support the concept of smart contracts when compared to Bitcoin. For example, Ethereum is a decentralized platform that runs decentralized applications programmed to be executed amongst untrusted parties, without any possibility of downtime, censorship, fraud or third party interference. One can easily craft smart contracts by leveraging such functionality from the Ethereum platform.

2.5.5 Support for an environment that doesn't allow fraud

Bitcoin is frequently associated with cybercrime and financial crime. But the technologies that enabled Bitcoin can also enable anti-fraud activities, and they are already used by governments. The potential of blockchain is acknowledged when assisting governments in reducing criminal phenomena. On the Isle of Man, blockchain is used to register digital currency firms and fight money laundering. In Honduras, blockchain is utilized to eliminate land title fraud. In Estonia, blockchain systems vouch for the authenticity of documents via a notarization system.

3
Economic aspects of crypto-currencies

3.1 Definition of crypto-currency

Digital information that represents a monetary value expresses that value in a specific currency. Traditionally, such as in banking data systems, the currency was encoded as one of the units defined in the ISO 4217 standard. This standard defines textual and numeric codes for all national currencies and for some currencies used only for noble metals (e.g., gold) and international accounting, such as the special drawing rights created by the World Bank.

As this last class of standardised currencies indicates, in the digital domain, in addition to recording tangible currencies, virtual values can be processed as well. In the present economy, even the amount of value in tangible currencies, when processed digitally, vastly exceeds, by several orders of magnitude, the value of physical bank notes and coins in circulation in these currencies. Effectively, all currencies in the world have become virtual.

The term *crypto-currency* has come to describe virtual currencies that have no prescribed relation to existing currencies or existing financial institutions. A crypto-currency does express monetary value, not least as rates of exchange exist between them and traditional currencies. A payment in a crypto-currency can only be made in a digital protocol that uses cryptography to ensure security for both payer and payee. Traditional currencies use cryptography only for some of the transfers of value, for instance in the Swift inter-bank transfers or in consumer payments with cards when realised by, for example, ApplePay.

A narrower definition of crypto-currency could apply when it refers to electronic cash made out of cryptographically-constructed data structures that mimic physical coins. An early example of this narrowly–defined crypto-currency is MicroMint, designed by Rivest and Shamir.

The emergence of Bitcoin has focused the use of the term crypto-currency on its more general meaning.

3.2 Example of Bitcoin and Ripple and different models for creating crypto-currencies

For any virtual currency, one that is not defined in ISO 4217, there are several ways to create an amount of value in that currency available for its users in payments. First, all value can be created in advance of any use. This approach can be used in an electronic payment system that uses accounts. The data representing the created value is stored as belonging to a specific account, a way of creating value used in the Ripple system.

A second way is to create value continuously in small amounts over a longer period, either at regular intervals or associated with events. An account-based payment system can use this period value creation system. The created value can be assigned to a dedicated account as in the first approach or to accounts of specific users. This approach of creating monetary value periodically is taken by Bitcoin, using the created value as the reward for consolidating the account database. However, in Bitcoin there is additionally a limit to the total amount of value to be created.

A third way is to create value on demand by a user. This mechanism is suitable for an electronic cash system where a virtual currency is loaded into a user purse representing an amount in another currency that has been paid by the user for conversion into electronic cash.

3.3. Economic modeling of distributed and peer-to-peer systems

When peer-to-peer systems were the subject of economic study in the late 1990s and early 2000s, specific economic characteristics of such systems were noted (e.g., Chuang (2004) [6]). These studies highlighted characteristics of peer-to-peer systems relevant for economic analysis, such as the absence of a dedicated infrastructure or service provider, absence of monitoring and the prevalence of ad hoc communities. Disincentives for such systems were identified but, more importantly, incentives to build economically-efficient peer-to-peer systems were addressed. Incentives used in these study models included tokens (economic benefits), reputation, taxation (sometimes in the form of barter), contracts and the positive effects of reciprocity.

Other researchers (e.g., Oberholzer-Gee, Strumpf [7] and Gopal, Bhattacharjee, Lertwachara, Marsden [8] addressed the economics of specific peer to-peer systems in conjunction with their effect on legitimate business models, such as music distribution. We expect that a similar area of research will appear in tandem with the economics of blockchain-based crypto-currencies.

Researchers agree that Bitcoin systems possess a level of stability that has not been explained theoretically in terms of infrastructure and economics. Monetary systems have been modeled since the 18th century, and the roles and advantages of monetary systems in comparison to exchange markets was explained by Jevons in 1875 [9]. But it is not clear that approaches in classical economics apply to modern crypto-currencies. Kroll, Devey, and Felten (2015) [10] focused on approaches to modeling of the decentralized markets represented by Bitcoin. The focus of their paper is on the economics of the mining process and the design of incentives that support rational mining behaviours. The authors contend that the field of crypto-currencies lacks thorough analysis of the economic soundness of the protocols in use.

3.4 History of electronic and crypto-currencies (before Bitcoin)

The first crypto-currency, in the widest sense of its definition, was first presented by David Chaum in 1983 [11] when he described a way to ensure privacy in cryptographic protection for payments followed by two further publications (1985 [12], 1988 [13]) and then together with Amos Fiat and Moni Noar (1990) [14]. These last three publications focus on cryptographically-mimicking physical cash.

In 1990 David Chaum started a company, DigiCash, to implement an electronic cash system with smart cards as an electronic purse to store spendable electronic value. While based on the ideas developed in the 1990 paper, the implementation required many novel solutions. This electronic cash system could do a payment in less than half a second while maintaining payer privacy. As there are no publications on the first system implemented at DigiCash, many of its details are not publicly known.

During the 1990s many different approaches to electronic cash were published [15]. In the 2000s research into electronic cash continued albeit at a slower pace. The idea that such cryptographically-engineered cash payments could be seen as involving the creation of a different, virtual currency was not present in any of these publications.

