JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2019, 1–12
doi: 10.1093/cybsec/tyz004
Research paper

Research paper

Cryptocurrencies and fundamental rights

Christian Rueckert*

FAU Erlangen-Nuremberg/Karlsruhe Institute of Technology (KIT), Schillerstraße 1, Erlangen 91054, Germany

*Correspondence address: FAU Erlangen-Nuremberg/Karlsruhe Institute of Technology (KIT), Schillerstraße 1, Erlangen 91054, Germany. Tel: +49 09131 85 22144; E-mail: christian.rueckert@fau.de

Received 14 October 2018; revised 18 February 2019; accepted 25 April 2019

Abstract

Cryptocurrencies,[1] like bitcoin, raise new legal questions due to their innovative technological concepts. While academic research covers nearly all areas of the technological concepts of those currencies, legal studies focus only on a few topics. The papers that have been published so far discuss mainly economic law, tax law, and financial regulations. At the same time, governments are starting to explicitly regulate cryptocurrencies in terms of anti-money-laundering (AML) and to clarify or strengthen the legal basis for prosecuting crimes in the context of cryptocurrencies. Furthermore, criminal investigation in the context of cryptocurrencies is intensifying with the rising number of cryptocurrency-related crimes. Moreover, governments should also start to consider crime prevention in the context of cryptocurrencies. AML regulation, crime prevention, and prosecution have to take heed of the fundamental rights of the citizens affected. To date, legal research has not discussed the relationship between AML regulation (regarding cryptocurrencies), crime prevention (in conjunction with cryptocurrencies), the prosecution of crimes involving cryptocurrencies and fundamental rights. Many future regulatory concepts will collide with the fundamental right to property of the owners of cryptocurrency units and the freedom to pursue a trade or profession of owners and operators of exchange platforms, mining pools, etc. In cryptocurrencies organized as peer-to-peer systems, the freedom of association also has to be mentioned. With particular regard to prosecution, law enforcement agencies restrict the freedom of telecommunication, data privacy (including the right to informational self-determination), freedom of expression, and the freedom of information. Whenever some of these fundamental rights are impinged upon, regulation concepts and investigation or prosecution approaches must be provided for by law and must fulfill the criterion of necessity. Further interdisciplinary research is needed to develop efficient and legit prevention as well as criminal investigation concepts.

Key words fundamental rights; cryptocurrency; Bitcoin; criminal investigations; regulatory approaches; law

Introduction

This article examines the relationship between cryptocurrencies, regulation concepts, investigation methods, and fundamental rights. Despite the increasing importance of the regulation of cryptocurrencies, the papers that have been published so far discuss mainly economic law [1–3], tax law [4–6], and financial regulations [1–4, 6–14]. To date, legal research has not discussed the relationship between anti-money-laundering (AML) regulation (regarding cryptocurrencies), crime prevention (in conjunction with cryptocurrencies), the prosecution of crimes involving cryptocurrencies, and fundamental rights [15–17]. I will focus on the fundamental rights as codified in the Charter of Fundamental Rights of the European

1 In this article, the term "cryptocurrency" only refers to schemes with the following properties: decentralized organization governed by a network protocol, cryptography as means to secure transactions, and a public ledger which documents the system state and history.

Union (CFR) [18] and the European Convention on Human Rights (ECHR) for two reasons: First, investments in and trade with cryptocurrencies have a cross-border dimension. Hence, regulation concepts require an international context and should be discussed in the context of transnational fundamental rights. Second, the CFR and the ECHR not only belong to the few international fundamental rights charters that are legally binding on Member States but also provide the most extensive jurisprudence with regards to their application [see Art. 6 (2) (3) Treaty on European Union (TEU)].[2] Nevertheless, most of the findings can be transferred into other fundamental rights systems. The analysis of other legal systems is surely a worthwhile focus for future research (see "A brief glance at the international situation" section for more details).

Due to the large (and continuously growing) [19] number of so-called "cryptocurrency" systems with different technological characteristics, the term "cryptocurrency" is not easy to define (p. 13 in [20]). The spectrum of classification possibilities is as broad as the technological design space [21] for "cryptocurrencies."[3] In this article, the term "cryptocurrency" only refers to schemes with the following properties: decentralized organization governed by a network protocol, cryptography as means to secure transactions, and a public ledger which documents the system state and history. Bitcoin will serve as reference example for these currencies since it is the most popular cryptocurrency with the widest acceptance and the largest market capitalization to date [18]. The arguments also apply to other cryptocurrencies modeled after Bitcoin (e.g. "alt-coins" such as Litecoin). They may in principle generalize to schemes with different (combinations of) properties, but further research needs to reassess the applicability for each instance.

In terms of regulation, the article will focus on crime prevention concepts, especially AML and prosecution measures in the context of cryptocurrencies.

The section "Bitcoin's specific features in terms of regulation" provides a brief overview of Bitcoin as an example of decentralized, public ledger-based cryptographic currencies and expounds its most important features for the subsequent legal analysis.

The section "Conceivable regulatory approaches and the development of new investigation methods" draws attention on conceivable regulatory approaches in terms of crime prevention, AML, and criminal investigation methods. The lack of a central administrative institution necessitates a regulation concept that is aimed at the natural and legal persons participating in the cryptocurrency system directly or indirectly through its surrounding ecosystem. For the same reason, investigators cannot rely on bank documents, bank employees, or automatic account screening. This section gives an overview of regulatory approaches and investigation methods which seem to be promising.

The section "Natural and legal persons in and around the Bitcoin system affected by regulation and investigation" focusses on the natural and legal persons in and around Bitcoin. Such persons can take various roles in the Bitcoin core system (e.g. users sending and receiving payments in bitcoins), in the "Bitcoin ecosystem" (e.g. exchange platforms), the financial sector (like banks, trusts, etc.), and the real-world economy (e.g. merchants) (p. 18 in [22]). Furthermore, the section "Natural and legal persons in and around the Bitcoin system affected by regulation and investigation" examines in which ways the regulation approaches and investigation methods discussed in section "Conceivable regulatory approaches and the development of new investigation methods" affect the interests and needs of the persons in and around the Bitcoin network.

Finally, section "Regulation, investigation and fundamental rights" analyzes which fundamental rights of the persons mentioned in section "Natural and legal persons in and around the Bitcoin system affected by regulation and investigation" are affected by both, the regulatory approaches and investigation methods described in section "Conceivable regulatory approaches and the development of new investigation methods." The fundamental rights will therefore be divided into three main categories. The first group consists of fundamental rights affected by nearly every regulatory approach in every cryptocurrency system (e.g. the right to property). The second contains some fundamental rights which become relevant specifically in peer-to-peer-based cryptocurrencies like Bitcoin, for example, the freedom of association. The third group encompasses fundamental rights which do not—at first sight—have an obvious impact on governmental regulation and prosecution, like the freedom of speech or the freedom of information. Authorities have to respect the fundamental rights of the persons affected and find the legitimate balance if multiple conflicting rights are concerned.

Besides the conclusion, section "A brief glance at the international situation" points out that further (interdisciplinary) research is necessary in order to develop efficient prevention concepts and investigation methods and to examine the legal limitations of those measures.

Bitcoin's specific features in terms of regulation

Fundamental rights protect specific conducts of an individual against interference by the state. For example, the freedom of telecommunication (Art. 7 CFR, 8 ECHR) safeguards any form of undisclosed communication between natural and legal persons from intervention by any governmental authority ([23], Art. 8 paras 3, 4, 28 in [24], para. 60 in [25], para. 01.21 A in [26], Art. 7 para. 25 in [27], Art. 7 para. 24ff in [28], para. 43 in [29]). In order to invoke a particular fundamental right, the conduct in question has to be related to specific objects. For example, a behavior only falls within the scope of the right to property if it is connected to an object that meets the definition of "property." Hence, to answer the question of which fundamental rights apply to behaviors related to holding, trading and using Bitcoins or running the Bitcoin system, it is necessary to understand which characteristics define Bitcoins, which kinds of behaviors occur in and around the Bitcoin system, and what distinguishes Bitcoin from money, chattels and bank money. This overview will restrict itself to the most important properties for the legal analysis since most readers already possess (basic) knowledge of Bitcoin's technology. If further information is required, there are specific articles addressing the technical perspective [2, 4, 30, 31].

2 Others are the International Covenant on Civil and Political Rights (ICCPR) and the Inter-American Convention on Human Rights (IACHR) for example.

3 Sometimes also referred to as "virtual currencies", for example: "1) Closed virtual currency schemes. These schemes have almost no link to the real economy and are sometimes called "in-game only" schemes"; "2) virtual currency schemes with unidirectional flow. The virtual currency can be purchased directly using real currency at a specific exchange rate, but it cannot be exchanged back to the original currency"; "3) Virtual currency scheme with bidirectional flow. Users can buy and sell virtual money according to the exchange rates with their currency" (p. 13 in [20]).

