FinTech

DeFiing Gravity

DYOR? We did it for you!

DeFi, stablecoins & crypto assets – an introduction

Decentralized Finance (DeFi) projects are flooding the blockchain platform *Ethereum*. Smart contracts have become a valuable tool for shaping the future of financial services. Stablecoins rise in popularity. Blockchain-based financial innovation is disrupting the traditional financial market.

At first glance, DeFi systems astonish us. At second glance, we find old concepts designed differently. This assessment is important when approaching DeFi from a legal perspective. Current laws apply in the absence of laws designed specifically to cover DeFi solutions.

We want to help your business succeed by providing help in two main areas: one of them is to provide information about the basic legal aspects that might be relevant in particular cases. Another is to inform our clients about risks: building and using DeFi systems means investing in something unknown.

On the following pages, we will introduce you to the answers to your most important questions:

What is a:

- crypto asset?
- crypto custody business and when is it subject to a permission requirement?
- stablecoin and does it qualify as e-money?
- DAO and is it a company in a legal sense?
- no-loss lottery and is it legal?
- MTF and is trading on-chain legal?
- flash loan (attack)?

Take the lead.
With Dentons.

What is a crypto asset?

Basics

On November 29, 2019, the German legislator adopted new rules on crypto assets. The new rules have been adopted as part of the implementation of Directive (EU) 2018/843 of May 30, 2018, (**5th AML Directive**). Rather than amending the German Anti-Money Laundering Act (*Geldwäschegesetz* (**GWG**)), the German legislator has decided to take a much broader approach. The new law contains, amongst other things, changes to the German Banking Act (*Kreditwesengesetz* (**KWG**)), which provide that crypto assets qualify as financial instruments in accordance with Section 1 para. 11 sentence 1 no. 10 KWG.

These German-drafted rules may be complemented or supplemented in the future if the EU decides to finalize legislation on crypto assets.

Definition(s)

Crypto assets are defined in Section 1 para. 11 sentence 4 KWG as

- digital representations of a value that
- were not issued or guaranteed by any central bank or public authority, and
- do not have the legal status of currency or money, but
- can be transmitted, stored and traded electronically
- by natural or legal persons on the basis of an
- agreement or actual practice,
- and are accepted as means of exchange or payment, or
- serve investment purposes.

The following are not regarded as crypto assets according to Section 1 para. 11 sentence 5 KWG

- electronic money within the meaning of Section 1 para. 2, third sentence, of the Payment Services Supervision Act (*Zahlungsdiensteaufsichtsgesetz* (**ZAG**)), or
- a monetary value that either
  - meets the requirements of Section 2 para. 1 no. 10 ZAG (payment systems in limited networks or with very limited product range and instruments for social or fiscal purposes) or
  - are only used for payment transactions under Section 2 para. 1 no. 11 ZAG (payment transactions in electronic communications networks/services).

The term “crypto assets” in Section 1 para. 11 sentence 1 no. 10 KWG is conceived as a catch-all provision, because the existing categories, that cover most types of crypto assets, are not sufficient to cover all conceivable applications of virtual currencies, as envisaged by Recital 10 of the 5th AML Directive.

According to Art. 3 no. 18 of the 5th AML Directive, virtual currencies are "a digital representation of a value that has not been issued or guaranteed by any central bank or public authority and is not necessarily linked to a currency defined by law and does not have the legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and can be transferred, stored and traded electronically".

According to the definitions set out above, the term “virtual currencies” is restricted to “means of exchange” and is in itself insufficient to cover all kinds of crypto values that are commonly referred to as tokens or coins.

What is a crypto custody business and when is it subject to a permission requirement?

Basics

Many market participants will not risk investing capital in crypto assets if the custody of their crypto investments is less secure than that of traditional assets.

Crypto custody business within the meaning of Section 1 para. 1a no. 6 KWG covers the safekeeping, management and saving of cryptographic values or private cryptographic keys used to hold, store or transfer cryptographic values. A permit according to Section 32 para. 1 sentence 1 KWG is necessary if the provider implements only one of those alternatives. There is no need to keep safe, manage and protect either crypto assets or cryptographic private keys at the same time.

Definition(s)

Safekeeping means the taking into custody as a service for third parties. This service could be offered by a so-called crypto exchange, which stores crypto assets for their customers in a collective wallet without the customers themselves having knowledge of the cryptographic keys used.