4
Regulatory and legal considerations

4.1 Politics and crypto-currencies: control over currencies by national authorities

One of the features that contributes to the hype around Bitcoin and crypto-currencies is their independence from national governments and financial authorities. In fact, in a Bitcoin-decentralized system, network nodes verify the transactions on the blockchain without the need to involve any third party organization or intermediary. In this way, central banks lose their controlling role over the money supply.

What seems evident from our analysis is that blockchain has defined a new mode of governance, while building consensus and coming to agreements among parties without intermediaries. However, creating consensus among peers in a Bitcoin environment would be easier if users could rely on designated authorities to receive, order and sign transactions. Laurie was the first to propose this model [16], which has been deployed by Ripple and a few other crypto-currencies.

Recently, to address some of the limitations crypto-currencies suffer from, for example, computational costs and scalability, Danezis and Meiklejohn introduced RSCoin, a centrally-banked virtual currency [17]. In this new framework, a central bank delegates other institutions – *mintettes* – to validate transactions. The radical change from traditional miners to mintettes is that the latter are known and can be held accountable for any misbehaviours.

Improving accountability in crypto-currencies represents a key factor for public acceptance and broader deployment in the future. More generally, with reference to blockchain applications, reliability, verifiability and traceability of information recorded on blocks also improve transparency and accountability of the organizations using them. In the case of e-government services based on blockchain, we can expect citizens to have higher trust in public administrations.

4.2 Criminal aspects

A factor, which may impinge on virtual currency deployments and, by extension, on blockchain technology development, is the perception of crypto-currencies as tools for money laundering, tax fraud, tax evasion, terrorist financing and other criminal activities.

The risk of typical criminal activities such as fraud in a crypto-currency environment, as explained in 2.5.5, is lower than in the real-world; nevertheless thousands of episodes of mining and wallet scams have taken place since 2011 [18].

Leveraging the anonymity guaranteed to users by crypto-currency frameworks, criminal groups can exploit these possibilities to launder the proceeds of crime using online crypto-currency trading sites where they can cash-in or cash-out high volumes of money [19]. Although several international organisations and agencies such as Europol, the European Banking Authority (EBA), the FBI and the Financial Action Task Force (FATF) have raised concerns about Bitcoin over the last few years, UK authorities found that banks remain the most common vehicle for money laundering while Bitcoin represents the lowest risk [20].

The popularity of Bitcoin among criminal groups has grown in recent years, especially as a preferred method for online purchases of illicit commodities, drugs, firearms and child pornography. Bitcoins have been widely used for transactions on the Dark Web and in the Silk Road marketplace.

However, the space for anonymity and impunity seems to be shrinking as law enforcement authorities can track transactions made with Bitcoins and crypto-currencies, using analytical tools or blockchain explorers in order to arrest criminal suspects [21].

4.3 Considerations regarding a regulatory framework to ensure broad and legal use of crypto-currencies

One of the risks following from the current lack of a comprehensive regulatory approach toward crypto-currencies is that countries may adopt highly divergent national approaches. An example of this is the way in which different EU Member States have proposed handling the tax treatment of crypto-currency transactions. Some Member States have indicated that they do not wish to consider crypto-currency exchange services under VAT regulation. Examples include the Netherlands [22], Belgium [23], Finland [24], Denmark [25] and Spain [26]. Not all Member States agree with this view. Estonia, for instance, holds that crypto-currency exchange transactions are subject to VAT [27] as does France [28]. Luckily, this matter became the subject of a case before the European Court of Justice at the request of the Swedish Tax Authority [29]. In this case, the Court was asked whether:

> "the exchange of virtual currency for traditional currency and vice versa [...] constitute the supply of a service effected for consideration, [and, if so, whether these] exchange transactions are tax exempt".

Here, the Court decided that an exchange service, exchanging crypto-currencies for legal tender and the other way around, can be exempted from VAT [30]. This judgement will impose an important level of harmonization in the treatment of crypto-currencies, at least from the perspective of taxation. This will also provide Member States with a starting point from which EU-level regulation of this matter can be discussed.

4.4 Regulations on crypto-currencies around the world

At this early stage, there is significant diversity in the basic approach to crypto-currencies:

- Some countries have banned crypto-currencies. They include Bangladesh, Bolivia, Ecuador, Kyrgyzstan, and a few other nations.
- Most developed countries don't regulate Bitcoin for various reasons (or state no reason for the lack of regulatory control). Most developing countries, like Brazil or Chile, don't have regulations with regard to crypto-currencies. In other countries, such as Argentina, crypto-currencies are not banned, but also are not considered legal currencies.
    - By contrast, some countries, such as Germany, recognize Bitcoins as units of account for the purposes of trading and taxation.
    - Other countries, such as Israel, allow the use of Bitcoin as legal tender if it is recognized within a professional group. For example, attorneys in Israel can be paid in Bitcoins following the decision of the Israeli Bar Association.
- In China, private ownership of Bitcoin is allowed, but financial companies cannot use them as legal tender (at least officially).
- In most countries where regulations exist, crypto-currencies are regulated under money laundering and cybercrime provisions. Countries using this approach include Canada, Hong Kong, Switzerland, France and some others.

To conclude, the regulatory status of crypto-currencies is nuanced and doesn't offer a consistent picture that will allow an observer to anticipate vital trends. The general assumption is that crypto-currencies will eventually be regulated, on par with regular currencies.

4.5 China

While China doesn't allow Chinese corporations to hold crypto-currencies, individuals are allowed to. The Chinese government is actively looking at integrating blockchain technologies into the most common processes. One of the latest announcements highlighted the intent to use blockchain for social security payments. Jack Ma is using the technology to monitor the integrity of transactions in Chinese charities. Chinese government and near-government organizations are working with Western technology companies on blockchain prototype. For example, IBM is engaged in one such project with UnionPay.

