Background Paper

Crypto, Decentralized Finance, Web3, Smart Contracts, Digital Assets – An Overview

Most of the hype themes like crypto, blockchain, decentralized finance or DeFi, Web3, digital assets are completely different in their meanings but have one thing in common: independence by decentralization. In some cases, it means independence from finance establishment, from central banks, or big techs like Google, Amazon, Facebook or Apple. This paper provides an overview about the topic and shows what this all means for Anti-Financial Crime Compliance.

Definitions, meanings, and status quo of current public discussions:

- **Bitcoin.** The first crypto currency built on blockchain technology in 2009. Bitcoin is limited to 21 million coins. It is used more as an investment vehicle than as a real currency because of its volatility and unclear liability issues. The high energy consumption often directly associated with Bitcoin is a general blockchain problem rather than a specific Bitcoin problem. So far, different efficiencies are known for blockchains, with Bitcoin being very resource-intensive compared to others.
- **Blockchain.** A specific form of distributed ledger with a decentral public database consisting of data blocks stored on a high number of computers within the network. Each system within the network stores a copy of the transaction data. The more transactions that need to be stored the more blocks are needed in the blockchain. This is to provide stability and resilience, but also trust, as data manipulation is difficult and almost impossible the larger the network. Proof of the impossible was provided by "The DAO Hack" in 2016, in which fraudsters were able to steal 3.6 million Ether worth USD 60 million. To ensure investment security, the Ethereum blockchain was reset to the status before the hack. This procedure is called a fork. It means deciding which transactions on the blockchain are valid and which are not. Until now, the energy consumption of blockchains, which are needed to solve complex mathematical issues, has been problematic. This requires processing power and ultimately large amounts of energy. According to research by Alex de Vries[1], Bitcoin consumes as much energy in a year as all the world's data centres combined and creates the same carbon footprint as the entire city of London. The Cambridge Bitcoin Electricity Consumption Index (CBECI)[2] estimates an annual consumption of approx. 120 TWh (as per May 24, 2021) and a theoretical cap of 410.70 TWh. The volatility of energy consumption is caused by the number of new Bitcoins and new blocks on the Bitcoin blockchain. Modern blockchain implementations are working to avoid this high energy consumption. For example, EOS and Flow are more efficient than Bitcoin or Ethereum. Besides being used for decentralized finance (see DeFi) or crypto currencies (see Crypto Currency), blockchains are increasingly being used for other use cases, such as smart contracts, supply chain transparency or food compliance.

- **Crypto Currency.** A subset of digital currencies (see Digital Currency), often mixed with virtual currencies (see Virtual Currency) and based on blockchain technology. It is a cryptographic, algorithm-driven currency. It enables exchange between peers without any 3rd party like financial institutes. Based on the founding idea of crypto currencies, they are intended to function as an alternative to government-controlled central bank currencies. The concept of crypto currencies is based on strong cryptography to secure transaction records, create additional coins and transfer ownership of coins. That explains the origin of the name. Besides financial speculators, crypto currencies could be an alternative for the so-called unbanked population in poor economic situations, poor countries, or regions. It is a valid option for financial inclusion. Crypto wallets (see also Crypto Wallets) are easy to handle and easily available and crypto transactions, especially cross-border transactions, are quite inexpensive in relation to cross-border banking transactions. As in most regions with high usage rates, where users often do not have an ID card or passport, the anonymity of crypto currencies and the absence of traditional KYC processes is even conducive to its broad adoption. The best-known crypto currencies are Bitcoin (see Bitcoin), Ethereum, Tether, and Binance Coin. As nearly everyone can create an own crypto currency, there are approximately 8,500 crypto currencies existing.[3] Since crypto is all about anonymity, it is outside the control of any authority and free from censorship. It is used by whistle blowers and critics of totalitarian governments. Of course, this anonymity has also its dark side: darknet marketplaces, organized crime, financial crime. Another risk is the peer-to-peer network that enables bypassing of sanctions and frozen banking accounts of sanctioned parties.
- **Crypto Exchange or Digital Currency Exchange (DCE).** Exchange for crypto currencies. Crypto currencies can be traded via personal wallets. Like stock exchanges, DCEs are market makers and take a transaction commission for their services. Well-known exchanges are Binance, Coinbase or Kraken. DCEs are part of the FATF's definition of virtual asset service providers (VASPs).
- **Crypto Mining.** Creation of new coins by providing computing power for transaction execution and storage. Besides the hardware investment, mining is only interesting in regions with low energy prices due to the intensive energy consumption. See also Blockchain.
- **Crypto Staking.** By blocking coins in a proof-of-stake (PoS) blockchain, coins are paid as a form of interest. This practice is called staking. Persons who block their coins in a PoS are called "validators". Reason for this interest is the gain in stability and security of the blockchain and the crypto currency used. PoS rulesets differ from blockchain to blockchain in terms of minimum deposits, holding periods and validation mechanisms at PoS.
- **Crypto Wallet.** A personal account to buy, sell or exchange digital currencies. There are two types of wallets: Hot wallets connected with the internet and cold wallets, also known as hardware or paper wallets. Samples for hot wallets are wallets at crypto exchanges. As they are connected to the internet for trading purposes, a hot wallet is at risk of cyber-attacks. In 2014 the largest crypto exchange at this time, Mt. Gox, filed for bankruptcy protection as large amounts of bitcoins were stolen over a timeframe of three years. More secure are cold wallets which store the private keys offline on a hardware device. A less expensive alternative are paper wallets where the personal keys were printed on paper.
- **Decentralized Autonomous Organization (DAO).** An organisation based on the given rules of smart contracts and financed by issuing tokens (see also ICO). Current discussions revolve around the liability of a DOA or, more specifically, whether a DAO can be a separate legal entity.
- **Decentralized Finance (DeFi).** A system of financial applications, often referred to as decentralised applications (DApps), built on blockchain technologies. The system is built to avoid any central instances, 3rd parties or authorities. DApps also avoid a central platform approach by using blockchain technologies to distribute the application within the network. The core of DeFi is Ethereum. It is a programmable blockchain and is used for smart contracts (see Smart Contracts) and DApps.
- **Digital Asset.** The term is generally used to refer to any asset issued and/or transferred using distributed ledger or blockchain technology, including but not limited to virtual currencies, crypto currencies, coins and tokens. A particular digital asset may or may not meet the definition of a security under local securities laws.

