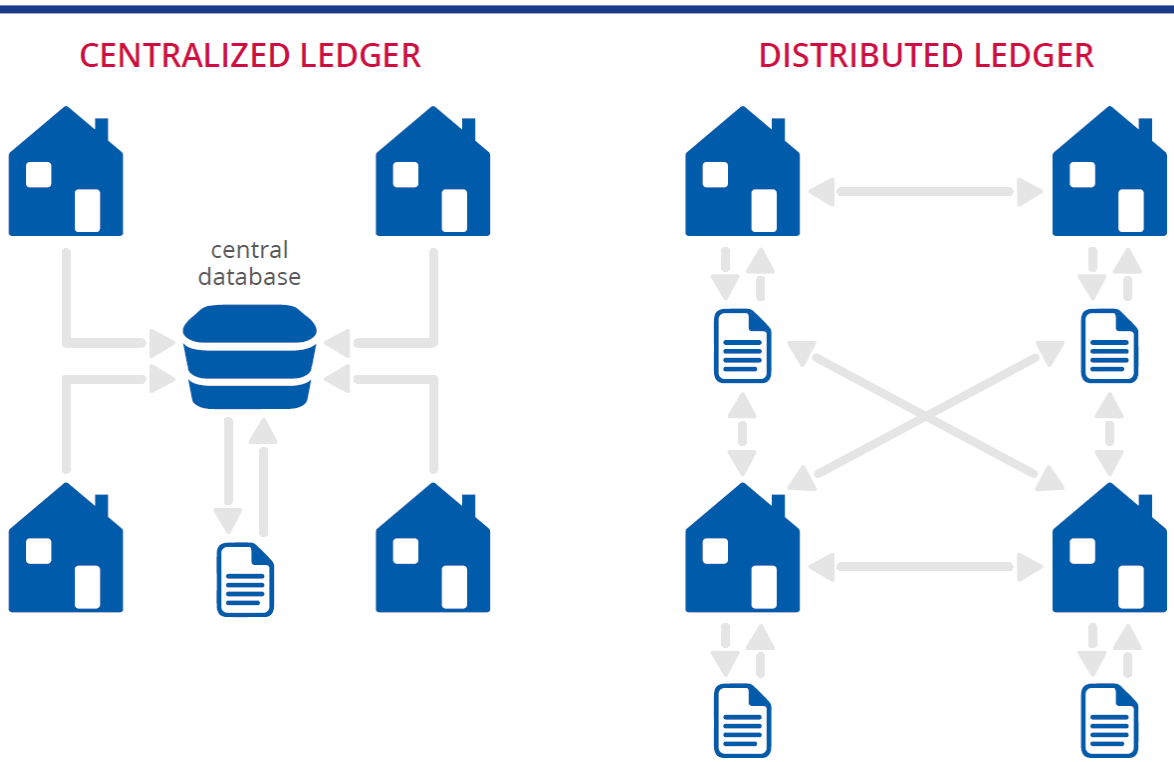

ENISA Opinion Paper on Cryptocurrencies in the EU

STATUS: FINAL

VERSION 1

SEPTEMBER 2017

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For media enquires about this paper, please use press@enisa.europa.eu.

Table of Contents

1. Introduction

As cryptocurrencies are increasingly employed for both legitimate and illicit purposes, there is a need for a debate on the cybersecurity concerns that may arise surrounding their use. A number of administrations are well advanced in their plans to authorise the use of cryptocurrencies[1]. For example, Japan has legalised the use of one cryptocurrency and the Philippines has granted cryptocurrency exchange licenses.

The main drivers for the adoption of cryptocurrencies, according to ENISA[2], include cost reductions, improved risk management, and automated regulatory compliance. The increasing use of cryptocurrencies may yield a number of benefits for citizens and industry. For instance, the decreased transaction and operational costs associated with cross-border transfer of funds could (optimistically) reduce the total global costs for remittances by up to EUR 20 billion[3].

However, with the growing use of cryptocurrencies, greater attention needs to be given to the cybersecurity associated with their use, as well as the regulatory aspects, in order to protect the users and society from illegal activities, including money laundering and terrorism financing. At present, ENISA understands that there is no EU law addressing cryptocurrencies specifically.

In this paper, ENISA presents its views on cryptocurrencies, summarising the technical aspects thereof, highlighting the key risks they may involve and discussing various potential regulatory approaches.