The Bitcoin system does not operate like traditional currency systems. In real-world currency systems, governments,[4] central banks, and private banking institutions function as central administrative and control units. On the contrary, in the Bitcoin system volunteers (i.e. users who run a full client[5]) contribute processing power to a peer-to-peer network that runs a program (the Bitcoin protocol) to keep track of the account balances of all users. A bitcoin is basically a track of transactions between several public keys in the blockchain [30]. Hence, "holding" bitcoins means controlling the public key (Bitcoin address) which has received the last recorded transaction. A Bitcoin user exercises power over a public key by possessing the corresponding private key. Every transaction is stored in a public distributed ledger, called the "blockchain." The latter cannot only be viewed by participants in the peer-to-peer network but also by everybody who uses blockchain analytic tools on the Internet like www.blockchain.info. Adding a data block (which contains transactions of the users) to the blockchain is called mining. Bitcoin miners are users who provide their CPU power for the mining process [2, 31, 32]. A successful miner is rewarded with newly mined bitcoins (besides the transaction fees offered by the parties of the transaction [30]) in order to motivate users to provide computing power for the network's operation [31, 32]. Even if the blockchain is public, participants in the Bitcoin network remain (if they choose to do so) pseudonymous [4]. This is possible because every client can create an infinite number of unique and independent public keys [31]. Thus, no user has to identify himself to an administrative unit (in contrast to opening a bank account). Usually, only the holder of the private key knows to whom the associated public key is related. Besides through the aforementioned mining process, an individual can get bitcoins by changing real currency into bitcoins at specialized exchange markets (also vice versa) [8], Bitcoin ATMs (not vice versa) [33] and on Internet platforms like localbitcoins.com or bitcoin-treff.de.

Due to technological features of cryptocurrencies, governments not only have to face obstacles but can also make use of opportunities when regulating them: on the one hand, regulation scenarios have to find a solution for the lack of central administrative parties. Standard Know-Your-Customer (KYC) systems will not work if users do not have to identify themselves when opening an account [34]. Furthermore, the pseudonymity of cryptocurrencies hinders any concept that is depended on the knowledge of the users' identity, for example, as it is required by law enforcement agencies' supervision of an individual (p. 469ff in [7]). On the other hand, the public transaction record enables new regulatory approaches. For example, in comparison to regaining stolen cash from circulation, it is possible to isolate and devalue bitcoins through transaction blacklisting [30, 35]. The same applies to the profit of other illicit activities like drug-trafficking and blackmail [35]. The possibility to track every single bitcoin back to its origin provides for another opportunity for regulators: even if several bitcoins are stored in the same wallet of a user (precisely, the private keys are stored in it) or even if several bitcoins are related to the same public key, every bitcoin in the wallet or related to the public key is distinguishable owing to its traceable and unique history. Hence, unlike in classic banking systems, single transaction outputs are separated from each other at any time and thus can be blacklisted without "poisoning" all bitcoins related to the respective public key [34, 35].

Conceivable regulatory approaches and the development of new investigation methods

What governments and prosecutors have been doing for decades in terms of AML and financial crime investigations is difficult to apply and enforce in the context of Bitcoin and other cryptocurrencies [8, 13, 36, 37].

Regulating cryptocurrencies in terms of AML

Traditionally, AML concepts rely on KYC systems, due diligence, compliance systems and monitoring and reporting duties of banks and other financial service providers [7, 13, 31, 38]. Depending on the scale of transactions, the domicile of the business partner and, especially in contractual relationships with politically exposed persons, financial service providers have to check the identity of their contractual partners, gather information regarding the purpose and the type of the business relationship sought, make a risk assessment and monitor the relationship continuously (see FATF Recommendations No. 10–23 [31, 39]). In the context of traditional, "real" currencies, this concept is (arguably p. 8ff in [31]) effective because a person can only participate in the deposit money system with a bank account (and huge amounts of cash are hard to store and transport, especially across borders). In contrast to that, in the Bitcoin system users can create their own "account" (= the wallet) on their own device and create as many key pairs as they want without involving any financial service provider. Hence, AML measures have to be directed towards the legal and natural persons who exchange cryptocurrencies for real currencies or goods, like exchange platforms and merchants (p. 23 in [31]). Furthermore, "classic" KYC is not effective in cryptocurrency systems for three reasons: first, for merchants in the mass market, KYC is simply not practicable (p. 57 in [38]). Second, if criminals find persons (or exchange platforms located outside the respective jurisdiction; see p. 30 in [31]) who exchange real money for cryptocurrencies, they do not need to use any regulated exchange platforms (located inside the respective jurisdiction) (p. 22 in [40]). Seeking out those persons/exchange platforms—even abroad—is relatively easy, because there are intermediary platforms on the Internet, for example, localbitcoins.com. Moreover, no suspicious-looking amounts of cash have to be physically smuggled over borders in order to exchange them abroad (p. 20ff in [31]). Third, exchange platforms "pop up and disappear so quickly" (p. 23 in [31]) on the Internet that it is not possible for (national) law enforcement agencies to be aware of all platforms located in the respective jurisdiction. Nevertheless, several governments and transnational organizations are planning to install—or have already installed—KYC systems for exchange platforms (and other types of users), like the BitLicense Law of the State of New York, section 200.15 (e) (1), the Payment Services Act of Japan from April 2017, Canada's Bill C-31 (An Act to Implement Certain Provisions of the Budget Tabled in Parliament on February 11, 2014 and Other Measures, Second Session), the inclusion of Digital Currency Exchange Providers in the Anti-Money Laundering and Counter Terrorism Financing Act in Australia (came into force 2018) or the Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849, Art. 2 lit. g, lit. h ([2, 4], p. 457ff in [7, 9, 11, 31, 36, 38, 41], p. 39ff in [42, 43]). As a necessary preliminary stage to KYC and due diligence,

4 This article will not distinguish legislative measures from executive or judiciary acts because different authorities are responsible for different measures in different legal systems. Therefore, in this paper the term "government" refers to all authorities that are responsible for measures concerning regulation, prevention and prosecuting in the context of cryptocurrencies.

5 You can download a full client at: https://bitcoin.org/en/choose-your-wallet.

governments started to place the permission to trade with and exchange cryptocurrencies under reservation of supervisory approval (e.g. BitLicense of the State of New York [1, 2, 7, 10, 43, 44], Canada's Bill C-31 or the draft law on digital financial assets of the Russian Ministry of Finances from 20 January 2018 [43]).

Besides classic KYC systems and licensing, there are many conceivable regulation approaches in the context of cryptocurrencies [8, 11, 35]. Again, it has to be mentioned that differently designed "cryptocurrencies" need to be regulated differently depending on their technological characteristics. The (current) technological design of the Bitcoin system offers many opportunities for regulators. First, authorities could restrict the access to cryptocurrencies. Besides a blanket ban (p. 35 in [10]), limiting the access to the Bitcoin software (e.g. Bitcoin clients, online wallets) is a conceivable albeit hardly enforceable regulatory approach. Second, public authorities could try to control or at least influence the mining process by either participate with governmental mining pools or by regulating the production of or the access to mining hardware.[6] Third, the exchange of cryptocurrency with real money and goods (and vice versa) could be restricted and/or controlled by authorities [35, 38], like China and India are doing right now [43].

As mentioned above, the decentralized character of the Bitcoin network is a strong argument for implementing prevention concepts which are directed toward the "gatekeepers" who operate on the border between cryptocurrencies and the real world [8]. A notable example of such approaches is transaction blacklisting [34, 35]. The goal of this concept is to blacklist transactions (precise: transaction prefixes) which were caused by criminal offenses like blackmail, fraud or money laundering. Actors in the "Bitcoin ecosystem" like exchange platforms and merchants who accept bitcoins for payment would not be allowed to accept blacklisted transactions or transactions which can be traced back to a blacklisted transaction [34, 35]. The advantage of such an approach is that exchange platforms and merchants are tangible for law enforcement agencies because they operate in the real world [22]. Another benefit lies in the (at least partial [22, 35]) devaluation of bitcoins from blacklisted transactions. This devaluation is caused by both an economic and a legal effect: Bitcoin users will not pay the same price for blacklisted bitcoins as for non-listed bitcoins because they cannot use listed bitcoins to pay for goods or exchange them [22]. If the transaction blacklist were public (or at least users could request whether bitcoins offered originate from a listed transaction), users would be forced to check the list in order to avoid criminal prosecution for money laundering. This makes criminal activities with the aim of gaining Bitcoins less attractive. It has to be mentioned that the devaluation of blacklisted Bitcoins could lead to a problem for the Bitcoin system: It has been stated that blacklisting leads to a dramatic loss of Bitcoins' fungibility since blacklisted Bitcoins have less value than not-blacklisted ones [22, 45, 46]. Nevertheless, it can be argued, that the lack of fungibility is (from an economic point of view) a necessary consequence of the "unique transaction history" (p. 28 in [22]) of every Bitcoin and the dependence of the price of a Bitcoin on the "information encoded in the transaction history" (p. 28 in [22]). Moreover, there are market mechanisms like risk assessment that could probably manage the problem of different values of different Bitcoins (p. 28 in [22]).