- **Digital Currency.** In general, it subsumes all non-physical money/currencies. This includes virtual currencies (see Virtual Currency), crypto currencies (see Crypto Currency). As the money that is transferred from one account to another is fully digital, we are talking about digital currencies as well as Central Bank digital currencies (CBDC) which are currently under discussion (Digital EUR) or have already been introduced (Digital Yuan). Digital currencies are intangible, real currencies in a digital currency format that makes them convenient, fast, and seamless.
- **Digital Currency Provider (DCP).** Businesses that keep and administer accounts for their customers, but generally do not issue digital currencies. Customers can trade digital currencies via crypto exchanges who then transfer the digital currency into or out of the customer's DCP account.
- **Distributed Ledger Technology (DLT).** A distributed ledger is a database that exists across multiple peers. Records are only stored within the ledger when processing, validation and authentication was agreed between the parties involved. Those transactions get a timestamp and a cryptographic signature to ensure verification and full audit trail of all information stored in the respective record. Blockchains are based on distributed ledger technology. By that, a blockchain is just one type of a distributed ledger, a subset of it (see Blockchain) but a distributed ledger is not automatically a blockchain. DLT does not need to structure data in blocks nor does it need a proof of work and stake (PoW/PoS).
- **Fork.** Technically a fork is a change in the blockchain's protocol. A soft fork means a change that needs to be accepted by the majority of the network's hash power to be successful but is still backward compatible. A hard fork means a need for an update of the whole network and a break in backward compatibility. In the event of a hard fork, you see two different coins based on two different blockchains with typically two possible outcomes: one blockchain becomes dominant (e.g. Ethereum becomes dominant over Ethereum Classic after "The DAO Hack") or both blockchains are adopted (e.g. Bitcoin Cash and Bitcoin).
- **Fractional Ownership.** Distributed ownership rights through tokens.
- **Initial Coin Offering (ICO).** Means the initial issuing of own tokens to raise capital either in government issued currencies, crypto currencies, ownership shares, revenue/profit shares, or other rights. A token is often similar to a digital asset/share. Similarly used terms to ICO are token sales or token generating event (TGE). An ICO can happen in an unregulated crowd funding way or through regulated security token offerings (STOs) based on national security trading acts.
- **Meta-Blockchain.** See also Web3. A blockchain that is used to secure, connect and interoperate with other blockchains, so called parachains. This blockchain of blockchains from W3F is called Polkadot.
- **Non-Fungible Token (NFT).** Proof of authenticity of a digital asset. It is a smart contract based on blockchain that connects exact one digital asset, for example one JPG picture, with exact one crypto wallet/owner. Each NFT is unique. That separates NFTs from crypto currency tokens where the tokens are fungible. NFTs can also be used for digital ID cards, digital vaccination cards or other important documents to be stored in a blockchain.
- **Peer-to-Peer (P2P).** Decentralized network model that connects peers directly without a central server in between. This model was widely used by Napster in 1999, but its origins can be found in the Internet Society (ISOC) and its Requests for Comments (RFC) back in 1969.
- **Presidio Principles.** Ethical blockchain principles launched by the World Economic Forum to preserve and protect user rights.[4]
- **Smart Contract.** A digital contract in the form of an application built on a blockchain. First smart contracts were programmed based on the programmable Ethereum blockchain. A smart contract can act by its own application if certain conditions become true. Contracting parties are defined by tokens.
- **Stablecoins.** Some crypto currencies are closely tied to central bank currencies, such as the USD. This is intended to avoid strong price fluctuations, such as those seen with Bitcoins, and guarantee more price stability. Tether, for example, uses the USD as a 1:1 price anchor. Stablecoins are also used as income protection against high inflation. In some countries like Nigeria, Bolivia, Nepal, Morocco and Turkey, crypto currencies have been partially or completely banned.