[1] Examples include the Philippines and Japan. See: Coindesk, *Philippines Central Bank Grants First Cryptocurrency Exchange Licenses,* August 21st 2017, and Cointelegraph, *Japan Financial Services Agency Claims that 50 Bitcoin Exchanges Filed for License*, August 23rd 2017.
[2] European Union Agency for Network and Information Security, p. 7, *Distributed Ledger Technology & Cybersecurity: Improving Information Security in the Financial Sector*, 2016.
[3] European Parliament, p. 3, *European Parliament Resolution of 26 May 2016 on Virtual Currencies*, 2016.

2. Defining "cryptocurrency"

An effective dialogue on cryptocurrencies requires as a first step developing a common taxonomy at EU level.

The Commission currently provides a working definition of virtual currencies as:

"a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically"[4].

This broad categorisation of virtual currencies can be further broken down into various subcategories. Virtual currencies can for instance be convertible, meaning they can be directly exchanged for "real" currency by virtual currency exchangers, or non-convertible, meaning they cannot be exchanged for real currency. Furthermore, virtual currencies can be centralised, meaning they have a single administrating authority, or decentralised. ENISA considers cryptocurrencies as a subset of virtual currencies that are used in a decentralised manner, using for example Blockchain technology.

A proposed definition for cryptocurrency is:

*"**Cryptocurrency** refers to a math-based, decentralised convertible virtual currency that is protected by cryptography.—i.e., it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy".*[5]

Though neither of these definitions are as of yet legally binding, they provide a framework for engaging with technical and policy-related issues surrounding cryptocurrencies from a cybersecurity perspective.

As with other fiat currencies, the value of cryptocurrencies is driven by supply and demand. Where the supply of a cryptocurrency is capped, and demand exceeds supply, the value of the cryptocurrency will rise. Presently, Bitcoin is a good example of this situation.[6] At the time of writing of this paper, 856 cryptocurrencies were in existence, with a total market capitalisation of close to 120 billion euros.[7] Many of the new cryptocurrencies are attempting to address existing inefficiencies, such as the number of transactions being processed per second and the use of smart contracts.[8] At the time of writing, approximately 3 billion euros of capital was being invested in cryptocurrencies per day.[9]

[4] European Commission, p. 21, *Proposal for amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing,* 2016.
[5] Financial Action Task Force, p. 5, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, 2014.
[6] For example, set at a total of 21 million for Bitcoins.
[7] For an overview of cryptocurrencies and their value, see: https://coinmarketcap.com/currencies/views/all/.
[8] Smart contracts are introduced in section 3.4.
[9] Supra note 7.

3. Cryptocurrency technologies explained

3.1 Distributed ledger technology (otherwise known as Blockchain)

The basic principle underlying Blockchain is that all participants share a consistent and distributed copy of the database as opposed to a traditional model, where databases are generally centrally stored. Transactions delivered on the Blockchain cannot be reversed or removed[10]. Network connections are made on a peer-to-peer basis and participants are obliged to comply with the ledger rules. A consensus protocol is also necessary to validate transactions. In normal transactions, one central party generally validates transactions (e.g. a clearing bank). In the consensus protocol, all users of the distributed ledger agree on the validity of the underlying data. Electronic digital signatures are used to sign the ledger entries and are the only way prove ownership of assets.

Forks may occur in cryptocurrencies when certain users deviate from the existing consensus protocol, creating split-off currencies. An example of the use of the fork was when the cryptocurrency Ethereum was subject to a hack11, and, to counteract the dubious transactions, a fork was created, allowing users to retain their assets. Some users decided to remain with the original cryptocurrency, which was renamed "Ethereum Classic". A more recent fork occurred in relation with Bitcoin when a new Bitcoin Cash occurred. A reason published for this fork was the need to have increased transaction speed and the delivery of more transactions per second.

3.2 Mining

The term "mining" refers to the validation of a pool of transactions by adding new blocks (transaction records) on the Blockchain. A block is a list of transactions to be approved by the network. The mining service can be provided by any person/entity with computer processing power. Miners deliver this process in line with a consensus protocol and are incentivised by receiving a financial reward for the provision of their services.

3.3 Cryptography

Distributed ledger technology may rely on the use of asymmetric cryptography (using pairs of public and private keys) and hashing algorithms to sign messages and/or encrypt data between users. Hashing refers to a process that irreversibly transforms a piece of data into a short and unique representation thereof.[12] The advantage of asymmetric cryptography is that it provides confidentiality, as well as authentication and integrity. The security associated with the ledger depends on the implementation of the ledger, and the consensus protocol.

