# Crypto mining business models: Points of contact to the AIFMD

Received (in revised form): 21st September, 2018

**Stefan Tomanek**

is a legal expert in the Department for Prudential Supervision Asset Management, Prospectus, Consumer Information, at the Austrian Financial Market Authority (FMA). While the supervision of undertakings for collective investments in transferable securities (UCITS) and alternative investment funds (AIFs) is the main focus of his work, he is also heavily involved in the area of crypto assets and related business models. In this context, he is also a delegate in international committees as well as The European Securities and Markets Authority (ESMA) committees. Prior to his work at the FMA, he gained valuable experience in the Legal & Compliance Department of a large Austrian bank. He holds a master's degree in law from the University of Vienna.

Prudential Supervision Asset Management, Prospectus, Consumer Information, Austrian Financial Market Authority (FMA), Otto-Wagner-Platz 5, A-1090 Vienna, Austria
Tel: +43 (0)1 249 59 – 3412
E-mail: Stefan.Tomanek@fma.gv.at

**Ralph Rirsch**

is a supervisor at the Austrian FMA in the Department for Integrated Conduct Supervision of Banks. He is specialised in the PRIIPs Regulation (on key information documents for packaged retail and insurance-based investment products) and new technologies. Before his time at the FMA, he worked as a consultant in the Austrian banking sector with a focus on regulatory issues (eg markets in financial instruments directive (MiFID II), payment services directive (PSD2)), large-scale IT implementations and database management. Additionally, he was active as a freelance systemic consultant for small and medium enterprises specialised in group dynamics. His academic background is in law (University of Vienna) and international business administration (Vienna University of Economics and Business).

Austrian Financial Market Authority (FMA), A-1090 Wien/Vienna, Otto-Wagner-Platz 5, Austria
Tel: +43 (0)1 249 59 – 4312
E-mail: ralph.rirsch@fma.gv.at

**Marlene Wintersberger**

is a legal expert at the Austrian FMA in the Department for Prudential Supervision Asset Management, Prospectus, Consumer Information. She is responsible for the supervision of management companies that manage UCITS or AIFs and Corporate Pension Insurance Funds. She passed her legal examination with distinction, was admitted to practice as an attorney-at-law and worked for many years as an independent lawyer. She holds a doctorate in law (University of Vienna).

Austrian Financial Market Authority (FMA), A-1090 Wien/Vienna, Otto-Wagner-Platz 5, Austria
Tel: +43 (0)1 249 59 – 3402
E-mail: marlene.wintersberger@fma.gv.at

**Abstract** This paper provides a technical overview and legal analysis of the activity of miners in proof of work-based crypto assets, focusing on the Bitcoin Blockchain as the most prominent example. The result of this analysis — mainly that mining is a financial service similar to the services performed by traditional financial intermediaries — is used as the foundation of a detailed legal analysis of a widespread crypto mining business model under the Alternative Investment Fund Managers Directive (AIFMD). The paper shows that such business models offer mining packages directly to retail investors via the Internet, and the operators of these so-called mining farms thereby raise capital from the public to generate a pooled return for investors in the form of 'mined' crypto assets, for example, Bitcoin ('BTC'). A detailed analysis of this fund-like structure leads to the conclusion that many currently operating crypto mining business models are already regulated by the AIFMD if all the relevant criteria of the AIFMD are fulfilled. This legal assessment has to be made on a case-by-case basis and entails serious consequences — depending on the national transposition of the AIFMD, it can even result in the prohibition of marketing units and shares of such AIFs to retail investors, as is the case in Austria. Operators of such business models that are already active on the market and that fall under the regulation of the AIFMD would be faced with registration or authorisation requirements and potential legal repercussions for operating an AIF without licence.

KEYWORDS: AIFMD, Bitcoin, Blockchain, crypto assets, mining, virtual currencies

## INTRODUCTION

With the steady evolution of crypto assets into a mainstream phenomenon, various business models have emerged in this field. Diverse investment opportunities in such assets are marketed to clients — directly — via the Internet. A common example is the offering of profitable investments in the crypto market either in the form of mining packages or as a participation in mining pools to (retail) clients. By selling these products, the operators of so-called mining farms raise capital from the public to generate a common return for investors in the form of 'mined' crypto assets, for example, Bitcoin (BTC). The news is full of stories of investment fraud connected to crypto assets, whether alleged or actually having occurred. The day-to-day interest in crypto assets by investors and the fund-like structure of such business models prompt the urgent question of the applicability of the Alternative Investment Fund Managers Directive (AIFMD).