On the regulatory front, a recently proposed regulation recognizes Bitcoin as a human right in a unique twist in the regulatory efforts in this space. Although limitations on the use of crypto-currencies by companies are well documented, Bitcoin is unofficially allowed, leading to a number of initiatives in this area. On a less optimistic note, the Chinese government is studying the effects of the use of Bitcoin on the success of the proposed anti-terrorism law, making the future somewhat less certain.

4.6 United States

In early 2013, the US Financial Crimes Enforcement Network (FinCEN, a bureau of the United States Department of the Treasury), published a guidance document in which it considers a virtual currency as a medium of exchange that can operate like a tangible currency, but that does not possess the attributes of an official currency, such as being legal tender [31]. Despite a virtual currency not being accepted, FinCEN does consider virtual currency exchangers (those that exchange virtual currency for real currency, funds, or other virtual currency and administrators (those that issue or redeem virtual currency as money services businesses (MSB when they either accept and transmit convertible virtual currencies, or buy or sell convertible virtual currencies for any reason [31A]. FinCEN has also been active in enforcing this matter, for instance in the action against Ripple, a payment system and currency exchange supporting various legal tender currencies, virtual currencies, as well as its own native currency. The Ripple system is operated by Ripple Labs, which wholly owns a subsidiary – XRPII – which was fined 700.000 USD [32]. At state level, legislative action has also been taken or is underway. The State of New York is the first state to have adopted a regulatory framework on virtual currencies [33]. The State of California passed an act to repeal a section of its Corporations Code that limited corporations to putting into circulation only "the lawful money of the United States" [34]. The State of Texas, on the other hand, does not consider virtual currency exchange or transmission as valid under the Texas Financial Code [35]. Due to its broad use of the term payment instrument, the State of Florida also requires virtual currency services to register as money service businesses [36]. A proposed amendment to the North Carolina Money Transmitters Act would introduce regulation on the sale and receipt for the transmission of virtual currencies and maintaining control over virtual currencies on behalf of others [37]. The State of Connecticut enacted rules requiring money transmitters seeking a licence to conduct their business to state whether that business would include the transmission of monetary value in the form of virtual currency [38].

4.7 EU issues

At the level of the European Union, there are three specific legal frameworks that are relevant to crypto-currencies [39]. Firstly, there is the legal framework regarding payment services, set by the Payment Services Directive (PSD, 2007/64/EC), which is currently undergoing revision (PSD2, 2015/2366/EU) [40]. Secondly, there is the legal framework on e-money, currently set by the second E-Money Directive (2EMD, 2009/110/EC) [41]. Lastly, there is the legal framework on anti-money laundering, set by the fourth Anti-Money Laundering Directive (AMLD4, 2015/849/EU) [42]. However, when examining these legal frameworks closely, their application to crypto-currencies appears all but certain [43].

The main scope of PSD2 concerns payment service providers [40A]. The formulation of such payment services [40B] does not leave much room for the inclusion of crypto-currency services. Principally, payment services revolve around the notion of *funds*, which are defined as *banknotes and coins, scriptural money and electronic money as defined in Article 1(3)(b) of Directive 2000/46/EC* [40C]. Here, it can indeed be held that privately-issued currencies also fall under the scope of this definition [44], regardless of their denomination. However, where such currencies are not denominated in euros or other Member State currencies – as is the case for crypto-currencies – titles III and IV of the directive do not apply [40D]. Moreover, the broad scope exceptions make the application of PSD to crypto-currencies implausible at best. While a broad interpretation of the notion of funds could therefore slightly open the door for crypto-currencies, the scope exceptions almost certainly rule out the application of the directive to this technological development. The new PSD2 maintains largely the same definitions. Though the exemptions have been substantially rewritten, the revision appears not to result in a different treatment of crypto-currencies. While originally PSD and 2EMD should have been subjected to a review at the same time, the European Commission decided to postpone the review of 2EMD. This effectively rules out a merger between both legal frameworks, which had been anticipated given the strong reliance of 2EMD on PSD.

2EMD uses a very narrow definition of e-money, which thus limits its scope of application significantly. More precisely, e-money is defined as

> *"'electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions [...] and which is accepted by a natural or legal person other than the electronic money issuer" [41A].*

Also, e-money must be redeemable at par value, meaning that a link is preserved between the value of e-money and physical money [45]. From the requirement that e-money is to be issued on receipt of funds, it follows that an e-money issuer cannot decide to create new e-money units at will [46]. This means that e-money under 2EMD must inherently be considered as a prepaid good. It is this element that poses difficulties regarding crypto-currencies, which are by nature issued following the algorithm underlying the crypto-currency and are thus not subjected to the will of a central issuer. Such would therefore exempt crypto-currencies from the scope of application of 2EMD [47]. Moreover, the scope exceptions of PSD discussed before also apply to 2EMD. The result of this would be that, even if crypto-currencies could be argued to be e-money, *quod non*, the broad range of scope exceptions could still allow crypto-currency service providers to escape the scope of application of this legal framework.