Management, in the broadest sense, means the ongoing management of the rights derived from the crypto asset.

Saving covers both the digital storage of the private cryptographic keys of third parties provided as a service and the storage of physical data carriers (e.g. a USB stick or a sheet of paper) on which such keys are stored. The offering of storage space, e.g. by web hosting or cloud storage providers, does not qualify as crypto custody business as long as the storage service is not offered explicitly for the storage of the private cryptographic keys.

Correspondingly, the mere development or distribution of hardware or software for securing the cryptographic values or the private cryptographic keys is excluded, if such a product is operated by the users on their own responsibility. However, this holds only as long as the providers do not have intended access to the cryptographic values or private cryptographic keys thus stored by the user.

Misunderstandings could arise from the fact that “access” to the private cryptographic key is necessary. A private key is called “private” because it has to be kept secret. Consequently, “access” cannot mean that the service provider has to know the secret. In order to trigger the permission requirement it is sufficient that the service provider has access to the private key in any form: whether hashed, encrypted, or as an element of the software itself.

What is a stablecoin and does it qualify as e-money?

Basics

A stablecoin is a token designed to minimize its fluctuation in value. Is a stablecoin stable? Well, it depends. The fact of being soft-pegged to a currency like USD or EUR does not imply a stablecoin is more secure. The risks involved are simply different.

Generally, stablecoins can be categorized into so-called centralized and decentralized stablecoins:

So-called centralized stablecoins are issued by a person or institution. Consequently, the stability of the respective stablecoins first of all depends on the stability of the issuer. The issuer has full control of the smart contract, the stablecoins and the collateral that is meant to back up the stablecoins. However, the issuer has no control of technical issues that might occur. The users also have no protection mechanism in place that keeps the issuer from misusing powers or prevents attackers from exploiting vulnerabilities.

On the contrary, decentralized stablecoins are not issued or controlled by a natural or legal person. A protocol controls the existence of decentralized stablecoins. However, this fact does not make decentralized stablecoins stable. Again, the risks are different – and diverse – when it comes to a DeFi stablecoin system: the creator of the protocol could have made a fundamental mistake. One smart contract of many interacting with each other could involve a technical problem, passing it on and on. The acceptance of the users could decrease or rise in the blink of an eye. Especially a high rise of acceptance could put the security of a blockchain network at risk.

Our approach

When market participants talk about stablecoins, they think about *Facebook*'s Libra: a future project that might never materialize. Nonetheless, there are many ongoing stablecoin projects at various stages of development illustrating the pros and cons of crypto financing.

Do such businesses need a permission? The smarter question is: which one?

In many cases, a stablecoin would likely be characterized as a crypto asset (i.e. a financial instrument). However, on a case-by-case basis, stablecoins could instead qualify as electronic money (e-money) as defined by Directive 2009/110/EU (**2nd European Electronic Money Directive** ("**EMD2"**)). Article 2 para. 2 of EMD2 defines "electronic money" as electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions (…) and which is accepted by a natural or legal person other than the electronic money issuer. As reported by the European Banking Authority (EBA) on January 9, 2019, national competent authorities have identified cases in which tokens satisfied the definition of "electronic money".

The EBA found that a significant amount of tokens do not fall under either financial instruments (i.e. crypto assets) or e-money and are thus out of the scope of EU financial services regulation. Therefore, issuers of stablecoins should be vigilant for future regulatory developments and regulators' statements.

What is a DAO and is it a company in a legal sense?

Basics

A DAO (Decentralized Autonomous Organization) operates on the "super computer" *Ethereum* blockchain and is thus merely a set of interacting smart contracts, i.e. a computer program consisting of several computer programs. Simply put, it is software.

This software has been designed by humans and is used by humans based on pre-set rules (set out in a protocol). The pre-set purpose of a DAO can be, for example, a crypto-lending platform. System governance and participation roles as well as obligations have to be defined and fulfilled in order to achieve the purpose.

The question is: does this make a DAO a German company in a legal sense? Well, it depends.

Our approach

A DAO itself has no corporate form. Software has no legal status. The question is, however, whether the users, as a result of jointly using the DAO based on the same pre-defined purpose, connect in a way that under certain circumstances can be understood as representing a business form under German law.