At the outset, it is necessary to clarify that neither does the AIFMD explicitly cover crypto assets or mining business models nor does it cover every business model in this business area. The crypto economy is technically complex and new for both clients and regulators alike. Consequently, a comprehensive analysis of the technical and economic processes underlying this new market is essential to be able to adequately establish the facts of the case for any (regulatory) legal assessment. This paper, therefore, examines how BTC mining works and the tasks and functions performed by a 'miner'. Thereafter, considering a common business model in Austria (and similarly structured models) based on BTC mining as an example, we examine the scope of the AIFMD. In the event that all criteria for its applicability are satisfied, such a construction would be classified as an alternative investment fund (AIF). We, therefore, argue, contrary to popular opinion, that such business models do not operate in a legal vacuum. Such investment offers already fall under the supervision of the competent national authorities supervising the respective national laws transposing the AIFMD, for example, the Austrian Alternative Investment Fund Managers Act (AIFMG).

## A TECHNICAL AND ECONOMIC ANALYSIS OF BITCOIN[1]

The first step and the basis of any thorough legal analysis is to establish the facts of the case. In casu, this requires a basic understanding of the economic and technical workings of BTC mining. We, therefore, start by providing a summary of the technical and economic fundamentals of the Bitcoin Blockchain to serve as the basis for the subsequent legal analysis regarding the applicability of the AIFMD.[2]

## Technical basics of the Bitcoin Blockchain

The BTC network uses asymmetrical cryptography based on digital signatures. Every user in the network has two digital keys for each address they own — a private key and a public key. The private key is similar to a passcode that allows BTC on the related public key (similar to a bank account/public address) to be spent, that is, transferred to another address. Further, the BTC Blockchain utilises two types of transactions: regular transactions and coinbase transactions. The former make up the bulk of the transactions on the payment network (this term is not used in the strict legal sense of national or EU law but as a synonym for the transfer of value on the Blockchain) between users. The latter are the incentive the miners receive.

Each (derived) regular transaction requires sufficient inputs (unspent outputs of previous transactions — as funding) and at least one output (the receiving address — the public key) to be valid. This creates a seamless sequence of outputs of previous transactions that are used as inputs for new transactions (and thereby irreversibly spent) and results in a continuous chain of all transactions in the BTC network, up to the very first transaction in 2009.

The computers participating in this network are called 'nodes'. Nodes that enforce all the rules of the Bitcoin network (the network uses 18 rules that, among others, concern the technical features of the transaction as well as the assessment whether sufficient unspent BTC are available to fund the transaction) and hold a full copy of the entire Blockchain are referred to as 'full nodes'. Each of these nodes, as long as it is active, continuously participates in an on-going, iterative and decentralised 'voting process' to achieve a shared consensus about the valid state of the Blockchain. Essentially, this means that a consensus on the 'account balance' of every single address (public key) in the network is created continuously among the participants without a central authority (eg a bank) with the final power of decision. In addition to this task, each participating node performs a routing function for the network. In this capacity nodes receive and verify transactions and in turn transmit the transactions they verified successfully to the nodes they know. To be able to perform this task nodes continuously maintain connections to other nodes and create new connections to unknown nodes in the system.

## How does a transaction on the BTC Blockchain actually work?

This question can best be answered by analysing a simple example. User A intends to transfer two BTC to user B. To do this, A creates a transaction on the Blockchain and digitally signs it using his private key. He then broadcasts the transaction (himself or via his wallet provider) to the Bitcoin network by sending it to all nodes known to him (or his wallet provider — this is handled automatically by the Bitcoin protocol). The transaction is then checked individually by every single receiving node. This check includes, among others, the correct technical structure of the transaction, the maximum size of the transaction and the required authorisation (private key to public key). Only after successful verification do these nodes relay the transaction to the nodes known to them, resulting in new and valid transactions spreading through the network.