AMLD4 does not mention crypto-currencies, or virtual currencies at all. Also the opinions issued by the European Central Bank, the European Economic and Social Committee and the European Data Protection Supervisor on the proposal to this directive do not make any reference to this issue [48]. Only in the Committee report tabled before the European Parliament's first plenary reading has an amendment been inserted referring to anonymous e-money products [49]. This amendment can, however, not be understood as covering crypto-currencies, since these forms of virtual currencies are note-money under the EU's definition. In the meantime, the EBA adopted an opinion on virtual currencies [50] in which a strong call was made to bring virtual currencies – including crypto-currencies – under an existing legal framework. The European Commission reacted positively to this call for action, hinting that the possibility to include virtual currencies under the proposed AMLD4 would be discussed at the trialogues [51]. In those discussions, held in February 2015, France (in response to the January 2015 attack on the magazine *Charlie Hebdo*) made a statement in support of strengthening the legal framework against terrorist financing in which the need to assess the risks posed by virtual currencies is mentioned [52]. However, the Council's position adopted in April 2015 makes no explicit mention of virtual currencies and only includes the European Parliament's amendment on anonymous e-money instruments [53]. In the final text, recital 19 refers to new technologies, holding that: *The competent authorities and obliged entities should be proactive in combating new and innovative ways of money laundering.*

This, however, does not necessarily exclude crypto-currencies from AMLD4's scope altogether. The UK, for instance, has already proposed steps to include virtual currency service providers – especially exchange services – under its national AML and CFT (Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act) frameworks [54]. Moreover, it has been suggested that virtual currency service providers could fall under the scope of AMLD4's obliged entities [55]. The precise degree with which crypto-currencies can be included under AMLD4's scope given the lack of a direct formulation in this regard can therefore be expected to become the subject of further discussion during the directive's implementation stage [56]. However, on 2 February 2016, the European Commission announced its Action Plan to strengthen the fight against terrorist financing [57]. Under this plan, it is proposed to extend *the scope of the AMLD to include virtual currency exchange platforms, and have them supervised under Anti-Money Laundering / countering terrorist financing legislation at national level* [58].

The European Parliament recently adopted a resolution on virtual currencies [59] exploring the opportunities and risks of virtual currencies and distributed ledger technologies, the advantages of their uses beyond payments as well as the relevance of more tailor-made legislation. In particular, the Parliament called for the creation of a horizontal task force on distributed ledger technology led by the European Commission and composed of technical and regulatory experts who would be asked to analyse the benefits and shortcomings of a broader deployment of some blockchain applications.

5 Privacy

5.1 Public ledgers and privacy versus anonymity and privacy

In centralized payment systems, user privacy is often measured with respect to the honest-but-curious centralized entity (e.g., Bank of Mint) that maintains the accounts of individuals. In these systems, privacy typically means guaranteeing payer/payee anonymity with respect to the bank. However, existing privacy-preserving solutions in this area indirectly assume that, although the bank can have a complete view of daily or monthly withdrawals and deposits of individuals, it is not aware of all transactions that take place within the system.

In an open payment system, such as Bitcoin, this model is clearly not applicable. In particular, the centralized entity is substituted by the distributed time-stamping server which is governed by *the majority of the available computation power*, and has the ability to confirm or reject transactions. This distributed mechanism requires that participants check the validity of all transactions that occur in the system. Therefore, the privacy adversary in this case should be adjusted to account for the public view of all payments, although it may not be able to link payments to individuals. For instance, in Bitcoin a user is only aware of the pseudonym (the address) of the person they send a payment to or receive a payment from, but do not know other addresses that pertain to that person.

Recent studies show the limits of privacy within such open ledgers. Namely, several heuristics can be applied to cluster different accounts belonging to a pseudonymous entity, thereby allowing an adversary to estimate the balance of Bitcoin users [60,61]. Moreover, several studies suggest that the transactional amounts and times of making transactions can reveal considerable information about the profile of users [60,62]. This information can be used to link different Bitcoin addresses pertaining to Bitcoin users in order to implement accountability measures within the system (e.g., *blacklist*-linked addresses from the network) with blockchain users.

5.2 Encryption, government mandates and privacy

Practices like anonymisation, decentralisation and data minimisation are common to crypto-currencies and help reduce the risk of compromising transactions: the identity of a payer is not essential to conclude a payment (see 5.3). The anonymity ensured for transactions with crypto-currencies has drawn the attention of law enforcement agencies to this technology and led to the criticism that crypto-currencies are tools for money laundering and financing terrorism (as already pointed out in 4.2).

The debate as to whether technology could neutralize the investigative capabilities of law enforcement authorities date back to the 1990s. Since then, police and government agencies have claimed to suffer from *going dark* [63]. Access to information by law enforcement agencies plays a central role in the current policy debate around digital security: citizens have the legitimate expectation to see both national security and civil liberties protected at the same time. The United States, for instance, set up a dedicated multi-disciplinary commission to provide recommendations on technological and political solutions that would provide the best way forward for security and privacy [64].

It is widely acknowledged today that government mandates to create back doors or weaken technology for law enforcement purposes would not be effective in fighting organized crime and terrorism, but would instead make society, infrastructures and citizens *more* vulnerable [65].

It would also be the case for blockchain technology too. Mandatory design requirements for law enforcement purposes would finally undermine trust around the technology: users would no longer be able to rely on the non-modifiable, non-repudiable, permanent and irreversible nature of single blocks. Developers would be discouraged or simply not able to fully unleash the potential of the technology, missing multiple applications and therefore opportunities for economic and societal benefit.

In contrast, a broader deployment of blockchain technology driven by innovative solutions could spur privacy and security across public and private sectors. The application of blockchain to identity management is a good example of mitigating privacy risks: it could be widely deployed in very different organisations, from public administrations to banks, to transform real-world identities into data sealed with public/private keys and sent to a ledger.

5.3 Anonymity in payment systems

In a payment two principal parties are involved: a payer, who owns monetary value, and a payee who is the receiver of some monetary value previously owned by the payer. If a payment is made in conventional cash, that is, coins or banknotes, the payee does not obtain any information about the identity of the payer. Depending on the context of the payment such information may be available anyway. For instance, when settling an outstanding bill, the payer is most likely the person mentioned on the bill. In this example the actual payer can be someone else, though very likely someone who knows the creditor. With payment in traditional cash, the payer is in principle anonymous.