In Germany, there are two types of business forms: partnerships between humans (and corporations) and corporations. The incorporation of the latter business forms requires, amongst other things, the notarization of the articles of association and a registration in the commercial register. In contrast to a corporation, a DAO does not claim rights or obligations of its own. It is not supposed to act in the real world. There is no representative and no board that decides on behalf of the DAO. The users interact and work together in their respective roles, led by the same purpose set out in the DAO code – but they do not represent the DAO.

Having this in mind, it is conceivable that the users of a DAO – as a whole – make the simplest form of a German civil law partnership (*Gesellschaft bürgerlichen Rechts*, (**GbR**)). Whether the criteria of a GbR are met has to be analyzed on a case-by-case basis, as each DAO is programmed differently, with different goals.

Those criteria are:

- The cooperation is based on the conclusion of a contract (so-called articles of association, *Gesellschaftervertrag*),
- The pursuit of a common purpose (*Gemeinsamer Zweck*) and
- The obligation to contribute to the common purpose (*Zweckförderungspflicht*).

The code of the DAO ultimately determines the mode of operation of the DAO, the roles, possibilities and impossibilities, and thus also the mode of operation and orientation of the cooperating users. By joining the DAO-community having a certain purpose (e.g. operating a crypto-lending platform) and choosing a specific pre-set role, being willing to contribute to the community's purpose, they commit themselves to the DAO-code, i.e. the articles of association. This contract does not need a specific form. Contracting parties do not need to know each other by name. If they want to cooperate under certain rules, computer code is enough.

What is a no-loss lottery and is it legal?

Basics

Blockchain and smart contract business models are often not entirely new but rather old business ideas newly interpreted using technological innovations. An example of this phenomenon is the so-called no-loss lottery, which is automatically executed by smart contracts on the blockchain. No-loss lottery providers promise the participants the chance to win without risking their stakes.

No-loss lottery providers accept a predetermined crypto asset for which they issue a "ticket". Each ticket holder is entitled to take part in the upcoming draw immediately or after a certain time holding the ticket. The deposited crypto assets are lent to or via third parties in order to generate an economic return. The hereby-collected economic return represents the later raffled prize pool. At the end of each lottery cycle, all participants get back their stake and the winner receives the raffled return in addition to his stake.

Our approach

Contrary to the wording "lottery", no-loss lotteries are not subject to the provisions regarding gambling. The German definition of gambling, deriving from Section 184 German criminal code (*Strafgesetzbuch* (**StGB**)), requires the possibility of losing one's stake as part of the lottery concept. No-loss lotteries purposely do not fulfil this prerequisite and are thus not to be considered as gambling.

Another question regarding no-loss lotteries is whether the issued "tickets" qualify as securities. Such a ticket is a token. According to the German Federal Financial Supervisory Authority, the Bundesanstalt für Finanzdienstleistungsaufsicht (*BaFin*), a token qualifies as security if it is transferable, tradeable and shows significant similarity to a (traditional) security, for example by containing certain rights of the holder.

- Transferability means the ability to exchange the token without great difficulty. For example, ERC20/777-Token are standardized in order to transfer such tokens between wallets.
- Tradability requires an existing market for the tokens or that, at the very least, such a token market could be established.
- The similarity to a (traditional) security is not that easy to affirm. At least on the German capital market(s) there is no financial instrument that grants similar rights as the "tickets" issued by a no-loss lottery.

However, no-loss lotteries offered on a blockchain platform are the modern version of what in other parts of the world and known as premium or bonus bonds. These are lotteries based on zero-coupon (government) bonds, which qualify as securities under the applicable national laws. Thus, the issued "tickets" could qualify as securities and be subject to the relevant capital market regulations.

The question whether offering a no-loss lottery requires a permit or not can only be answered on a case-by-case-basis. Since the model of a no-loss lottery is new to the German market, one should take into consideration that the laws or regulator's practice might adapt soon.

What is a MTF and is on-chain trading legal?

Basics

A multilateral trading facility (MTF) brings together the interests of a large number of persons in buying and selling financial instruments within this system and according to specified rules in such a way as to result in a contract for the purchase of those financial instruments (Section 1 para. 1a no. 1b KWG).

The prerequisites of a MTF are as follows:

- a multilateral system is operated in which
- the interests in buying and selling financial instruments of
- a multitude of persons
- within the system and in accordance with established rules bundle in a way that leads to a contract for the purchase of these financial instruments.