This mechanism of proliferation also ensures that invalid transactions cannot spread through the network. It protects the addressee of a transaction insofar as the creator of a transaction is not able to 'spend' Bitcoin he does not have available on his public key. It does not, however, solve the double spending problem, which means that the creator of a transaction could potentially transfer the 'same' BTC simultaneously (ie use the same unspent inputs multiple times within the same block — more about this follows) to multiple recipients. To address this issue the Bitcoin network employs a system to collect transactions in so-called blocks. Simply put, a block is a bundle of transactions with a fixed number, that is, position on the Blockchain. It should also be noted that transactions do not become part of the accepted version of the Blockchain and thus 'effective' simply by being spread through the network but only if they become part of a block that is accepted by the network.

### The tasks of Bitcoin miners

Nodes that create new blocks are called 'miners'. Miners are comparable to 'network operators' of the BTC network. They continuously 'listen' (ie search) for unprocessed transactions in the network and gather them into blocks. Before accepting a transaction into a block the miner performs a comprehensive check of every single transaction and for each block a 'proof of work', which will be described in detail later in this paper. After all this is done the node publishes the new block to the network.

Owing to the decentralised nature of the BTC network the following issue could arise: a miner may receive multiple transactions in the same block that use the same 'unspent' output of a previous transaction as input. Technically, on the basis of the current version of the Blockchain, all these transactions would be valid as the relevant input has not been 'spent' in an accepted block. To understand this concept, one has to keep in mind that the Blockchain 'thinks' in blocks. This means that approximately every 10 minutes a new shared understanding of the 'account' balances is created in the network. Transactions that have not yet been part of a block have to satisfy all checks based on the last valid version. Between two versions it is, therefore, technically possible to create multiple technically valid but conflicting transactions. Put simply, this would lead to one Bitcoin becoming two or more as the same Bitcoin is spent multiple times — 'double spending'. A mechanism to resolve this issue in the Bitcoin network is that miners generally only accept the first of multiple technically valid transactions pointing to the same input. The other transactions are not integrated into the block, which means that double spending cannot take place.

Anyone doing business using Bitcoin transactions should, therefore, wait for transactions to be confirmed by multiple (at least six or more) subsequent blocks before initiating 'real life' economic activities, because multiple miners (without any malicious intention) could be mining the same block simultaneously and incorporating different transactions based on the same input, as the transactions reach them at different points in time. The solution to this issue is provided by the distributed consensus mechanism described in this paper.

### 'Proof of work': Providing trust in a trustless system through a security mechanism

Besides validating transactions the miner has to perform a proof of work. The proof of work is an intentionally complex and resource-intensive computational task based on the 'HashCash' function. This task can be solved only by rapidly 'trying to guess' the correct answer ('nonce') — by 'brute force'. It therefore uses up a large amount of computing power and cannot be sped up by using a 'smarter' algorithm. Its solution, however, is very easy to verify for other participants in the network. The more computing power (hash rate) a node expends, the 'faster it can guess the solution' and the higher the chance of solving the computational task first (ie before the other miners performing the same task simultaneously).

This proof of work solves the problem of missing trust between actors in the distributed consensus system. Were the majority of the vote based on the principle 'one node–one vote' the system could fairly easily be manipulated by creating a large number of nodes in the network. To counteract such behaviour, consensus is based not on the number of voting nodes but on the length — the 'depth' of the chain of transactions. Each block in the chain requires a proof of work, and the solution of the computational task ('nonce' — 'number only used once') changes completely on the basis of the content of the block and can, therefore, not be reused for any other (manipulated) block. Accordingly, the longest chain of transactions necessarily also contains the most proof of work, meaning that this chain is representative of the majority of the computing power spent in the network and is thus accepted by the network. To change a block in the past an attacker would have had to perform the proof of work of the block he wished to manipulate as well as the proofs of work of all following blocks while the rest of the 'honest' miners would simultaneously still be mining blocks for the 'honest' chain. This means that the attacker would have to expend more computing power than the rest of the participants combined in the network to overtake them, an extremely costly and technically difficult undertaking. Aside from this, it can be argued that such an attack would also not be economically feasible as the attacker would have to control 51 per cent of the computing power in the network, but the attack would destroy the value of Bitcoin since users would not trust it anymore, thus making any investment in hardware to acquire the necessary computing power worthless.

To sum up, the aforementioned, the proof of work is not directly connected to the process of verification and routing of transactions. In fact, it acts as proof that the network can trust the miner without knowing him and as a technical security mechanism. Blocks, as long as they are valid and in line with the latest version of the Blockchain, are generally accepted by the network on a first-come-first-served basis, meaning that the fastest miner has the best chance to have his block accepted and receive the corresponding reward — the 'incentive'.