Despite the improvements that transaction blacklisting brings to the regulation of cryptocurrencies, this concept also has shortcomings. First of all, a blacklist maintained by public authorities cannot cover off-chain transactions; the public authorities would therefore be dependent on the cooperation of the service providers carrying out the off-chain transactions. However, these could be forced to cooperate by corresponding laws and sanctions if necessary. Furthermore, the transaction blacklisting system would have to be implemented worldwide in order to develop its full effectiveness. However, it seems unlikely at present that all states will be able to agree on a common blacklist, not least because different activities are classified as "illegal" in different states. Within the EU an agreement seems possible, but a solely European blacklist would possibly collide with the regulation of other states and confederations of states, for example, in cryptocurrency transactions between citizens of the EU and those of non-EU states. In order to resolve these conflicts, appropriate international agreements would have to be concluded with these states. And finally, a functioning blacklisting system could be abused by authoritarian regimes to deprive political dissidents of a so far largely unrestricted possibility of financing. This risk is inherent in any effective cross-border regulatory measure. A current example outside the world of cryptocurrencies is the misuse by authoritarian states of the instrument of the international arrest warrant to detain regime critics.

Other conceivable regulatory approaches (p. 33ff in [35]) using listing of transactions and/or accounts are account blacklisting, account or transaction whitelisting [38, 48] and transaction redlisting [49] (enforced by miners). They will not be discussed in detail here, because they are less effective compared to transaction blacklisting for several reasons. For example, every method that tackles accounts (precise: public keys) is easy to bypass by simply creating new accounts (p. 66 in [38]).

Criminal investigations in the context of cryptocurrencies

The decentralized structure of the Bitcoin network and the users' pseudonymity cause similar problems for prosecutors as they do for regulators. Traditionally, criminal investigators in the field of financial crimes (or investigators in general when tracing the money trail) rely on the search and seizure of bank documents and files, the questioning of bank employees as witnesses and the automatic screening of bank accounts. Without central administration and the ability of every user to create an indefinite number of accounts by himself or herself, those investigation methods must fail. They are only promising when the suspect uses an account offered by a service provider which has an obligatory KYC system (§10 in [50]). Although the number of KYC systems will rise with governmental regulation, investigators must find ways of identifying Bitcoin users who are not covered by KYC systems (p. 99 in [13]). To tackle this challenge, investigators can use the public blockchain data: every transaction can be traced back through the blockchain to the genesis of the transferred bitcoins. Investigators can use forensic software to process the blockchain data and combine it with datasets from other internal and external (e.g. Internet data) sources. In this way investigators are (sometimes) able to draw conclusions about the natural and legal persons involved [3, 4, 32, 38, 51, 52]. This approach could be supported by the implementation of Central Cryptocurrency User Databases for Financial Intelligence Units like

6 There are only a few companies that manufacture efficient mining hardware [47].

proposed in the 5th AML-Directive of the European Union (15, p. 57ff in [53, 54].

Natural and legal persons in and around the Bitcoin system affected by regulation and investigation

As shown in the previous section, governments and prosecutors must develop new regulatory concepts and investigation methods and/or adjust the traditional ones. Both ways can affect the needs and interests of several natural and legal persons in and around the Bitcoin system. As a first step, it is necessary to identify the "natural" and "legal" actors of the Bitcoin network in order to examine the fundamental rights which have to be taken into account. In the traditional currency and banking system, governments, central banks, private banks and other payment processors are the main actors. Governments create currencies and banks operate the system, subduing to governmental rules. Other natural and legal persons, like bank customers and merchants, are only allowed to participate among the required conditions. For example, every bank customer has to identify himself with an official document when opening a bank account. In contrast thereto, every Bitcoin user can create bitcoins by providing computing power to the system. The system is operated by the peer-to-peer network, in other words, by all users (who provide CPU power). Hence, regulation approaches and investigation methods cannot focus (only) on banks (see section "Conceivable regulatory approaches and the development of new investigation methods"). They have to consider many different kinds of natural and legal persons in and around the Bitcoin system. Similar to the classification of the Bitcoin system and the real world by *Möser/Böhme/Breuker,* the persons in and around the Bitcoin System can be divided into three groups: persons "inside" the Bitcoin system, persons in the so-called "Bitcoin ecosystem", and persons operating within the real-world economy [22]. First, the developers of the Bitcoin protocol, Bitcoin miners (especially mining pools) and users can be described as operating "inside" the Bitcoin system.[7] Second, there are persons, who operate as intermediaries between the Bitcoin system and the real-world economy (in the Bitcoin ecosystem). Exchange platforms, remote wallet providers and mixing service providers are included in this category.[8] The third category contains several groups of natural and legal persons in the real-world economy like banks, trusts, merchants and service providers who buy and sell cryptocurrency units or accept cryptocurrencies for payment. By regulating cryptocurrencies and investigating in the blockchain, governments and prosecutors collide with several interests and needs of the currently affected persons. In the literature it has recently been claimed that most Bitcoin users nowadays no longer manage their Bitcoins themselves (i.e. do not store the private keys of their Bitcoin addresses in a wallet themselves), but leave the management of the private keys completely to a service provider (e.g. Exchange Service, Wallet Provider). Therefore, these persons are not Bitcoin users in the narrower sense, but only customers of "shadow banks." They would therefore have the same legal status as "normal" bank customers (debt holders) [55]. It is true that persons who merely hold a claim against a Bitcoin service provider enjoy the same protection by fundamental rights (e.g. the right to property) as other holders of claims outside cryptocurrency systems. However, this does not alter the relevance of the following remarks on fundamental rights for those users who manage their private keys on their own and are therefore actually themselves to be regarded as "owners" of the Bitcoins. To the best of my knowledge, no empirical study has been published on the question of how many Bitcoin users actually manage their Bitcoins themselves, how many users use service providers and how these service providers handle the Bitcoins for their customers exactly. Moreover, the behavior of users in Bitcoin or other cryptocurrency systems can change at any time, so that the basic considerations regarding the protection of fundamental rights will continue to be important in the future. And finally, regulatory concepts must cover those users who deliberately do not use regulated service providers in order to circumvent traditional AML regulation.

Regulation, investigation, and fundamental rights

The natural and legal persons mentioned in section "Natural and legal persons in and around the Bitcoin system affected by regulation and investigation" have different interests and needs in the context of cryptocurrencies. For example, exchange platforms want to conduct their business, mining pools want to earn their reward in Bitcoins, users want to make transactions in the pseudonymous network and store value in bitcoins, etc. Many of these interests and needs might be protected by fundamental rights (e.g. the right to pursue a trade or profession, the right to property, the right to protection of personal data, etc.). Anytime the government or law enforcement agencies interfere with these fundamental rights they have to ensure that their acts "are provided for by law and respect the essence of those rights" (Art. 52 (1) CFR). Moreover, they have to fulfill the criterion of necessity and "genuinely meet objectives of general interest" (Art. 52 (1) CFR). In order to develop new regulation concepts and investigation methods, governments and law enforcement agencies need to identify the fundamental rights they have to consider. To date (and to the knowledge of the author), no examination of the relation between AML regulation, crime prevention, criminal investigation and fundamental rights in the particular context of cryptocurrencies has been published. Hence, this section tries to start the dialogue by examining the interference of the regulation models and investigation tools mentioned in section "Conceivable regulatory approaches and the development of new investigation methods" with the fundamental rights of the persons mentioned in section "Natural and legal persons in and around the Bitcoin system affected by regulation and investigation." There are three categories of fundamental rights that can be distinguished with regards to cryptocurrencies: the first group includes fundamental rights that play a major role in every cryptocurrency system.[9] I shall refer to these as the "cryptocurrency classics." The second group consists of fundamental rights which have to be considered only in peer-to-peer based cryptocurrencies like Bitcoin. The third category encapsulates fundamental rights with a less obvious relation to cryptocurrencies.

7 This description lacks absolute technical precision: Users and miners use the client software to get access to the peer-to-peer network and to the blockchain data. Nevertheless, describing users and miners as being "in" the Bitcoin System is useful to distinguish those kinds of actors from persons operating on the dividing line between the Bitcoin System and the real-world economy (the so-called "Bitcoin ecosystem").

8 It is justifiable to include mining pools in this category as well [22] because they invest electric power and hardware to generate bitcoins. This can be perceived as an "exchange" of real world currency into bitcoins.

9 Including centralized, not peer-to-peer based systems.

Cryptocurrency classics

In every cryptocurrency system, users transfer data to one another. This transfer of data represents a transfer of value. During this process, the scope of two fundamental rights can be affected: freedom of telecommunication (i) and the protection of personal data and private life (ii). Since transferred data represents value, it is self-explanatory to take the right to property into consideration (iii). Moreover, the transaction of value always involves traders and investors. Therefore, the right to pursue a trade or profession has to be taken into account as well (iv).