From an information point of view, the identity of the payee in a traditional cash payment is notrelevant, the payment is a one-way protocol with information (i.e., money being transferred from payer to payee. In most practical payment contexts, the payer has previous knowledge of the payee as the supplier of a good or service being paid. In many circumstances a payee is expected, or legally required, to provide a receipt stating the amount and the name of the payee. Protecting the privacy of the payee, at least from the payer, is not a general requirement for payment.

Electronic payment exists in two distinct models, either with electronic cash or with a transfer of value from a payer account into a payee account. An electronic cash payment is off-line; the payment is effected by the exchange of multiple messages in a dedicated protocol between a device owned by the payer and a device owned by the payee. A few protocols for electronic cash payments exist that strongly protect payer privacy. On the other hand, a value transfer between accounts takes place on-line with messages between the keeper of the accounts and both the payer and the payee. In order to protect the payer's funds, the keeper of the account uses an authentication protocol to initiate the payment. Consequently identity information about the payer and the intended payee are transferred to the account keeper at the start of the payment. All currently existing protocols share payer identification with the payee. In a system like Bitcoin the payer information is pseudonymous; with the register of payments publicly accessible, the pseudonymous information is traceable, with a high chance of full payer identification. In an alternative protocol, like ApplePay, payer information is anonymised during communication, yet fully available to the record keeper.

6
Risk management models and approaches

As with other multi-disciplinary fields, an understanding of risks is essential in order to adapt to complex environments, although creating adequate risk models is challenging.

6.1 Integrated risk models

Different types of risks have been defined and considered for the analysis of operations in industry and government. Traditionally, risk models for security include three dimensions: people, processes and technology. The increasing complexity of the technology environment rendered these models insufficient. In order to compensate for these shortcomings, additional dimensions, such as organizational strategy and structural design [66], were added.

Risk-management approaches for more complex fields began to integrate additional risk domains, such as assurance and resilience [67], and risk assessment was integrated into the system development cycle. This risk aware development was first adopted in very structured environments, such as military technology and aerospace system development, and cybersecurity was added to already rigorous risk-assessment models. It will be challenging to apply this approach to the risk analysis of peer-to-peer systems.

Although people have formed an evaluation area in the early risk analyses of organizational security, this aspect of risk has been significantly extended in recent approaches. In addition to sophisticated models of threat agents (e.g., as described in a model developed by Intel Corporation [68]), and their common use in mitigation processes, the examination of insider threats became more detailed. Views on the role of human error have matured, and organizational behaviours have been studied in more detail.

In today's complex multi-domain systems, the risk analysis from different domains needs to be integrated. An example of an integrated risk framework combining risk domains of security, privacy, safety, reliability and resilience can be found in the draft deliverable of NIST's Cyber-Physical Systems Public Working Group [69].

Risk domains are different for a generic model embracing blockchain applications. These domains are likely to include security, privacy, economic and regulatory risks, as well as human behaviour risks. A separate assessment of these domains is insufficient to address potential risks because requirements optimized for one domain can be detrimental to the composite risk picture for the overall system.

6.2 Risk composition

For complex environments, only an integrated system of composed risks could present an accurate picture of the environment that can define an adequate risk posture. However, several obstacles will need to be overcome in order to create a solid foundation for future work. One of these early challenges is a semantic framework that is necessary to enable a consistent terminology and ability to reason about the environment based on a shared view. A multi-domain ontology is needed to accommodate this requirement. Today, even the most elementary terms, such as *incident*, have different definitions within different risk communities. In the area of safety, *incident* denotes an event that doesn't have safety-critical consequences, whereas for the security community, an *incident* is a serious breach. Semantic disconnect is even larger between more diverse risk domains, such as privacy and economic.

Another obstacle is a consistent approach to metrics that could lead to objective measurements of risk, a serious problem when an integrated risk model is considered. For example, probabilities in the risk domain of safety are extremely small, with tiny probabilities of failure. On the other hand, the probabilities of a breach in security and privacy, where diverse and evolving attacks need to be taken into consideration, are much larger. The challenge is even greater in situations where a probability cannot be reliably computed. For example, EU data protection legislation requires the anonymisation of personal data, but applies a *reasonableness* test to determine whether or not the data is anonymous. While reasonableness may be an adequate legal test, it is very difficult to translate it into probability of re-identification. Thus, an integrated view on risk metrics is necessary to ensure success in building a risk model for blockchain systems.

If consistent semantics and metrics could be achieved, risk composition, the ability to measure integrated risks that compose, in a meaningful way, risk parameters in multiple domains, would be within reach. But the risk community is very far from this point.

7
Notable projects and initiatives

The unexpected success of Bitcoin brought additional attention to both the potential of crypto-currencies and the opportunities to use the approaches that have been instrumental in the deployment of Bitcoin in other areas. As a result, in addition to academic efforts, some practical initiatives have started to emerge. This section is dedicated to some of these initiative. A list of these initiatives is provided below.

7.1 e-Government

- Estonia (notarization system)
- Honduras (Land titles verification)
- Isle of Man (Identification of digital currencies providers)
- Oman (Healthcare)

7.2 Open Source

- Linux Foundation's Hyper Ledger

7.3 Standardization

- R3
- A new Committee focusing on blockchain has been created in ISO. The TC (TC370) will be headed by the Australian National Body. The official name is "TC (ISO/TC 307) on Blockchain and electronic distributed ledger technologies." Other standards are emerging. The most notable may be Chain Open Standard (https://chain.com/os/) that grew out of an R&D project.