### *The incentive for mining*

The so-called incentive (as it is called in the Bitcoin whitepaper) is the financial stimulus for miners. It consists of the coinbase transaction, which, in turn, contains the block reward and transaction fees. The coinbase transaction differs from the regular (derived) transactions described earlier insofar as the miner is allowed to address it to himself, and it is the only transaction in a block that does not point to another transaction as input. It transfers original Bitcoin — the block reward (ie Bitcoin that have not previously been in circulation in the network) — to the miner. The transaction fees, on the other hand, originate from all the transactions combined in the current block. These fees are chosen freely by the creators of the transactions and are paid by them. Thus, it can be said that the miner receives original (ie 'new') Bitcoin as well as derived (ie 'already circulating') Bitcoin for the successful mining of a block if their block is accepted by the network (which means that it has to be valid and provided faster than other miners' blocks). If there is a backlog of transactions (Bitcoin is currently facing serious scaling issues), miners tend to prefer transactions with higher transaction fees, which means that transaction times for such transactions are usually much shorter than for transactions with lower or no transaction fees.

After performing the proof of work the miner transmits the new block to all the nodes he knows. This block is, in turn, checked individually by every single node that receives it. In case of positive verification each node then adds the block to their local copy of the Blockchain if it is the first valid block (ie carries the position number of the last accepted block plus one) and transmits it to all the nodes they know and so forth. Nodes also regularly check if their version of the Blockchain is in line with the rest of the network. As a rule, nodes always accept the longest chain. So if a 'split' (ie 'fork') occurs, this will become obvious once some further blocks have been mined. First, blocks mined by miners on the basis of the majority version will not be valid from the point of view of the nodes accepting a minority version of the Blockchain as content will differ between the versions. Second, and based on this, their version will not grow as quickly as the majority version as fewer miners will mine on the basis of the minority version and blocks will be rejected by minority nodes since they do not fit their version of the Blockchain. If a node notices that its version of the Blockchain is shorter than the versions of other nodes, it will at some point discard its version and instead adopt the majority version again. This way the network reaches a consensus about the valid version of the Blockchain by propagating and individually checking each new block. Eventually, only the successful miner (the miner whose block is accepted by the majority of the network) receives the incentive, and the block becomes part of the new and valid version of the Blockchain. Returning to the example discussed earlier, this means that aside from hundreds of other transactions in the block, A's 'balance' is reduced by two BTC, B's 'balance' is increased by two BTC (excluding transaction costs), and the miner's balance is increased by the incentive.

## APPLICABILITY OF THE AIFMD

The following legal analysis is based on the Austrian Financial Market Authority's (FMA's) supervisory approach to crypto assets. No official legal opinion has been issued by the European supervisory authorities (ESAs), so the Austrian FMA has had to subsume and assess the cases that have arisen on an independent basis.

### Mining as a financial service

On the basis of this analysis, the tasks of Bitcoin miners consist of the verification and validation of (payment) transactions as well as the execution and routing of these transactions. It follows that the processing of (payment) transactions (the goal of the BTC whitepaper was to create a 'Peer-to-Peer Electronic Cash System' outside the traditional financial system and thereby independently of financial intermediaries and the financial establishment) [3] on the BTC Blockchain is functionally equivalent to the tasks and services performed by financial intermediaries (such as banks) in traditional payment systems.

We, therefore, argue that BTC is used as a 'means of payment' or 'payment instrument' in the broader sense (not to be confused with the term 'legal tender' as in a currency issued by a nation state). While BTC is not universally accepted as a means of payment in the commercial world, it has already found a certain degree of acceptance and proliferation as a means of payment in daily life aside from its use as a speculative investment. In Austria, for example, various businesses, such as online stores, delivery services and even law firms, already accept payment in BTC.[4] Furthermore, the European legislature has already defined Bitcoin as a 'means of payment' in the Fifth Anti-Money

Laundering Directive.[5] The directive aims to prevent terrorist groups from 'being able to transfer money into the Union financial system or within virtual currency networks'. While the legislature primarily identifies virtual currencies as 'means of payment', the directive uses the more neutral term 'means of exchange' in the newly added point 18 of Article 3 to cover all the potential uses of virtual currencies, such as investment, store of value or use in online casinos. This is reflected in recitals 1, 8 and foremost 10 of the Fifth Anti-Money Laundering Directive. This assessment is also in line with the intended (and at least partially realised) goal of the Bitcoin whitepaper, namely, to create an alternative peer-to-peer payment network.