Freedom of telecommunication

The right to freedom of telecommunication is provided for in Art. 8 ECHR and Art. 7 CFR. Art. 8 § 1 ECHR speaks of "respect" for everyone's "correspondence" while Art. 7 CFR uses the word "communications." Even if the exact wording is different, both rights have the same scope of application (Art. 7 para. 1 in [27], para. 53 in [56]). The Explanatory Note on Art. 7 CFR determines that Art. 7 CFR is based on Art. 8 ECHR (among others). Hence, as Art. 52 (3) CFR states, the meaning and scope of these provisions "shall be the same." Moreover, the ECtHR's case law has to be taken into consideration when interpreting Art. 7 CFR (para. 07.03A in [26], Art. 7 para. 1 in [27], Art. 7 para. 24 in [28], para. 42 in [29]). Art. 7 CFR, 8 ECHR protect any form of undisclosed communication between natural and legal persons from intervention by any government authority ([23], Art. 8 paras 3,4, 28 in [24], para. 60 in [25], para. 07.21A in [26], Art. 7 para. 25 in [27], Art. 7 para. 24ff in [28], para. 43 in [29]). The protection of only private, that is, 'undisclosed' communication, means that only messages with a specified or specifiable addressee are protected by Art. 7 CFR, 8 ECHR (Art. 7 para. 25 in [27]). Any form of public communication does not fall within the scope of Art. 7 CFR, 8 ECHR (Art. 8 para. 28 in [24], Art. 7 para. 25 in [27]). Even if the receiving party of a Bitcoin transaction were considered as a specifiable addressee, the data in the blockchain remains public. Hence, the transaction data in the blockchain is not protected by Art. 7 CFR, 8 ECHR due to its non-confidential character. Therefore, prevention and/or criminal investigation measures which collect and/or process data from the blockchain are not in any way restricted by Art. 7 CFR, 8 ECHR [57].

The protection of personal data and private life

The protection of personal data is part of the protection of "private life" in Art. 8 ECHR (Art. 8 para. 10 in [24]). Data protection is mentioned specifically in Art. 8 CFR. Nevertheless, Art. 7 CFR is based on Art. 8 ECHR (Art. 8 para. 10 in [24]). Therefore, personal data is also protected by Art. 7 CFR (para. 07.66 A in [26], para. 47 in [58], para. 44 in [59]). Hence, the protection of private data is guaranteed by Art. 7, 8 CFR, 8 ECHR. The right to data privacy is concerned when authorities collect, store, share or process data related to a natural (or legal)[10] person and the person's "private life" is thereby affected (Art. 8 para. 10 in [24], para. 74 in [60]). In contrast to the scope of freedom of telecommunication, the scope of data privacy can include the protection of public data (Art. 8 para. 6 in [27], para. 31 in [61]): Art. 7, 8 CFR, 8 ECHR are affected when government bodies collect and store public data systematically (Art. 8 para. 10 in [24], para. 43 in [62]). It is crucial to clarify that "systematically" does not necessarily mean collecting, storing or processing data on a massive scale (and not even by using automatic means, see Art. 2 (b) Directive 95/46/EC). This can be concluded from the fact that Art. 8 ECHR was seen to be affected by filming a single suspect in a police station and storing the film (para. 43 in [63]), by sharing videos filmed on public places with the media (para. 63 in [64]), sharing photos of a suspect with the media (para. 29 in [65]) and by filming protestors and storing the video (para. 15 in [66]). However, the video monitoring of public areas "without" storing the videos is no interference with the right to data protection according to the European Commission on Human Rights [67].

Applying these principles to public internet data (like the data in the blockchain) leads to the following classification: the mere browsing of and searching for data in the blockchain (e.g. with tools like blockchain.info [68]) is not deemed an interference in the right to protection of personal data. However, an intervention in the right to protection of personal data is conceivable, when law enforcement agencies, prosecutors and/or regulators systematically collect, store and/or process data from the blockchain. For example, the implementation of Central Cryptocurrency User Databases, like proposed in the 5th AML-Directive of the EU (p. 57 in [53], [54), would be a serious and far-reaching interference with the right to protection of personal data (para. 34ff in [69]). Furthermore, the use of searching tools that collect and store data from the blockchain by authorities can also be seen as interference as long as the authorities have access to the stored data (either because the data is stored within the authorities' sphere of control (e.g. when criminal investigators use special searching tools specifically designed for law enforcement agencies that store data to provide or improve searching speed or results [4, 32, 51, 52, 70, 71]) or the authorities oblige private citizens (e.g. the companies that provide searching tools] to store the data and grant prosecutors access to it) (para. 34ff in [69]). These measures would interfere with the right to protection of personal data if the blockchain data is considered to be "personal data."

In accordance with Art. 2 (a) of the Directive 95/46/EC (on which Art. 8 CFR is based according to the Explanatory Note (Art. 8 para. 2 in [28]) *personal data* "shall mean any information relating to an identified or identifiable natural person."[11] In general, the whole term is interpreted widely. "Any information" means literally any type of information (para. 08.85 in [72]). It is not even necessary for the data to contain information about a natural (or legal) person. The information can concern an object, as long as this object is related to a natural (or legal) person (para. 08.85 in [72]). Pursuant to Art. 2 (a) of the Directive 95/46/EC an identifiable person is one "who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (Art. 8 para. 5 in [27]). Recital 26 of the Directive states that "all the means likely reasonably to be used (...) to identify the said person" should be taken into account when determining whether a person is identifiable (para. 08.85 in [72]). On the other hand, the right to data protection is not applicable when the data is "rendered anonymous in such a way that the data subject is no longer identifiable."[12]

10 It is a matter of an ongoing debate whether legal persons are protected by Art. 8 CFR ([23], Art. 8 para. 7 in [27], para. 08.96 in [72]).

11 A similar definition can be found in Art. 2 (a) of the Council of Europe Convention 108 which is, according to the Explanatory note, another source of Art. 8 CFR.

12 See recital 26 of Directive 95/46/EC.

On the basis of the principles described above, transaction data in the blockchain is protected by the right to data protection in Art 7, 8 CFR, 8 ECHR. Similar to the discussion about IP addresses (para. 08.86 in [72]), it has to be considered that knowing the public keys, which are part of a transaction, does not necessarily lead to the identification of the participating entities since everybody who has access to the private key has the power to transfer bitcoins from the relating public key. Thus, it is not necessarily the "legitimate owner" of the public key, who causes the transaction of bitcoins. Moreover, it has to be taken into account that the transaction data in the blockchain is pseudonymized. Hence, it cannot be solely used to identify the particular Bitcoin user. Nevertheless, the blockchain data can be combined with data sets from other sources (e.g. web forums, investigation records, etc.) in order to identify the respective user [51]. Therefore, Bitcoin users can be classified as persons who are "indirectly identifiable." Following recital 26 of Directive 95/46/EC the mere possibility of identifying users is enough to include blockchain data in the scope of the protection of personal data. Of course, the lower risk of de-anonymization lowers the legal obstacles to overcome when setting up legitimate grounds for data processing by law (para. 08.110ff in [72]).

The right to property [73 for a common law perspective]

The right to property is laid down in Art. 17 CFR and Art. 1 of the Protocol to the ECHR (which is a source of Art. 17 CFR as explained in the Explanatory Note). It includes "all rights with an asset value creating an established legal position under the legal system, enabling the holder to exercise those rights autonomously and for his benefit" (para. 17(1).16 in [74]). Therefore, the scope is not limited to moveable und immoveable physical objects (para. 17(1)16 in [74], para. 22 in [75]). Several immaterial pecuniary positions were regarded as being protected (para. 17(1)16 in [74]), like company shares [76] or intellectual property rights [77] (see Art. 17 (2) CFR) or even the "good will" [78] of a company (Protocol No. 1 para. 4 in [24]). However, rights must be "sufficiently established to be enforceable" (para. 59 in [79]) to fall within the scope of the right to property (Protocol No. 1 para. 3 in [24], para. 22 in [75, 80]). Consequently, "mere commercial interests or opportunities" are not protected (para. 22 in [75], para. 34 in [81]). The ECtHR extended the scope to "assets" in case the holder has a "legitimate expectation" of retrieving useful enjoyment of the asset (Protocol No. 1 para. 3 in [24], para. 51 in [82, 83]). This is the case when it has a "sound legal basis" in the respective domestic law (Protocol No. 1 para. 3 in [24], para. 47 in [80]).

It seems to be difficult to determine whether holding bitcoins (and other cryptocurrencies) falls within the scope of the right to property. On the one hand, the legal status of cryptocurrencies is one of the most controversial debates within this context. Considering the lack of materiality, cryptocurrency units are not chattels. Furthermore, they are neither a right nor a debt as it would require an obligee (at least one) on the one side and an obligor (at least one) on the other side [for German law: 84–86]. Even the category of "intellectual property" does not fit well because it relies on intellectual creation and bitcoins are created "mechanically" through mining without any intellectual achievement [86, 87]. On the other hand, cryptocurrency units meet all criteria for the positions and assets protected by the right to property: first, bitcoins have a market value. This is a strong argument to include bitcoins in the scope of the right to property because essentially the right to property protects definable units of value as a basis for freedom [for the right to property in the German constitution: 88]. Second, bitcoins can be seen as an "exclusive entitlement" (para. 17(1)16 in [74]), not by law but by their nature. As long as the user ensures that he is the only one who knows/stores the private key, he has exclusive access to the bitcoins assigned to the related public key. Hence, the user can "exercise those rights [read: bitcoins] autonomously and for his benefit" (para. 34 in [79]). Unlike other virtual goods like Linden-Dollar ([8], p. 14 in [20, 89, 90]) or WoW-Gold (p. 13 in [20, 91–94]), bitcoins cannot be simply deleted by a system administrator because there is not a single one with this power. This gives cryptocurrency units durability similar to other assets protected by the right to property. Third, cryptocurrency units are definable. One can exactly tell how many bitcoins are associated with the respective public key at any point in time ["Who owns what concept": 95]. In short, it can be said, therefore, that bitcoins meet all criteria of "virtual property": rivalrousness (= "on actors use of a resource bars others from use as a consequence"; p. 1049 in [95]), persistency, interconnectivity (other users can interact with it), definability and market value [12, 95–99].