7.4 Startups

- Coinometrics (behaviour analysis)
- Guardtime (various: from notary to network management to document endorsement)
- Helloblock (development environment for Bitcoin)
- Kraken (digital asset trading platform)
- BTCJam (lending platform)
- Blockcypher (blockchain as a service)
- DigitalTangibleTrust (investment portfolios for digital/digitizable assets)
- BiFuBao (proof of reserves platform)
- BitPay (payment gateway)
- Abra (payment platform)
- BitPagos (Bitcoin savings platform)
- OneName (digital identity)
- Keybase (digital identity)
- Tierion (verification)
- Proof of Existence (verification)
- Factom (verification)
- Etherium (smart contracts)
- Rootstock (smart contracts)
- Storj (file storage)

8
Outlook and Future Work

8.1
Introduction

The TDL workshop held in June 2016 in The Hague identified some technological and policy priorities which, in the light of the large scale adoption of blockchain, we deem critical for its development and deployment and provide a template for future TDL collaborative work in this area.

8.2
Technical Priorities

Despite the industry attention that blockchain has received in recent years, it is still effectively a new technology albeit one with considerable promise that is as yet unfulfilled and relatively unproven. From a technical point of view, the most important issues are performance and scalability, including throughput capacity, storage limits and ever increasing power consumption. Of similar importance is ensuring that the orchestration of blockchains and integration with legacy systems are efficient and well-managed: it is unlikely that companies will consider incorporating or even switching to blockchain-based applications if there is any likelihood of disruption to established processes. Finally, there is no reason at this stage to question whether the basic building blocks of distributed ledgers - the replication of data across a wide geographical-distributed network without loss of integrity - do not work as intended. However, it is remains vital that these capabilities are extensively demonstrated and stress-tested.

8.3 Policy Priorities

The long term and widespread uptake and application of blockchain technology will depend on effective governance and 'only-as-required' regulation that protect the interests of both consumers and providers of distributed ledger-based services. We believe that blockchain can address some of the current and future societal concerns, especially with regard to privacy and security. These aspects need to be fully understood by policymakers to allow a broad deployment of the technology.

- Security
  Being decentralised, blockchain is inherently resilient and robust, particularly with non-permissioned ledgers, and its consensus-based approach to governance obviates a central point of failure. Blockchain provides confidentiality, authenticity and non-repudiation to all transactions and activities. As our lives are increasingly spent online and our societies rely more and more on digital tools and platform, the adoption of blockchain-based services would minimize security risks and threats. However, one of the inherent weaknesses of any system is at the points of human interaction which are susceptible to compromise and require a secure mechanism for users to access blockchain applications.

- Privacy
  In the modern ICT environment, fast technology developments challenge effective protection of individuals' data. On the one hand, blockchain offers a certain degree of pseudonimity with no need to share identities for trusted transactions nor to store personal data on the blockchain. On the other hand, public blockchains record permanently and disclose publicly every transaction: these features put privacy potentially at odds, especially when it comes to individuals' data protection rights such as right to be forgotten, data portability or rectification, recently enhanced by EU regulations

- Standardization
  With the proliferation of blockchain initiatives within and across industry sectors as well as the emergence of other distributed ledger systems, a clear set of standards to ensure interoperability and applicable levels of interworking within blockchain as well as legacy applications is paramount.

8.4 Conclusion

While we acknowledge the innovative and transformational power of blockchain, the promise of this technology still needs to be kept. Industry bodies and governments are looking at effective and deployable applications of blockchain in numerous fields. TDL will continue to monitor all aspects of the evolution of blockchain and carry out research work on both technological and policy topics. In particular we would like to analyse the most viable applications for large scale adoption of blockchain and to discuss the possibility of blockchain becoming a tool for addressing privacy and security policy concerns.

Bibliographic References

[1] From Wikipedia, Blockchain (database)

[2] Armknecht, F., Bohli, J-M., Karame, G., Youssef, F., "Transparent data deduplication in the Cloud", *Proceedings of the ACM Conference on Computer and Communications Security*, 2015

[3] Armknecht, F., Bohli, J-M., Karame, G., Liu, Z., Reuter, C., "Outsourced proofs of retrievability", *Proceedings of the ACM Conference on Computer and Communications Security*, 2014

[4] Bonneau, J., Clark, J., Goldfeder, S., "Bitcoin as a public randomness source", *Cryptology ePrint Archive: Report 2015*/1015

[5] Bailey, J., Oullier, O. and Marzouki, Y.,, Can the Bitcoin protocol morph Virtual Collective Consciousness, July 3, 2014

[6] Chuang, J., (2004) "Economics of Peer-to-Peer Systems", Academia Sinica 2004 Summer Institute on P2P Computing

[7] Oberholzer-Gee, F., Strumpf, K., "The Effect of File Sharing on Record Sales: An Empirical Analysis", *Journal of Political Economy*, 2007, vol. 115, no. 1

[8] Gopal, R.D., Bhattacharjee, S., Sanders, G.L., (2006) "Do Artists Benefit from Online Music Sharing?" *The Journal of Business*, 79(3), 1503-1533

[9] Jevons, W.S., "Money and the Mechanism of Exchange", 1875

[10] Kroll, J., Davey, I., and Felten, E., "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries", The Twelfth Workshop on the Economics of Information Security (WEIS 2013), Washington, DC, June 10-11 2013

[11] Chaum, D., "Blind Signatures for Untraceable Payments", *Advances in Cryptology: Proceedings of CRYPTO '82*, pp. 199—203, 1982

[12] Chaum, D., (1989) "Numbers can be a better form of cash than paper", *Smartcard 2000*, pp. 151-156

[13] Chaum, D., (1985) "Security without identification: Transaction systems to make big brother obsolete", *Communications of the ACM*, volume 28, 10, pp. 1030-1044

[14] Chaum, D., Fiat, A., Naor, M., (1988) "Untraceable electronic cash", *Proceedings on Advances in Cryptology—CRYPTO '88, 8th Annual International Cryptology Conference*, Santa Barbara, California, pp. 319–327