On the basis of the classification of Bitcoin as a means of payment and in the face of its actual use and proliferation, the Bitcoin network can indeed be acknowledged as a 'payment system' or 'payment network'. Bitcoin mining is, therefore, a service that the miner performs in a payment network and is thus to be classified as a financial service. This qualification is also applied by the Austrian FMA in the respective Frequently Asked Questions (FAQ) regarding the Austrian AIFMG.[6] Bringing new BTC into circulation is only part of the incentive for the miners. It should therefore not be assessed separately from or independently of the service that is being performed for the payment network, even if one disregards the growing importance of derived transaction fees in the BTC network.

## Application of this analysis on a common mining-based business model

The provider runs a so-called mining farm to mine crypto assets (eg BTC or Ether). The objective of this venture is to obtain a financial return for investors via the generation of incentives through the BTC mining process. The purpose of the contract between the provider and investors is often designated as the 'provision of IT services', supplying computing power to the investors over a certain period. The investors, in turn, provide the computing power to the mining farm and in case of successful mining are awarded a share of the incentive. This share is equivalent to the ratio of the investor's purchased computing power in relation to the total computing power of the mining farm. It may be paid out in the mined crypto assets or fiat currency (ie one that is actual legal tender, such as EUR, GBP). The investors' main motivation for purchasing computing power is thus not the operative use of the said computing power but the generation of a financial return.

## Test of the applicability of the AIFMD

According to point (a) of Article 4 (1) of the AIFMD and the Guidelines on Key Concepts of the AIFMD,[7] an entity has to fulfil the following criteria to be considered an AIF:

### *Number of investors*

The first criterion is that the AIF has to raise capital from a 'number of investors'. This condition is considered fulfilled as long as capital is not raised exclusively from a single investor and the offer is closed to further investors. Without a doubt, the business model described satisfies this definition since offers are directed to an audience that is basically unrestricted via the Internet. In contrast to the Undertakings for Collective Investments in Transferable Securities (UCITS) Directive,[8] a public offer is not a requirement. Consequently, a limited liability company can, in principle, constitute an AIF.[9]

### *Raising/pooling capital*

In the example provided, capital is raised from investors by selling computational power and is subsequently pooled. Therefore, the capital is pooled because the customer contributes the acquired computing power to the mining pool, that is, transfers it back to the mining pool for the sole purpose of mining. Capital in the sense of the AIFMD is not limited to the form of money (be it cash or book money). The term also encompasses all other benefits in kind.[10] This means that computing power can also be categorised as capital under the AIFMD as its value is assessable and it definitely constitutes a financial benefit.

To fully grasp this concept, the miner should be seen as a single node or large computer unit. The customer is involved in each attempt by the mining farm to mine a new block through the pooled use of their acquired computing power (pool mining). If a separate node were created for each customer (individual mining), there would be far too little computing power available to realistically be the first in the network to perform the proof of work. Therefore, it is de facto mandatory to pool the acquired computing power of the investors to make efficient and competitive mining possible in the first place.

### *Investment for the benefit of investors*

A pooled return[11] is generated using the pooled capital (computing power as an interim step) to mine crypto assets jointly for all investors in a single node (per crypto assets). The incentive created in the case of successful mining is transferred to the single mining node of the mining farm and subsequently distributed to the individual investors (proportionately to the computing power or capital provided).

As explained earlier, it would make no economic sense to offer investors the option to use their computing power for individual mining in their own separate node so that the individual investor would bear the risk of their individual mining process alone. Therefore, this choice is generally not offered. Consequently, the success or failure of the mining process is shared between the investors and is based on the success or failure of the mining pool as a whole (= pooled return).