To summarize, it can be stated that holding currency units like bitcoins should be seen as protected by the right to property [12, 87, 100]. Particularly in times of the "digital revolution", fundamental rights must remain open for further development to fulfill their protective function for the citizens. Therefore, the right to property has to be developed towards an all-encompassing protection concept for virtual assets. The aforementioned criteria can be used as a definition of "virtual property" in the scope of the right to property [85].

This gives rise to the question which kind of interferences with the right to property of bitcoin holders are conceivable. Traditionally, interferences with the right to property are divided into three categories: deprivations of possessions (expropriations), regulations to the use of property and other interferences with factual consequences (Art. 17 para. 18ff in [27], para. 17(1)28 in [74]). Deprivations of possessions can be sub-classified into legal and factual expropriations (Art. 17 para. 18ff in [27]). An example of an expropriation is a complete (or nearly complete; para. 122 in [101]) devaluation of bitcoins through a concept of transaction blacklisting.[13] The confiscation and seizure of bitcoins is likely to be seen as a regulation to the use of property (Art. 17 para. 18 in [27], para. 27 in [102]).

Finally, it should be mentioned that those Bitcoin users who have their Bitcoins administered by a service provider (e.g. wallet providers) and only have a claim under the law of obligations against the provider, enjoy the same protection by the right to property as other holders of claims.

The right to pursue a trade or profession

The right to pursue a trade or profession is codified in Art. 15 CFR (The Freedom to Choose an Occupation and Right to Engage in Work) and Art. 16 CFR (The Freedom to Conduct a Business). Art. 15 (1) CFR states that "everyone has the right to engage in work and to pursue a freely chosen or accepted occupation" while Art. 16 CFR emphasizes that "the freedom to conduct a business in accordance with Community law and national laws and practices is

13 Especially, when a "full poison" policy is applied (p. 21ff in [22]); the relationship between the devaluation of bitcoin through blacklisting and the "nemo-dat-rule" in the context of stolen bitcoins is a topic for future research; the "nemo-dat-rule" is (within its scope of application) one of several factors which affect the balance between the interests, needs and fundamental rights of the parties concerned and the public interest in AML and crime prevention.

recognized." It is controversial whether Art. 15 (1) CFR protects only employees or also entrepreneurs (Art. 15 para. 4 in [27]).

Art. 15 (1) CFR protects the choice and the practice of a profession. To be seen as a "profession", the respective activity must be for valuable consideration. This conclusion can be drawn from the wording of Art. 1 (2) European Social Charter (ESC): "the right of the worker to earn his living."[14] Therefore, the worker must have the intention of earning his livings. Furthermore, the worker must exercise the activity for a certain amount of time. Once only and (really) short-term activities do not fall within the scope of Art. 15 (1) CFR (Art. 15 paras 7, 8 in [27]).

The scope of Art. 16 CFR includes the commencement, the termination and the execution of a business (Art. 16 para. 9 in [27, 81]). Business can be defined as any independently conducted economic activity. The classification as a "business" in terms of Art. 16 CFR does not depend on the legal form or even the legality of the business (Art. 16 para. 8 in [27], Art. 16 para. 10a in [28]).

Professional traders, investors and operators of exchange platforms as well as miners and operators of mining pools can rely upon the freedom to conduct a business as long as they conduct their business independently and the activity is profit-orientated. Naturally, workers in such companies are protected by the freedom to choose an occupation and right to engage in work. Hence, any AML regulation concept (actually any regulation concept) which obligates companies or workers to check and monitor their business partners (like KYC systems including due diligence and compliance means) has to deal with those fundamental rights (p. 13 in [40]).

Peer-to-Peer networks and fundamental rights

One of the most innovative "features" of Bitcoin is the peer-to-peer basis of a currency system. In contrast to the classic banking system ran by governments, central banks and private banking institutes, the Bitcoin system consists of the entirety of users who participate voluntarily in the network (e.g. by providing computing power by enhancing the Bitcoin protocol or simply by transferring and receiving bitcoins).

This gives rise to a new question in terms of fundamental rights: can the Bitcoin community and/or every user rely upon the freedom of assembly and association?

The right to freedom of peaceful assembly and association is laid down in Art. 11 ECHR and Art. 12 (1) CFR (Art. 11 ECHR is the main source of Art. 12 CFR, see Explanatory Note). An assembly is defined as "every organized meeting of people with the intention to collectively form or express an opinion" (Art. 11 para. 5 in [24]). The scope includes private meetings as well as public ones (Art. 11 para. 5 in [24]). A political purpose is not required. Still, not every purpose is protected (Art. 11 para. 5 in [24, 103]). While the economic motivation of (most of) the participants in the Bitcoin network could (arguably) fall within the scope of the right to freedom of assembly, the Bitcoin network is not an assembly for another reason: assemblies of natural persons in the real world need a special kind of protection in comparison to the freedom of speech because of the very special dangers caused by the physical presence of many people in one place. The mere expression of an opinion without these dangers is protected by the freedom of speech. Virtual "assemblies" do not cause similar dangers. Hence, they do not fall in the scope of the right to freedom of peaceful assembly [104–109].

The term "association" is interpreted much more widely than "assembly": an association in terms of Art. 11 ECHR, 12 CFR is "any group of people pursuing specific common objectives with a minimum level of organization and stability" (Art. 11 para. 8 in [24], Art. 12 para. 14 in [27]). While economic associations are protected, public-law associations cannot invoke the right to freedom of assembly (Art. 11 para. 8 in [24], Art. 12 para. 15ff in [27, 110, 111]). The Bitcoin network is a group of people (=users) who run a system in order to transfer value (or at least participate voluntarily in the system). They are organized in two ways: the organization is based on the technical environment of the Bitcoin protocol and an unwritten consent of the users (could be seen as a "(virtual) social contract" [98]). An example for the "technical organization" is the fact that every mining node always adds its newly mined block with the most cumulative difficulty of the proof-of-work calculations to the blockchain (chapter 8 in [112]). The unwritten consent of users, for example, is illustrated by the fact that any modifications of the Bitcoin protocol can only be adopted by consensus (e.g. BIPs) [113]. In addition, there are elements of consensus between the participants of a Bitcoin transaction (e.g. the required amount of data blocks that are added to the blockchain after the data block containing the respective transaction had been attached to accept the transaction as valid) (chapter 2 in [112]). The existence of the Bitcoin network for around seven years proofs a "minimum of stability." Despite running a currency system, the Bitcoin network cannot be seen as a public-law association. According to the ECtHR, public-law associations are set up by governments or other authorities and they "enjoy prerogatives outside the orbit of ordinary law, whether administrative, rule-making or disciplinary, or that they employ processes of a public authority, like professional associations" (para. 101 in [111]). The Bitcoin network was set up and is operated by people on a fully voluntarily basis without any (known) influence from authorities. Moreover, it does not enjoy any legal prerogatives. Therefore, the Bitcoin network can be seen as an association in terms of Art. 11 ECHR, 12 CFR.

The right to freedom of association protects the foundation of associations as well as the right to join an existing foundation. To date, it is not clarified whether actions of the association (like the recruitment of members, the marketing of the association etc.) are also protected. Nonetheless, it is certain that specific work of the association without a close connection to the association itself (like transferring bitcoins in the Bitcoin system) is not protected by the right to freedom of association. These actions are protected by the respective fundamental right (Art. 12 para. 17 in [27]). The personal scope includes natural persons as well as legal persons, especially the association itself (Art. 11 para. 11 in [24], Art. 12 para. 19 in [27]). Keeping this in mind, it is evident that not every regulation concept collides with the right to freedom of association. However, any regulation concept that restricts the structure of the Bitcoin community itself or the access to the system (especially a blanket ban of Bitcoin) interferes with the right to freedom of association.

Some remarks on freedom of expression and freedom of information

Basically, a transaction in the Bitcoin system is a transfer of information from the sender to the network including the recipient of the Bitcoin transaction. Whenever information is transferred, the right to freedom of expression and information could be affected. These fundamental rights are provided for in Art. 10 ECHR, 11 CFR. The term "expression" is interpreted widely and includes *any form* of communication as well as "any content" of communication (Art. 10

14 Art. 1 ESC is a source of Art. 15 CFR, see the Explanatory Note of Art. 15 CFR.

paras 4, 5 in [24], para. 11.27 in [114]). In particular, it is not (like the term "opinion" in some domestic constitutions [115]) restricted to "value judgments" (Art. 10 para. 4 in [24]). Uttering facts, even if they are incorrect, are protected, too (Art. 10 para. 5 in [24]). Transferring information in electronic form is included within the "open" scope of Art. 10 ECHR, 11 CFR (para. 11.27 in [114, 116]). The scope of protection of the right to freedom of information is embellished in a similar way: it protects sharing and receiving information and ideas of any kind, regardless to the form of the information or the means of distribution and the access to any publicly available information (Art. 10 paras 9, 10 in [24]). In summary, it can be stated that freedom of expression and information protects (i) the sending, (ii) the receiving of any content[15] of communication, any ideas and any information in any form and (iii) the access to any publicly[16] available information.