[15] de Jong, E., "Electronic Money: From Cryptography and Smart Cards to Bitcoin and Beyond", Smartcard Workshop, Fraunhofer-Institut für Sichere Informationstechnologie, Darmstadt, 15/16 February 2017

[16] Laurie, B., "An efficient distributed currency", 23 July 2011

[17] Danezis, G., Meiklejohn, S., "Centrally banked cryptocurrencies", University College London, 2016

[18] Vasek, M., and Moore, T., "There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams", 2015

[19] Europol, "Why is cash still king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering", 2015

[20] HM Treasury and Home Office, "UK national risk assessment of money laundering and terrorist financing", October 2015

[21] *Reuters*, Spain arrests 30 suspected of laundering money in bitcoin centers, May 25, 2016;

The Guardian, Ten arrested in Netherlands over bitcoin money-laundering allegations, 20 January 2016

[22] Van Wirdum, A., Dutch Official: Bitcoin transactions probably not liable for VAT, coindesk.com, 25 November 2014

[23] Rizzo, P., "Belgian Tax Body: Bitcoin trades not subject to VAT", coindesk.com, 22 September 2014.

[24] Stanley-Smith, J., "Finland recognizes Bitcoin services as VAT exempt", *International Tax Review*, 14 November 2014.

[25] Sharkey, T., "Denmark declares Bitcoin trades are tax-free", *coindesk.com*, 25 March 2014.

[26] Bello Perez, Y., "Spanish Bitcoin community celebrates Bitcoin's VAT exemption", *coindesk.com*, 23 April 2015.

[27] Hajdarbegovic, N., "Estonia: VATshould apply to full value of Bitcoin trades", *coindesk.com*, 11 December 2014.

[28] Banque de France, "Les dangers liés au développement des monnaies virtuelles: l'exemple du bitcoin", 5 December 2013

[29] European Court of Justice, Skatteverket v David Hedqvist, 'Reference for a preliminary ruling — Common system of value added tax (VAT) — Directive 2006/112/EC — Articles 2(1)(c) and 135(1)(d) to (f) — Services for consideration — Transactions to exchange the 'bitcoin' virtual currency for traditional currencies — Exemption', Case C-264/14

[30] Judgement of the Court, in the Case C-264/14, §58.

[31] FinCEN (2013) "Guidance Document - Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies", FIN-2013-G001, 1.

[31A] *ibid*, 3. The reasoning used here is that the "definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies".

[32] FinCEN (2015) "FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger", *Press release*, 5 May 2015.

[33] New York State Department of Financial Services, NYDFS grants first charter to a New York virtual currency company, Press release 7 May 2015

New York State Department of Financial Services, NYDFS Announces Final BitLicense Framework for Regulating Digital Currency Firms, Speech by Benjamin M. Lawsky, Superintendent of Financial Services 3 June 2015

Regulation of the Conduct of Virtual Currency Businesses, New York State Register 24 June 2015, nr. DFS-29-14-00015-A, 7-9.

[34] California Assembly Bill 129, (2013-2014), "An act to repeal Section 107 of the Corporations Code, relating to business associations", Chapter 74, June 28 2014

[35] Texas Department of Banking, Supervisory Memorandum 1037, "Regulatory Treatment of Virtual Currencies Under the Texas Money Services Act", 2-3, April 3, 2014. However, it does view the exchange of crypto-currency for sovereign currency through a third party exchange – as is the case for most crypto-currency exchanges – as money transmission.

[36] Ewbank, L.T., Reyes, C.L., Hansen, J.D., "Two Florida users of local bitcoins.com arrested for money laundering and unlicensed money transmission", *Virtual Currency Report*, 11 February 2014.

[37] General Assembly of North Carolina, Session 2015, NC Money Transmitters Act.-AB, "A Bill to be entitled an Act to enact the North Carolina Money Transmitters Act as requested by the Office of the North Carolina Commissioner of Banks", H289, March 18, 2015

[38] State of Connecticut, Substitute House Bill No. 6800, Public Act No. 15-53, "An Act concerning mortgage correspondent lenders, the Small Loan Act, virtual currencies and security freeze on consumer credit reports", June 19, 2015

[39] Other pieces of key legislation referred to in the resolution of the European Parliament include:

- EMIR (European Market Infrastructure Regulation): Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories
- CSDR (Central Securities Depositories Regulation): Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012
- SFD (Settlement Finality Directive): Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems.
- MiFID2 (Markets in Financial Instruments Directive 2): Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU
- MiFIR (Markets in Financial Instruments Regulation): Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012
- UCITS (Undertakings for Collective Investment in Transferable Securities): Directive 2014/91/EU of the European Parliament and of the Council of 23 July 2014 amending Directive 2009/65/EC on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) as regards depositary functions, remuneration policies and sanctions

[40] PSD2 (Payment Services Directive 2): Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

[40A] *ibid*, Article 1 specifies six categories of payment service providers
[40B] As defined in the annex
[40C] *ibid*, Article 4 (15)
[40D] As follows from *ibid*, Article 2 (2)

[41] 2EMD (Second e-Money Directive): Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC

[41A] *ibid*, Article 2 (2)

[42] AMLD4 (Anti-Money Laundering Directive 4): Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

[43] Valcke, P., Vandezande, N., Van de Velde, N., The Evolution of Third Party Payment Providers and Cryptocurrencies Under the EU's Upcoming PSD2 and AMLD4, *SWIFT Institute Working Paper* No. 2015–001

[44] Your questions on PSD, Payment Services Directive 2007/64/EC, Questions and answers, question 164.