### *Defined investment policy*

In the example provided, the investment policy is determined and fixed by the limitation that the pooled capital can be invested only for the purpose of mining crypto assets. This limitation corresponds to no. 20 para. (d) subpara. (i) of the Guidelines on Key Concepts of the AIFMD 'to invest in certain categories of assets, or conform to restrictions on asset allocation' as well as subpara. (ii) 'to pursue certain strategies'. The mining farm has an obligation to its investors to follow the investment policy, and the pooled capital (= computing power) has to be managed according to this investment policy to generate a pooled return for the investors.[12] We therefore come to the conclusion that the discretion of the operator of the mining farm in regard to investment strategy is restricted to the 'mining of crypto assets', fulfilling this criterion of the guidelines.

### *No day-to-day discretion or control*

Investors are generally not given 'day-to-day discretion or control over operational matters relating to the daily management of the undertakings assets'[13] as defined in the guidelines for the type of business model described in this paper. They usually have no power of decision regarding the day-to-day use of the computing power of the mining farm. Additionally, the individual investor's potential right to choose the coin/token that is mined with his computing power at any time, based on a predefined list of coins/tokens, should not be understood as 'direct and on-going power of decision over operational matters'. In this case each coin/token offered as a potential mining investment constitutes a separate AIF, which means that the choice offered to the investor would equal switching between AIFs and not the power of decision over the relevant operational matters. It should be noted, however, that in view of the complexity and diversity of business models any actual assessment has to take into account the specific merits of the case and can, therefore, only be made case by case.

### *No general commercial or industrial purpose*

An undertaking with the purpose of pursuing a business strategy that includes characteristics such as running a predominantly commercial activity involving the purchase, sale and/or exchange of goods or commodities and/or the supply of non-financial services, or an industrial activity involving the production of goods or construction of properties, or a combination thereof is not considered an AIF under the AIFMD, according to the guidelines.[14]

It is often argued that the main use of the raised and pooled capital lies in the construction or rental of a computer centre employing powerful hardware. It is also propounded that some miners even run their own power plants to cover their energy needs and reduce costs. Based on this, it is argued that the capital raised is used mainly to create computing capacity that constitutes a general commercial purpose[15] or an alternative production method. An accurate assessment, however, should take into account the specific economic purpose of the contract. For investors in the business model in question — as well as the operator of the mining farm — the essential point of the agreement is not the provision of computing power for use outside the mining farm (eg to run a web business) but the provision of the 'mining service' by the operator and, most importantly, the pooled return in the form of the incentive (the 'mined crypto assets'). The provision of operating resources is an included and subordinated activity of each AIFM. The actual business purpose agreed on by the investor and the operator of the mining farm is to invest capital with the purpose of generating a pooled return in the form of crypto assets. From the operator's point of view, purchasing and maintaining of mining hardware and software and related activities can be qualified as included and as being subordinated activities to the main business activity, which is the mining of crypto assets. As such they do not constitute a non-financial service that precludes the applicability of the AIFMD — in a comparable way to the setting up of servers for any other financial intermediary.

In contrast, mining in a payment network — for example, the Bitcoinnetwork — includes the verification of transactions and their actual execution (creation of a new block of the Blockchain by combining the transactions and subsequent transmission to the entire network). Processing payment transactions is considered a financial service. Consequently, mining should be considered a financial service as well. This qualification is also applied by the Austrian FMA in the respective FAQ regarding the Austrian AIFMG.[16]

In addition to this, the technical analysis of the 'mining process' reveals that mining cannot be considered an industrial activity, in particular, the production of goods. Divergent opinions on this topic seem to be based more on fundamental differences in the technical understanding of the subject matter than on legal argumentation. In this context the absence of a uniform terminology significantly hinders the legal analysis. Attempts to make complex virtual procedures comprehensible to the broad public by the use of simple terms such as 'mining' in the sense of 'extraction' or 'production', in the sense of 'computation' of units of crypto assets, distort the factual technical and economic realities and complicate the discourse on this subject. This can be illustrated by a technical analysis of the term 'mining'. In examining the code of BTC, it becomes obvious that mining cannot logically encompass the production of units of crypto assets: the computing power expended to generate the proof of work does not produce BTC. On the contrary, as an incentive, the BTC algorithm enables the miner to address a transaction to himself that contains BTC that are newly brought into circulation, which does not constitute a production process in the technical sense. It is worth mentioning that the miner receives transaction fees in the form of BTC that are already in circulation from the creators of the transactions that the miner processes in the block in the same transaction. It should also be noted that there are other consensus algorithms that perform the same basic function as proof of work, such as proof of stake, that do not use large amounts of computing power, but other mechanisms, such as the miner 'betting' an amount of crypto assets on his block being valid and potentially being penalised in case the block is rejected by the network, and still achieve the same results. This shows that proof of work is just one of the multiple comparable consensus mechanisms that are used to create trust in a trustless system and provide security for the system.[17] The massive use of computing power in proof of work-based Blockchains, therefore, has nothing to do with the generation of units of the crypto asset but is used to successfully perform the aforementioned tasks.[18]