Sending and receiving information

Prima facie, a Bitcoin transaction falls within the scope of both, freedom of expression and freedom of information, because it is a transfer of information from one subject to many others (the network). However, it has to be taken into account that even though a bitcoin transaction transmits information, its primary purpose is to transfer value instead of communicative content. Transferring value is predominantly protected by the right to property and the right to conduct a business (see sections "The right to property" and "The right to pursue a trade or profession"). To additionally fall within the scope of the right to freedom of expression and information, at least a minimum of communicative content that goes beyond the mere transfer of value must be inherent in the respective information's nature. At this point, it should be mentioned that transactions in the Bitcoin system *can* be used to implement any kind of additional information in the blockchain [117] by using tools like http://cryptograffiti.info or http://apertus.io/. When a message is transmitted or information is embedded in the blockchain using a transaction of bitcoins, this transaction clearly falls within the scope of the right to freedom of expression and information. But the question of whether a mere transportation of value using a transaction of bitcoins is protected by Art. 10 ECHR, 11 CFR still remains unanswered. Owing to the fact that every transaction of value includes a minimum of additional information—at least the information regarding what contract or other cause the transfer of value is related to—it should be assumed that every bitcoin transaction falls at least within the scope of the right to freedom of information.[17] For example, a transaction following the signing of a contract includes the information that the sender wants to meet his contractual obligations by executing the transaction. All things considered, transactions of bitcoins consist of both: a transfer of value and a transfer of information. Therefore, they fall within the scope of the right to property, the right to conduct a business and the right to freedom of expression and information.

In conclusion, any criminal investigation measure and any regulation concept that restricts transactions of bitcoins interfere with the sender's and receiver's freedom of expression and information.

Providing infrastructure for sending and receiving information

In terms of the personal scope it has to be clarified that not only sender and recipient of information are protected by Art. 10 ECHR, 11 CFR. Persons who provide software as an infrastructure for the transfer of information can also invoke the right to freedom of expression and information (para. 11.27 in [114]). This follows from the *Pirate Bay* decision of the ECtHR where the Court decided that providers of a file-sharing website can rely on Art. 10 ECHR (para. 11.27 in [114, 118]). Therefore, both the developer of the Bitcoin protocol and the Bitcoin miners fall within the personal scope of protection of Art. 10 ECHR, 11 CFR. It cannot be argued against this that the mining process is automated by software, since at least the provision and availability of the mining software can be linked directly to human initiative. Since today a large part of the communication infrastructure is operated automatically, excluding automated information processing from the scope of protection of freedom of expression and information would be a significant step backwards for the protection of fundamental rights in this area in general. Therefore, the provision of automated infrastructure for information processing should generally also be considered to be included in the scope of protection. Hence, any regulatory action that restricts the access to or the execution of Bitcoin mining interferes with the freedom of expression and the freedom of information of the Bitcoin miners. Furthermore, any restriction of the Bitcoin protocol's development and any regulatory guideline for developers interfere with their right to freedom of expression and information.

Access to the publicly available information in the blockchain

Due to the public availability of the information in the blockchain, accessing it is protected by the freedom of information. Hence, any administrative restriction of the access to the blockchain has to be checked against the right to freedom of information.

Conceivable interferences

In brief, any kind of administrative restriction of sending or receiving Bitcoin transactions and of the access to the information in the blockchain interferes with the freedom of expression and the freedom of information of the Bitcoin user, miner and/or developer. Therefore, any of the regulatory approaches mentioned in section "Conceivable regulatory approaches and the development of new investigation methods" that aims directly or indirectly at a restriction of Bitcoin transactions or the access to the blockchain (e.g. blanket ban, regulation of mining hardware, governmental mining pools, licensing of the use of Bitcoin) have to be checked against those fundamental rights.

A brief glance at the international situation

In the context of cryptocurrenices, human rights find themselves in a challenging situation internationally. Most governments seem to focus exclusively on possible damage and criminal activities as well as possibilities of taxation in connection with cryptocurrencies, without considering the human rights of the individuals and legal entities involved [43, 119]. Also the recent academic legal discussion (outside of the EU) on the worldwide regulation of cryptocurrencies does not address the possible conflicts of these regulations with human rights [120–126]. Therefore, future legal research in different countries should deal with the national and international human rights relevance of regulatory concepts for cryptocurrencies. The starting point could be the ideas for the human rights situation in the EU described in this article.

15 Disregarding restrictions provided for by the provision.

16 The right to access to documents of the authorities of the European Union is laid down in Art. 42 CFR.

17 Or: The message to the Bitcoin network that bitcoins are transferred from one public key to another [32].

Conclusion and future research

As shown, the actions of persons in and around the Bitcoin network (and other peer-to-peer based cryptocurrency networks) are protected by several fundamental rights. AML regulation and other crime prevention concepts of governments will likely interfere with the right to property, the right to pursue a trade or profession, the right to freedom of association and the right to freedom of expression and information. Criminal investigation measures that collect, process and/or store data from the blockchain systematically interfere with the right to data protection and private life. Finally, the holder of bitcoins can appeal to the right to property against the seizure and confiscation of bitcoins by law enforcement agencies. This does not mean that each of the aforementioned measures necessarily violate the respective fundamental right since all of them are subject to restrictions. Thus, interferences with these fundamental rights are justifiable. As laid down in Art. 52 (1) CFR, any limitation of fundamental rights "must be provided for by law and respect the essence of those rights and freedoms." Moreover, governmental restrictions of fundamental rights must fulfill the criterion of necessity. Every new regulation concept and investigation method must respect those requirements. Regulators must find a balance between the aforementioned fundamental rights and the interests and needs they want to and are obliged to protect (e.g. law enforcement, AML, consumer protection, etc.). The search for this balance and the concrete design of regulation concepts in respect of the fundamental rights is a highly relevant topic for future research.

This article has shown that further research is needed focusing on two major aspects: first, new prevention concepts (especially AML regulation) and investigation methods have to be developed to tackle the problems of pseudonymity and decentralization of peer-to-peer based currency systems. The same applies to modern disguising techniques such as cross chain and off chain transactions as well as cryptocurrency with strong anonymity such as Monero and Mixing Services, CoinJoins, etc. Second, further examination of the requirements and limits of those concepts and methods is needed. Therefore, future legal research should enhance the relationship between cryptocurrencies, governmental means and fundamental rights. For example and as mentioned above, further examination of the scopes of application of the examined (and other) fundamental rights in different jurisdictions is needed. Moreover, researchers, law enforcement agencies and other governmental bodies have to develop investigation methods and regulation concepts that are useful in terms of fighting crime with cryptocurrencies and respect the fundamental rights of the affected persons, at the same time. Particularly, governments must enact laws that provide a sufficient legal basis for interventions in fundamental rights and that respect the principle of necessity. Due to the innovative and fast developing technology of cryptocurrencies, interdisciplinary research is needed. Legal researchers need a profound understanding of new technologies to develop new legal concepts. However, authorities have to refrain from using new technical concepts for prevention and prosecution that do not observe the legal limitations [13].

Acknowledgements

The author thanks Professor Christoph Safferling, Professor Rainer Boehme and Dr. Johanna Grzywotz for useful comments and critique as well as Dr. Kevin Pike, M.A. for grammatical corrections. He also expresses his gratitude to the six anonymous reviewers and their useful remarks.

Funding

This work was supported by the European Union (Horizon 2020 research and innovation programme under grant agreement number 740558).