- **Token.** The digital correspondence of physical assets. Tokenizing means the process to create a digital asset, typically for future economic usage. There is a variety of tokens available: equity tokens, asset tokens, currency tokens, and non-fungible tokens (NFTs).
- **Virtual Currency.** A subset of digital currencies (see Digital Currency). Virtual currencies are typically linked to a single platform, specific communities, specific individuals and/or facilities and their policies. Unlike digital currencies, virtual currencies are not universally accepted. A reward program might be a virtual currency, but it is only accepted within the specific community. Outside the community, the credit in this virtual currency is worth nothing.
- **Virtual Asset Entity (VAE).** It is an umbrella term for a range of businesses built on crypto currency transactions. Substitutional terms are digital asset entity or crypto asset entity. These VAEs may be financial institutions (e.g. virtual asset service providers, crypto exchange or digital currency exchange, crypto currency ATMs and others) or non-financial institutions (e.g. gambling sites or other entities).
- **Virtual Asset Service Provider (VASP).** As per FATF[5], a VASP is defined as a business that conducts one or more of the following actions on behalf of its clients:
  - exchange between virtual assets and fiat currencies,
  - exchange between one or more forms of virtual assets,
  - transfer of virtual assets,
  - safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets,
  - participating in and provision of financial services related to an issuer's offer and/or sales of a virtual asset.

  As per this, a VASP is defined by specific functions and process support and not by the specific type of the entities engaged or by the technology used to perform the services. This includes virtual asset service providers, crypto exchanges or digital currency exchanges, crypto currency ATMs, wallet custodians, hedge funds and even any other natural or legal person who performs services on behalf of a third party. This can also include decentralized exchanges (DEX), but also DApps (see DeFi) and thus also Smart Contracts (see Smart Contract).
- **Web3.** Our currently known internet is often referred to as Web2, while the distributed but static internet of the 1970s to 1990s is described as Web1. Web2 is directly linked to the platform economy. Web3 stands for a decentralized, grassroots internet built on blockchains and peer-to-peer models to provide data sovereignty for each individual including "social crypto" (social networks based on blockchains) like Bluesky, Diaspora or Mastodon. It can be seen as the counter-draft of the centralised platform approach. The Web3 Foundation (W3F)[6] is currently working on the basic infrastructure.

[1] See https://www.researchgate.net/publication/325188032_Bitcoin's_Growing_Energy_Problem
[2] See https://cbeci.org
[3] See t3n, issue 64, Q3/2021, p. 48
[4] See https://www.weforum.org/communities/presidio-principles
[5] See https://www.fatf-gafi.org/glossary/u-z/
[6] See https://web3.foundation

Dirk Findeisen
Managing Partner
dirk.findeisen@msg-compliance.com

Expert for Financial Crime Compliance | 20+ Years of Experience in Governance, Risk & Compliance (GRC), Data Management, Advanced Analytics, and Corporate Performance Management | Author, Speaker, Lecturer

Key Subjects:

- Anti-Money Laundering/Anti-Terrorist Financing
- Anti-Bribery & Corruption
- Fraud Prevention and Management
- KYC, CDD, ID Proofing & Corroboration
- Advanced Analytics, AI, Machine Learning

Industries:

- Financial Services
- Manufacturing
- Retail & Services
- Telecommunication