### Results of the legal analysis

In our opinion, the specific business model analysed in this paper fulfils all the criteria for the application of the AIFMD and, therefore, constitutes an AIF. The manager of the AIF is thus subject to the regulatory regime of the AIFMD and transposing national laws. Again, it should be kept in mind that the assessment in this paper is only an illustrative example, whereas the concrete assessment of any actual business models must be conducted on a case-by-case basis.

The aforementioned qualification is not affected by the classification of the underlying crypto asset Bitcoin as an object of property rights, good or digital good. Unlike the mining of gold, where the primary and immediate objective is the physical extraction of gold and, at the same time, the value of the extracted gold is the reward for the effort expended to mine it, the Bitcoin miner performs a completely different service. The real purpose of Bitcoin mining is the service provided by the miner to the entire Bitcoin transaction network, as shown earlier. The fact remains that while Bitcoin are brought into circulation, this is an (incentive) ancillary effect. The newly circulated Bitcoin merely serve as a part of the incentive for the miner. Moreover, providing the proof of work that causes the main effort in the mining process does not generate the new Bitcoin. They are incorporated as a transaction in a separate step, as part of the new block.

The second part of the incentive consists of Bitcoin that are already in circulation and are designated as transaction fees by the creators of transactions. To illustrate this point it should be noted that the code of Bitcoin is so set up that the number of Bitcoin brought into circulation per block is set to decrease geometrically, with a 50 per cent reduction for every 210,000 blocks, or approximately four years.[19] The result is that the number of Bitcoin in existence is limited to slightly less than 21 million. Once this predefined number of coins has entered circulation, the incentive will transition entirely to the transaction fees and be completely inflation free.[20]

The frequently made comparison of 'mining' to the mining of gold[21], that is, the physical extraction of a precious metal does not adequately address the technical and commercial nature of Bitcoin 'mining' and should be abandoned.

## CONCLUSION

The purpose of the AIFMD is to cover all funds that are not regulated under the UCITS Directive.[22] In such cases, where all the criteria for the applicability of the AIFMD are satisfied, the investment offer falls within the scope of the AIFMD. This must be assessed on a case-by-case basis. Similarly, this also applies to crypto asset mining business models, meaning that they fall within the scope of the AIFMD on the basis of the merits of the individual case. The fact that high-risk products without any operative activity are covered by the AIFMD (which applies in the case of many current mining models) shows the effectiveness of the AIFMD and its purpose to protect consumers. Such models are often very complex and hard to understand for retail clients, both from a technical and from a financial point of view. Consequently, crypto asset mining business models should not be treated any differently from other fund-like business models outside the crypto space.

Depending on the national transposition of the AIFMD, the classification of these business models as an AIF may result in the prohibition of marketing units and shares of such AIFs to retail investors, as is in the case of Austria. Operators of such business models that are already active on the market and who would fall under the regulation of the AIFMD would be faced with registration or authorisation requirements and potential legal repercussions for operating an AIF without licence. Retail investors could also turn to offers in non-member states, which would lead to significant issues regarding the enforcement of national legislation based on the AIFMD. Regulatory arbitrage between member states due to differing transposing laws and potential future adaptations of the said laws is an additional concern.