References

1. Brito J, Shadab H, Castillo A. Bitcoin financial regulation: securities, derivatives, prediction markets, and gambling. *Colum Sci Technol L Rev* 2014;**XVI**:144–219.
2. Burge ME. Apple pay, bitcoin, and consumers: the ABCs of future public payment law. *Hastings L J* 2016;**67**:1493–549.
3. Luther WRB. On what grounds? In: Peirce H, Klutsey B (ed.), *Reframing Financial Regulation: Enhancing Stability and Protecting Consumers*. Arlington, VA: Mercatus Center at George Mason University, 2016, 391–415.
4. Guadamuz A, Marsden C. Blockchains and bitcoin: regulatory responses to cryptocurrencies. *First Monday* 2015;**20**. http://firstmonday.org/article/view/6198/5163 (27 May 2019, date last accessed).
5. Akins B, Chapman J, Gordon J. A whole new world: income tax considerations of the Bitcoin economy. *Pitt Tax Rev* 2015. In press. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2394738 (27 May 2019, date last accessed).
6. Ahmed S. Cryptocurrency & robots: How to tax and pay tax on them. *S C L Rev* 2018. In press . https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3083658 (27 May 2019, date last accessed).
7. Bryans D. Bitcoin and money laundering: mining for an effective solution. *Ind L J* 2014;**89**:441–72.
8. Middlebrook S, Hughes S. Regulating cryptocurrencies in the United States: current issues and future directions. *Wm Mitchell L Rev* 2014;**40**:813–48.
9. Middlebrook S, Hughes S. Virtual uncertainty: developments in the law of electronic payment and financial services. *Business Lawyer* 2013;**69**:263–73.
10. Ponsford M. A comparative analysis of Bitcoin and other decentralised virtual currencies: legal regulation in the People's Republic of China, Canada, and the United States. *Hong Kong J Legal Stud* 2015;**9**:29–50.
11. Reyes C. Moving beyond Bitcoin to an endogenous theory of decentralized ledger technology regulation: an initial proposal. *Vill L Rev* 2016;**61**:191–234.
12. Tsukerman M. The block is hot: a survey of the state of Bitcoin regulation and suggestions for the future. *Berkeley Technol L J* 2015;**30**:1128–69.
13. Tu K, Meredith M. Rethinking virtual currency regulation in the Bitcoin age. *Wash L Rev* 2015;**90**:271–347.
14. Hacker P, Thomale C. Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law. *Eur Co Financ L Rev* 2017. In press. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820 (27 May 2019, date last accessed).
15. EU Commission to propose Central Database of Virtual Currency Users. *Bitlegal,* 24 July 2016.
16. Maxwell G. *[Bitcoin-development] Block Size Increase*. https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-May/007880.html (21 August 2018, date last accessed).
17. Olson C. Money laundering, bitcoin and blockchain: anonymity, transparency and privacy are not incompatible. *Blog article,* 27 May 2016, https://www.finextra.com/blogposting/12663 (27 May 2019, date last accessed).
18. Charter of Fundamental Rights of the European Union, Official Journal of the European Communities, 2012/C 326/02.
19. *CoinMarketCap: Cryptocurrency Market Capitalizations*. https://coinmarketcap.com/ (21 August 2018, date last accessed).
20. European Central Bank. *Virtual Currency Schemes*. Frankfurt: European Central Bank, 2012.
21. Bonneau J, Miller A, Clark J, *et al*. SoK: research perspectives and challenges for Bitcoin and cryptocurrencies. In: IEEE Computer Society

Conference Publishing Services (ed.), *2015 IEEE Symposium on Security and Privacy*. Piscataway, NJ: IEEE Computer Society Conference Publishing Services, 2015, 104–21
22. Moeser M, Boehme R, Breuker D. Towards risk scoring of Bitcoin transactions. In: Boehme R, Brenner M, Moore T *et al*. (eds), *Financial Cryptography and Data Security*. Heidelberg: Springer, 2014, 16–32.
23. ECtHR, Klass/Germany (9/6/1978); ECtHR, Malone/GB (8/2/1984) – No. 8691/79; ECtHR, A/France (11/23/1993).
24. Grabenwarter C. *European Convention on Human Rights*, München: C.H. Beck, 2014.
25. Pätzold J. In: Karpenstein U, Mayer F (eds), *European Convention on Human Rights: ECHR (German)*. München: C.H. Beck, 2015, Art. 8 ECHR.
26. Vedsted-Hansen J. In: Peers S, Hervey T, Kenner J, *et al*. (eds), *The EU Charter of Fundamental Rights*. Baden-Baden: Nomos Verlagsgesellschaft, 2014, Art. 7 CFR.
27. Jarass H. *The EU Charter of Fundamental Rights (German)*. München: C.H. Beck, 2016.
28. Bernsdorff N. In: Meyer J (ed). *The EU Charter of Fundamental Rights (German)*. Baden-Baden: Nomos Verlagsgesellschaft, 2014, Arts 7, 8, 16 CFR.
29. Tettinger P. In: Tettinger P, Stern K (eds). *Cologne Community Commentary on the EU Charter of Fundamental Rights (German)*, München: C.H. Beck, 2006, Art. 7 CFR.
30. Boehme R, Christin N, Edelman B, *et al*. Bitcoin: economics, technology, and governance. *J Econ Perspect* 2015;**29**:213–38.
31. Christopher CM. Whack-A-Mole: why prosecuting digital currency exchanges won't stop online money laundering. *Lewis Clark Law Rev* 2014;**18**:1–36.
32. Luu J, Imwinkelried E. The challenge of Bitcoin pseudo-anonymity to computer forensics. *Crim L Bull* 2016. In press. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2671921 (27 May 2019, date last accessed).
33. Genesis Bitcoin ATM. https://bitcoinatm.com/ (29 August 2018, date last accessed).
34. Moeser M, Boehme R, Breuker D. An inquiry into money laundering tools in the Bitcoin ecosystem. In: *Proceedings of the APWG E-Crime Researchers Summit*. Anti-Phishing Working Group, Inc., 2013, 1–14
35. Boehme R, Grzywotz J, Pesch P, *et al*. *Bitcoin and Alt-Coin Crime Prevention*. Erlangen: BITCRIME Project, 2017.
36. Hill J. Virtual currencies & federal law. *J Consum Commer L* 2014;**18**:65–71.
37. Trautman L, Harrell A. Bitcoin versus regulated payment systems: what gives?. *Cardozo L Rev* 2017;**38**:1041–97.
38. Marian O. A conceptual framework for the regulation of cryptocurrencies. *Univ Chic L Rev* 2015;**82**:53–68.
39. FATF. *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations*. Paris: FATF. http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf (29 August 2018, date last accessed).
40. European Commission. Proposal for a directive of the European parliament and of the council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending. Directive 2009/101/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0450 (27 May 2019, date last accessed).
41. Carney M. *The Future of Money, Speech by the Governor of the Bank of England*, 2 March 2018.
42. European Banking Authority. *EBA Opinion on Virtual Currencies*. https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (29 August 2018, date last accessed).
43. The Library of the Congress, Regulation of Cryptocurrency Around the World. https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf (18 February 2019, date last accessed).
44. NY Department of Financial Services. *New York Codes, Rules and Regulations. Chapter I. Regulations of the Superintendent of Financial Services. Part 200. Virtual Currencies*. http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf (29 August 2018, date last accessed).
45. Why Bitcoin Fungibility is Essential. https://www.coindesk.com/bitcoin-fungibility-essential/ (4 September 2018, date last accessed).
46. The Problem with Bitcoin that Everyone Seems to Ignore. https://www.reddit.com/r/Bitcoin/comments/374ss5/the_problem_with_bitcoin_that_everyone_seems_to/ (4 September 2018, date last accessed).
47. Bitcoin Mining Hardware Guide. https://www.bitcoinmining.com/bitcoin-mining-hardware/ (29 August 2018, date last accessed).
48. *Bitcoins in the US: Whitelisting and Licenses for a Clean Currency (German)*. https://www.heise.de/newsticker/meldung/Bitcoins-in-den-USA-Whitelisting-und-Lizenzen-fuer-eine-saubere-Waehrung-2047456.html (3 September 2018, date last accessed).
49. Dinesh E, Gilfoyle J, Richard JP. *Operational Distributed Regulation for Bitcoin*. arXiv: 1406.5440 (2014).
50. General Terms and Conditions of *Fidor Bank AG Regarding the Offer of the Exchange of Bitcoins on the Platform (German)*. https://www.bitcoin.de/de/agbFidor (4 September 2018, date last accessed).
51. Reid F, Harrigan M. An analysis of anonymity in the Bitcoin system. In: Altshuler Y, Elovici Y, Cremers AB *et al*. (eds), *Security and Privacy in Social Networks*. Heidelberg, Berlin: Springer, 2013, 197–223.
52. Ober M, Katzenbeisser S, Hamacher K. Structure and anonymity of the Bitcoin transaction graph. *Future Internet* 2013;**5**:237–50.
53. *Directive of the European Parliament and of the Council (EU) 2015/849*. http://data.consilium.europa.eu/doc/document/PE-72-2017-INIT/en/pdf (4 September 2018, date last accessed).
54. *Directive of the European Parliament and of the Council (EU) 2018/843*. https://eur-lex.europa.eu/legal-content/DE/TXT/? uri=CELEX%3A32018L0843 (18 February 2019, date last accessed).
55. Anderson R, Shumailov I, Ahmed M, *et al*., *Bitcoin Redux, Submission 38 to WEIS 2018*. https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/05/WEIS_2018_paper_38.pdf (18 February 2019, date last accessed).
56. CJEU, McB/L.E. (10/5/2010) – C-400/10 PPU.
57. Safferling C, Rueckert C. Telecommunication surveillance for Bitcoins (German). *MMR* 2015;**12**:788–94.
58. CJEU, Volker und Markus Schecke GbR and Hartmut Eifert/Land Hessen (11/9/2010) – C-92/09 and C 93/09..
59. CJEU, Pilkington Group/European Commission (9/10/2013) – C 278/13.
60. ECtHR, Wasmuth/Germany (2/17/2011) – No. 12884/03.
61. Nettesheim M. Right to respect for private and family life. In: Meyer-Ladewig J, Nettesheim M, von Raumer S (eds), *ECHR European Convention on Human Rights (German)*. Baden-Baden: Nomos-Verlagsgesellschaft, 2017, Art. 8.
62. ECtHR, Rotaru/Romania (5/4/2000) – No. 28341/95.
63. ECtHR, Perry/UK (7/17/2003) – No. 63737/00.
64. ECtHR, Peck/UK (1/28/2003) – 44647/98.
65. ECtHR, Sciacca/Italy (1/11/2005) – 50774/99.
66. EGMR, Friedl/Austria (5/19/1994) – No. 15225/89.
67. European Commission on Human Rights, Herbecq and others/Belgium (1/14/1998) – 32200/96 and 32201/96.
68. *Blockchain Luxembourg*. https://blockchain.info/ (04 September 2018, date last accessed).
69. CJEU, Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irland, The Attorney General (4/8/2014) – C-293/11 and C-594/12.
70. Snell J, Care D. Use of online data in the big data era: legal issues raised by the use of web crawling and scraping tools for analytics purposes. *Electron Commer L Rep* 2013;**18**:1–9.
71. Ling J. *The deep dark web is getting some company soon – from Canadian cops*. Vice News, 4 August 2015.
72. Kranenborg H. Protection of personal data. In: Peers, S, Hervey, T, Kenner, J, *et al*. (eds), *The EU Charter of Fundamental Rights*. Baden-Baden: Nomos Verlagsgesellschaft, C.H. Beck und Hart Publishing, 2014, Art. 8.
73. Low K, Teo E. Bitcoins and other cryptocurrencies as property? *L Innov Technol* 2017;**9**:235–68.