[45] European Central Bank, Virtual Currency Schemes, 16, October 2012 For instance, if a user purchases e-money valued at EUR 10, he will later be able to redeem that e-money for EUR 10. In other words, value fluctuations – such as those found in crypto-currencies such as bitcoin – should not affect e-money

[46] Weber, R., Darbellay, A., Legal issues in mobile banking, *Journal of Banking Regulation 11*, 135, 2010

[47] Stokes, R., "Virtual money laundering: the case of Bitcoin and the Linden dollar", *Information & Communications Technology Law 21*, 227–228, 2012

[48] European Central Bank, Opinion of 17 May 2013 'on a proposal for a directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and on a proposal for a regulation on information accompanying transfers of funds', CON/2013/32;

European Economic and Social Committee, Opinion of 23 May 2013 on the 'Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds' COM (2013) 44 final – 2013/0024 (COD); and the 'Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing' COM (2013) 45 final – 2013/0025 COD), ECO/344;

European Data Protection Supervisor, 'Executive summary of the Opinion on a proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and a proposal for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds', OJ C 32 of 4 February 2014, 9–12.

[49] European Parliament, Committee on Economic and Monetary Affairs and Committee on Civil Liberties, Justice and Home Affairs: Report on the proposal for a directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing COM (2013)0045) – C7-0032/2013–2013/0025(COD)), A7-0150/2014, amendment 10.

[50] European Banking Authority, Opinion on 'virtual currencies', EBA/Op/2014/08.

[51] Payment Systems Market Expert Group, Minutes of the meeting of 22 October 2014, Brussels, PSMEG 008/14, 2–3.

[52] Council of the European Union, 'Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (first reading), Adoption (a) of the Council's position (b) of the statement of the Council's reasons' - Statements, 7768/15 ADD 1, 2-3, 2015

[53] Council of the European Union, 'Position of the Council at first reading with a view to the adoption of a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) N 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC', Adopted by the Council on 20 April 2015, 5933/4/15 REV 4.

[54] HM Treasury, Digital currencies: response to the call for information, 2015, 19.

[55] Payments Council, HM Treasury – Digital currencies: call for information – Payments Council and BBA response, 3 December 2014, 3

[56] Payment Systems Market Expert Group (2015) "Minutes of the meeting of 28 April 2015", PSMEG/005/15, 3. While the European Commission did acknowledge that virtual currency exchange platforms were not included in the AMLD4, it does propose to look again into virtual currencies.

[57] "Commission presents Action Plan to strengthen the fight against terrorist financing" – 2 February 2016

[58] European Commission (2016), 'Communication on an Action Plan for strengthening the fight against terrorist financing', COM (2016) 50 final, 5

[59] European Parliament resolution of 26 May 2016 on virtual currencies (2016/2007(INI)).

[60] Androulaki, E., Karame, G, Roeschlin, M., Scherer, T., Capkun, S., "Evaluating user privacy in Bitcoin", *Proceedings of the International Conference on Financial Cryptography and Data Security*, Okinawa, Japan, 2013

[61] Meiklejohn, S., Pomarole, M, Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S., "A fistful of Bitcoins: characterizing payments among men with no names". *Proceedings of the Internet Measurement Conference*, 2013

[62] Gervais, A., Ritzdorf, H., Lucic, M., Capkun, S., "Quantifying location privacy leakage from transaction prices", *Cryptology ePrint Archive: Report* 2015/496

[63] Comey, J.B., Federal Bureau of Investigation Direction in a speech at Brookings Institution, Washington DC on 16 October 2014

[64] The McCaul-Warner Commission on Digital Security

[65] ENISA, On the free use of cryptographic tools for (self) protection of EU citizens, 20 January 2016

[66] Langfield-Smith, K., (2008) "Strategic management accounting: how far have we come in 25 years?", *Accounting, Auditing & Accountability Journal*, Vol. 21 Iss: 2, pp.204 - 228

[67] Katsumata, P., Hemenway, J., Gavins, W., "Cybersecurity risk management", *Military Communications Conference*, 2010-Milcom 2010

[68] Intel Corporation, "Prioritizing information security risks with threat agent risk assessment", Information Technology White Paper, 2009

[69] NIST, CPS PWG Cyber-Physical Systems (CPS) Framework Release 1.0

[70] Swanson, T., "Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems", 6 April 2015

Glossary

2EMD	Second E-Money Directive
AMLD4	Fourth Anti-Money Laundering Directive
BTC	Bitcoin coin
CFT	Countering Financing of Terrorism Act
CSDR	2009 Central Securities Depositories
EBA	Regulation European Banking Authority
EC	European Commission
EMIR	European Market Infrastructure Regulation, 16 August 2012
EU	European Union
FATF	Financial Action Task Force
FinCEN	US Financial Crimes Enforcement Network
HM	Her Majesty (as in UK government office)
IPFS	InterPlanetary File System
ISO	International Organisation for Standardization
MiFID	Markets in Financial Instruments Directive
MiFIR	Markets in Financial Instruments Regulation
NIST	National Institute of Standards and Technology
NYDFS	New York State Department of Financial Services
OJ	Official Journal (of the European Commission)
PoW	Proof of Work
PSD2	Payment Service Directive 2
SFD	Settlement Finality Directive 2009/44/EC
UCITs	Undertakings for Collective Investment in Transferable Securities
VAT	Value Added Tax
XRP	Ripple currency

trustindigitallife.eu

Trust in Digital life Association
Aarlenstraat 22 / Rue d'Arlon 22
1050 Elsene, Brussels
Belgium

office@trustindigitallife.eu
T +44 1738 583 533

TDL | Trust in Digital Life

trustindigitallife.eu

Trust in Digital life Association
Aarlenstraat 22 / Rue d'Arlon 22
1050 Elsene, Brussels
Belgium

office@trustindigitallife.eu
T +44 1738 583 533

TDL | Trust in Digital Life