At first glance, a blockchain-based DeFi trading platform for crypto assets, which qualify as financial instruments according to the new regulations as set out above, triggers the necessity of a permit. According to the lawmaker's understanding and regulator's practice, a trading platform in the technical sense is not required. Consequently, operating a fully automated MTF, i.e. a non-discretionary trading platform, needs a permit.

Our approach

A crypto MTF differs from a "classic" MTF. As long as the crypto assets to be traded do not qualify as securities, offering access to private traders does not qualify as a violation of law. However, the operator has to fulfil many requirements in order to obtain the permit. The details of the prerequisites are subject to a close case-by-case analysis, but can be outlined as follows:

- a proof of a certain minimum initial capital (€50,000 up to €730,000);
- an experienced and reliable management;
- a proper business organization, including, inter alia, a proper business plan, risk management as well as IT security.

What is a flash loan (attack)?

Flash loan

A flash loan is an innovative model of a zero-risk loan implemented using a smart contract. The “zero risk miracle” derives from the lack of need for collateral when taking out a loan, because the loan is paid back immediately. This is possible due to the use of smart contracts that allow for simultaneous buying and selling of assets in different markets, but which are also set to reverse the loan transaction if the payback fails.

Since loan and payback take place simultaneously, i.e. execution or failure of execution happen at the same time (or within the time span of one transaction), flash loans are referred to as “atomic”.

Flash loans are only possible in a blockchain, where transactions are being processed step-by-step, resulting in a freezing time during execution.

Flash loans involve no default risk for the lender and are therefore marketed as risk-free. However, they are not free of risk as the previous flash loan attacks have shown.

Flash loan attack

Imagine a flash loan worth €1 million in combination with a vulnerable smart contract. All an attacker has to do is to find a vulnerability. Due to the flash loan’s “atomicity”, its exploitation cannot be stopped.

Flash loan attacks, however, are not limited to manipulation of flash loan transactions; they can be executed in various arrangement options. For example, the attacker can use flash loan amounts as stakes for high-stake manipulation actions. The attacker does not have to put his or her own assets at stake.

Flash loans, therefore, have the potential to destabilize DeFi systems and, in the worst case, the blockchain network itself.

A sign of an unstable financing system

Flash loans are just another vulnerability of DeFi systems and could become a threat to blockchain networks. Consider the power of miners in proof-of-work-based blockchain networks, which are able to interfere with transactions, even rewrite confirmed blocks under certain circumstances.

However, proof-of-stake-based blockchain networks are subject to another security risk: the stakes necessary to maintain the network’s security could be triggered by conflicting incentives and used for high-profit lending instead. Knowing about this (human) conflict enables an attacker to manipulate stakeholders in order to gain control of the network with very low stakes.

Building a sustainable DeFi system will need a lot of time. We all know about the opportunities in DeFi systems. However, understanding the legal pitfalls and knowing about the financial and technical risks enables you to defy gravity, while protecting yourself and your business.

Shape the future.
With Dentons.

Key Contacts – Frankfurt

Robert Michels
Partner
D +49 69 45 00 12 399
E robert.michels@dentons.com

Oliver Dreher
Partner
D +49 69 45 00 12 320
E oliver.dreher@dentons.com

Michael Huertas
Partner
D +49 69 45 00 12 330
E michael.huertas@dentons.com

Clemens Maschke
Partner
D +49 69 45 00 12 208
E clemens.maschke@dentons.com

Holger Schelling
Partner
D +49 69 45 00 12 345
E holger.schelling@dentons.com

Claudia Otto
Counsel
D +49 69 45 00 12 392
E claudia.otto@dentons.com

Valeria Hoffmann
Senior Associate
D +49 69 45 00 12 390
E valeria.hoffmann@dentons.com