As some EU member states (such as Austria) are more directly affected by the phenomenon resulting from the absence of any crypto-specific legislation in place (whereas, for example, Germany covers crypto assets in some of its capital markets law,[23] Austria does not), differing energy prices and country-specific characteristics of the market create more attractive conditions for crypto mining ventures. Owing to this difference in practical relevance, most national competent authorities within the EU have not needed to take a stance on the issue in question to date, unlike, for instance, the case of Initial Coin Offerings (ICOs), which is why the discourse at the European level is still in its infancy. Without hands on experience with such business models in day-to-day supervision, a detailed legal opinion forming process would, at this stage, require a disproportionate amount of effort on the part of national competent authorities (NCAs), which already have to manage their limited resources expediently to ensure that they are able to fulfil their responsibilities. This is particularly applicable in light of the fact that the external focus of such business models is on the provision and use of computing power. In this view the widespread use of legally undefined terms such as 'mining' or 'production' in the sense of 'computing of crypto assets' (even though technically incorrect[24]) can easily lead to the false conclusion that mining is a production process and is therefore not covered by capital markets laws such as the AIFMD. In addition, market stakeholders have an obvious interest in keeping their business models unregulated. In Austria, this has led to some publications[25] that have attacked the viewpoint proposed in this paper following the FMA's publication of an opinion to this effect[26] and the FMA having taken supervisory action[27] in accordance with its opinion. A uniform European opinion, as pressing as the issue may be in certain member states, still remains some way off.

## References

1. Nakamoto, S. (2008) 'Bitcoin: A peer-to-peer electronic cash system', available at: https://bitcoin.org/bitcoin.pdf (accessed 1st June, 2018).

2. Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010.
3. *Ibid*. ref. 1 above.
4. Bitcoin Austria Verein zur Förderung von Bitcoin in Österreich (2018), available at: https://bitcoin-austria.at/de/bitcoininfo/die-vorteile-von-bitcoin (accessed 2nd July, 2018).
5. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 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 Directives 2009/138/EC and 2013/36/EU.
6. Austrian Financial Market Authority (FMA). (2018) 'Frequently asked questions zur Anwendung des alternativen Investment-Fonds Manager Gesetz (AIFMG)', available at: https://www.fma.gv.at/investment-fonds-und-verwaltungsgesellschaften/aif-verwalter-alternativer-investmentfonds/ (accessed 1st June, 2018).
7. European Securities and Markets Authority. (2013) 'Final report on the Guidelines on key concepts of the AIFMD of 24 May 2013' (ESMA/2013/600).
8. 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.
9. Tollmann, C. in Dornseifer/Jesch et al. (2013), 'AIFM-RL' Art. 4 pt. 14 (2013).
10. *Ibid*., ref. 9 above, pt. 8.
11. *Ibid*., ref. 7 above, pp. 3 and 6.
12. *Ibid*., ref. 7 above, p. 7.
13. *Ibid*., ref. 7 above, pp. 4 and 6.
14. *Ibid*., ref. 7 above, pp. 3 and 6.
15. Gorzala, J./Hanzl, M.. (2018) 'Mining - Bergbau oder doch alternatives Investment in das Schürfen von Kryptowährungen', österreichisches Bankenarchiv 8/18, p. 565.
16. *Ibid*., ref. 6 above.
17. Witherspoon, Z. (2018) 'A Hichhiker's guide to consensus algorithms', available at: https://hackernoon.com/a-hitchhikers-guide-to-consensus-algorithms-d81aae3eb0e3 (accessed 1st September, 2018).
18. Gassebner, M. (2018) 'Apropos: Warum Mining kein digitaler Erzeugungsprozess sein kann!', ecolex 09/2018, p. 801.
19. Bitcoin Wiki. (2018) 'Controlled supply', available at: https://en.bitcoin.it/wiki/Controlled_supply (accessed 1st June, 2018).
20. *Ibid*. ref. 1 above.
21. *Ibid*. ref. 15 above, p. 560f.
22. Commission of the European Communities (2009), Proposal for a Directive of the European Parliament and of the Council on Alternative Investment Fund Managers and amending Directives 2004/39/EC and 2009/. . ./EC, available at: http://ec.europa.eu/internal_market/investment/docs/alternative_investments/fund_managers_proposal_en.pdf (accessed 1st June, 2018).
23. BaFIN. (2018) 'In accordance with BaFin's legally binding decision on units of account within the meaning of section 1 (11) sentence 1 of the KWG, Bitcoins are financial instruments', available at: https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node_en.html (accessed 1st September, 2018).
24. *Ibid*. ref. 1 above.
25. *Ibid*. ref. 15 above, p. 560f.
26. *Ibid*., ref. 6 above.
27. Austrian Financial Market Authority (FMA). (2018) 'FMA prohibits business model of INVIA GmbH in conjunction with cryptocurrency mining', available at: https://www.fma.gv.at/en/fma-prohibits-business-model-of-invia-gmbh-in-conjunction-with-cryptocurrency-mining/ (accessed 1st September, 2018).