74. Wollenschläger F. Right to property. In: Peers, S, Hervey, T, Kenner, J, *et al.* (eds), *The EU Charter of Fundamental Rights*. Baden-Baden: Nomos Verlagsgesellschaft, C.H. Beck und Hart Publishing, 2014, Art. 17.
75. Depenheuer O. Right to property. In: Tettinger P, Stern K (eds), *Cologne Community Commentary on the EU Charter of Fundamental Rights (German)*. München: C.H. Beck, 2006, Art. 17.
76. ECtHR, Bramelid and Malmstroem/Sweden (12/12/1982) – No. 8588-89/79.
77. CJEU, Laserdisken ApS/Kulturministeriet (9/12/2006) – C-479/04.
78. ECtHR, Olbertz/Germany (5/25/1999) – No. 37592/97.
79. ECtHR, Stran Greek Refineries and others/Greece (12/9/1994) – No. 13427/87.
80. ECtHR, Kopecký/Slovakia (9/28/2004) – 44912/98.
81. CJEU, Sky Oesterreich GmbH/Oesterreichischer Rundfunk (1/22/2013) – C-283/11.
82. ECtHR, Pine Valley Developments and others/Ireland (11/29/1991) – No. 12742/87.
83. ECtHR, Pressos Compania Naviera S.A. and others/Belgium (11/20/1995) – No. 17849/91.
84. Rueckert C. Confiscation and Seizure in the Context of Bitcoin (German). *MMR* 2016; **5**:295–300.
85. Goger T. Bitcoins in Criminal Procedure – Virtual Currency and Real Life Enforcement (german). *MMR* 2016; **7**:431–34.
86. Kuetuek ME, Sorge C. Bitcoin in German Enforcement Law (German). *MMR* 2014; **10**:643–46.
87. Fairfield J. BitProperty. *SCL Rev* 2015;**88**:805–74.
88. BVerfGE 97, 350.
89. Ernstberger P. *Linden Dollar and Virtual Monetary Policy*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1339895 (4 September 2018, date last accessed).
90. Naone E. Making money in second life. *MIT Technology Review*, 14 August 2007.
91. Grinberg R. Bitcoin: an innovative alternative digital currency. *Hastings Sci Technol LJ* 2012;**4**:159–207.
92. Caldwell P. *Blizzard bans 59, 000 WOW accounts*. https://web.archive.org/web/20121106212709/ http://www.gamespot.com/news/blizzard-bans-59000-wow-accounts-6154708 (4 September 2018, date last accessed).
93. *PlayNoEvil Game Security - Game Cheating, Gold Farming and RMT News & Analysis: Blizzard bans 76, 000 accounts and removes 11 Million Gold from World of Warcraft*. https://web.archive.org/web/20061022125025/http://playnoevil.com/serendipity/index.php?/archives/883-Blizzard-bans-76, 000-accounts-and-removes-11-Million-Gold-from-World-of-Warcraft.html (4 September 2018, date last accessed).
94. Oswald E. *Blizzard Bans 30, 000 from WoW*. https://web.archive.org/web/20090226040328/ http://www.betanews.com/article/Blizzard-Bans-30000-from-WoW/1150137990 (4 September 2018, date last accessed).
95. Fairfield J. Virtual Property. *BUL Rev* 2005; **85**:1047–102.
96. Erlank W. Introduction to virtual property: lex virtualis ipsa loquitur. *PELJ* 2016; **18**:2525–59.
97. DaCunha N. Virtual property, real concerns. *Akron Intell Prop J* 2016; **4**:35–72.
98. Berberich M. *Virtual property (German)*. Tübingen: Mohr Siebeck, 2010.
99. Bollen R. The legal status of online currencies: are bitcoins the future? *JBFLP* 2013; **24**:272–93.
100. Aqui K. *IRS Notice 2014-21*. https://www.irs.gov/pub/irs-drop/n-14-21.pdf (04 September 2018, last accessed).
101. CJEU, Regione autonoma Friuli-Venezia and others/Ministero delle Politiche Agricole e Forestali (5/12/2005) – C-347/03.
102. ECtHR, Adzhigocich/Russia (10/8/2009) – No. 23202/05.
103. ECtHR, Countryside Alliance and others/UK (11/24/2009) – No. 27809/08.
104. Broehmer J. Chapter 19. In: Grote, R, Marauhn, T (eds), *ECHR/GG Concordance Commentary (German)*. Tübingen: Mohr Siebeck, 2006.
105. Arndt F, Schubert A. Freedom of assembly and association. In: Karpenstein, U, Mayer, F (eds), *European Convention on Human Rights: ECHR (German)*, Ed. 2. München: C.H. Beck, 2015, Art. 11.
106. AG Frankfurt/M. Criminality of an online rally (German). *MMR* 2005; **12**:863–69.
107. Seidel G. The right of assembly on the test-bench (German). *DOEV* 2002; **7**:283–91.
108. Depenheuer O. Versammlungsfreiheit. In: Maunz, T, Duerig, G (eds), *Constitutional Law – Commentary (German)*. Ed. 81, München: C.H. Beck, Art. 8.
109. Moehlen C. The right to freedom of assembly on the Internet - applicability of a classical human right to new forms of digital communication and protest (German). *MMR* 2013; **4**:221–230.
110. ECtHR, Sigurjónsson/Iceland (6/30/1993) – No. 16130/90.
111. ECtHR, Chassagnou/France (4/29/1999) – No. 25088/94.
112. Antonopoulos A. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, 2nd edn. Farnham: O'Reilly UK Ltd, 2017.
113. *GitHub: bitcoin/bips*. https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki (4 September 2018, date last accessed).
114. Woods L. Freedom of expression and information. In: Peers, S, Hervey, T, Kenner, J, *et al.* (eds), *The EU Charter of Fundamental Rights*. Oxford: Hart Publishing, 2014, Art. 11.
115. Art. 5 (1) Constitution of Germany.
116. CJEU, Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (11/24/2011) – C-70/10.
117. Ken *Shirriff's blog: Hidden surprises in the Bitcoin blockchain and how they are stored: Nelson Mandela, Wikileaks, photos, and Python software*. http://www.righto.com/2014/02/ascii-bernanke-wikileaks-photographs.html (4 September 2018, date last accessed).
118. ECtHR, Pirate Bay: Neji and Sunde Kolisoppi/Sweden (3/13/2013) – No. 40397/12.Ret
119. https://www.ai-cio.com/news/us-treasury-official-pushes-worldwide-cryptocurrency-regulation-kleptocrats-criminals/ (25 February 2019, date last accessed).
120. Blemus S. Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide, Revue Trimestrielle de Droit Financier, 2017, No. 4.
121. Chudinovskikh M, Sevryugin V. Cryptocurrency regulation in the BRICS countries and the Eurasian Economic Union. *BRICS L J* 2019;**4**:63–81.
122. Trautman L. Bitcoin, virtual currencies, and the struggle of law and regulation to keep pace. *Marquette L Rev* 2018;**447**:1–92.
123. Elven T. Cryptocurrency and constituency: understanding the existence of Bitcoin and its regulation in Indonesia, 2018. In: *4th International Conference on Management Science*, *Universitas Muhammadiyah Yogyakarta*, *Indonesia*.
124. Zelic D, Baros N. Cryptocurrency: general challenges of legal regulation and the Swiss model of regulation. In: *Proceedings of the 33rd International Scientific Conference on Economic and Social Development*. Varazdin, Croatia: Varazdin Development and Entrepreneurship Agency; Warsaw, Poland: Faculty of Management University of Warsaw; Koprivnica, Croatia: University North; Rabat, Morocco: Faculty of Law, Economics and Social Sciences Sale - Mohammed V University, 2018.
125. Drozd O, Lazur Y, Serbin R. Theoretical and legal perspective on certain types of legal liability in cryptocurrency relations. *Baltic J Econ Stud* 2017;**3**: 221–8.
126. Muedini F. The compatibility of cryptocurrencies and Islamic finance. *Eur J Islamic Fin* 2018;**10**:1–10