Heinrich Raisch
Associate
D +49 69 45 00 12 472
E heinrich.raisch@dentons.com

Key Contacts – Berlin

Thomas Schubert
Partner
D +49 30 26473 430
E thomas.schubert@dentons.com

Dr. Stefan Dittmer
Partner
D +49 30 26473 430
E stefan.dittmer@dentons.com

Key Contacts – Düsseldorf

Predrag Maksimovic
Partner
D +49 211 74074 271
E predrag.maksimovic@dentons.com

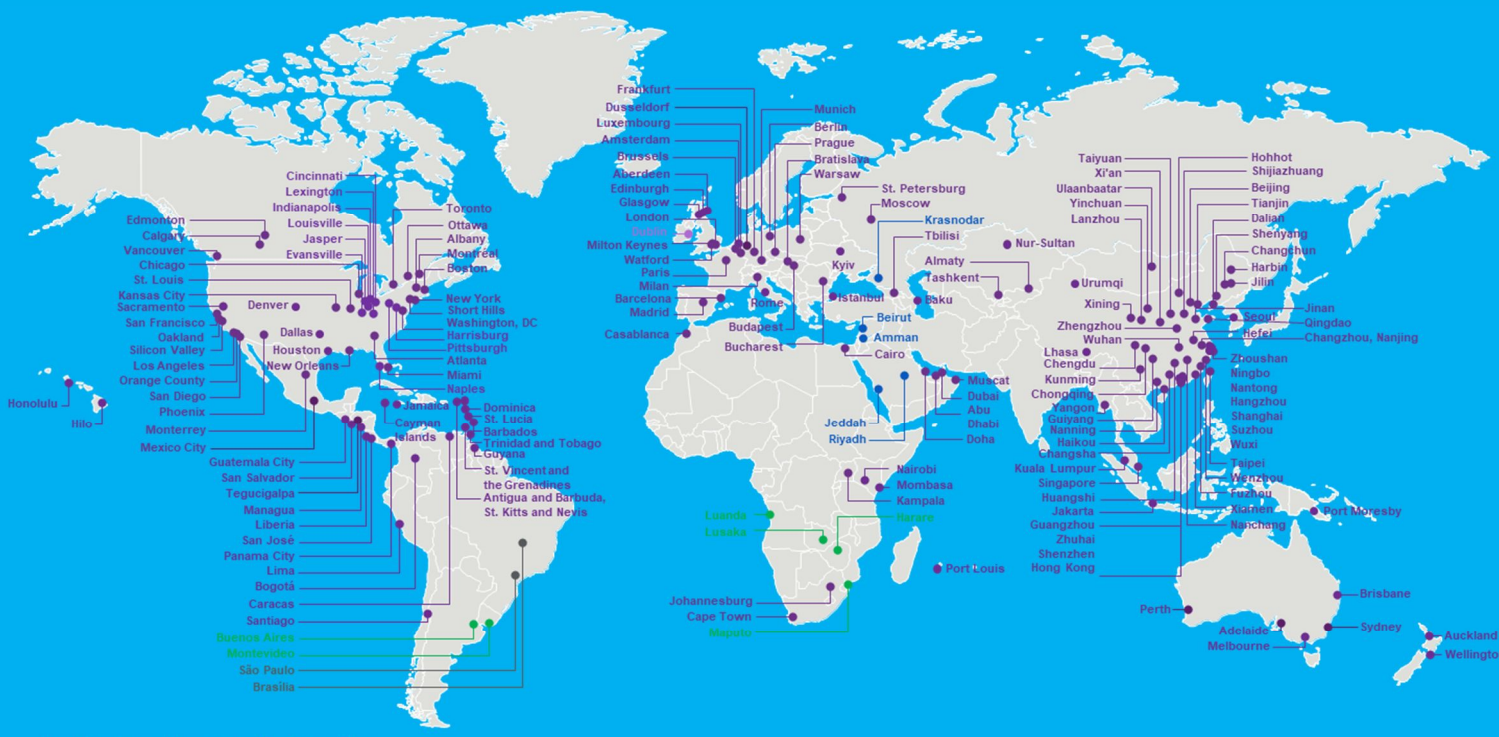
Frank Tepper-Sawicki
Partner
D +49 211 74074 272
E frank.tepper-sawicki@dentons.com

Key Contacts – München

Thomas Strassner
Partner
D +49 89 24 44 08 454
E thomas.strassner@dentons.com

Matthias Eggert
Partner
D +49 89 24 44 08 488
E matthias.eggert@dentons.com

Meet Dentons – the largest and only policentric law firm in the world



Locations in purple represent Dentons offices.
Office opening in 2020.
Locations in blue represent associate firms, offices and special alliances.
Locations in green represent proposed combinations that have not yet been formalized.
Locations in gray represent Brazil Strategic Alliance.

Polycentric – Leveraging our diversity for your competitive advantage

Looking forward to continuing the conversation or please do visit us on dentons.com