[10] see ENISA Report on Distributed Ledger Technology & Cybersecurity, supra note 2 at p. 10.
[11] Ibid., p. 29
[12] European Union Agency for Network and Information Security, p.18, *Recommended cryptographic measures: Securing personal data,* September 20th, 2013.

3.4 Smart contracts

Smart contracts can be defined as, "*Contracts whose terms are recorded in a computer language instead of legal language*". Smart contracts have the advantage that they can be automatically executed by a computing system. For smart contracts to operate, the parties need to be able to observe each other's performance, and approve that the contract has been performed or not. The Blockchain technology allows for the parties to be verified to each other and that privity of contract will apply—i.e. while many people can see the results of the contract, only the parties to the contract can execute payments.

3.5 Permissioned/permissionless ledgers

In Blockchain technology, a distinction is made between permissionless and permissioned ledgers. The former are open to anyone, whereas participation in the latter is subject to rules determined by the members. Permissioned ledgers essentially operate as a "members' club", meaning that members can communally choose to add new parties, or remove existing ones. Permissionless ledgers allow for a high degree of decentralisation, making them more difficult to modify in a non-authorised manner, as copies of the ledger are available, whereas permissioned ledgers allow for a more controlled operational environment. Permissioned ledgers would most likely be favoured by financial institutions in order to leverage their real-world reputation in terms of control.

4. Key risks associated with cryptocurrency technologies

4.1 Key and wallet management

Private keys are the direct means of authorising activities from an account. As in the real world, unauthorised access to the private by malicious users can compromise the security of any wallets or assets secured by private keys. Protecting the private key is therefore an essential task. Significantly, malicious users can limitlessly keep trying to discover or reproduce a private key. With Blockchain, there is no way of knowing that hackers are attempting to discover or reproduce the private key until they have succeeded.

It may be difficult to detect that a malicious user has accessed a wallet; such access may allow an unauthorized user to store and transfer cryptocurrency or any other asset on the Blockchain. By the time detection has occurred, it may be too late as the reversal of the transaction will not be possible.[13]

4.2 Cryptography risks

Most Blockchain implementations rely on cryptographically generated public and private keys to operate. In relation to cryptography, it is vital that stringent key management policies and procedures are followed. These policies and procedures include people, processes, and technologies. As an example, risks exist when the software programmes used to generate keys are identified as weak, which has already occurred in some cases.[14]

4.3 Attacks on consensus protocol

The consensus protocol of certain cryptocurrencies may be vulnerable to what is known as a consensus hijack or, in relation to certain consensus protocol, a “51% attack”. The core concept of such an attack is that a malicious party may take control of sufficient computing power (more than 50% of the computing power of the entire network) to tamper with the validation process and could possibly trigger double spending attacks (i.e. the asset has already been spent). Recall that, since client profiles are not directly linked to personal identity, an individual or entity can produce a large number of accounts in a permissionless ledger.

4.4 Distributed Denial of Service (DDos)

DDoS attacks may occur when multiple participants on the network push large numbers of spam transactions to the cryptocurrency network, causing denial of services. Essentially the flood of incoming transactions causes the network to slow down or to stop. An example of DDoS occurred with Bitcoin in March 2016.[15] Due to the distributed nature of Blockhain technology, malicious programmes might be difficult to shut down.

[13] For further details, see ENISA Report on Distributed Ledger Technology & Cybersecurity, supra note 2.
[14] Coindesk, *Open-Source Tool Identifies Weak Bitcoin Wallet Signatures,* October 16th 2014.
[15] Supra note 2 at p. 17.

4.5 Smart contract management

The smart contract code automates the "if this happens, then do that" part of traditional contracts. This code is replicated on the distributed, decentralised Blockchain. As with any computer code, there is a risk of known and unknown vulnerabilities affecting the integrity of the code.

Since smart contracts substitute legal language with code, they entail a risk of faults associated with the code, which increases with the complexity of the contract. As the function and security of smart contracts code generally depends on the author's capabilities, there is a risk of human error. For example, several template contracts available on the web for the Ethereum scripting system may contain significant vulnerabilities.[16]

To minimise this risk, best practice techniques need to be deployed to oversee and review the behaviour of the code, and to take the appropriate action where improper behaviour is identified.

4.6 Illegal use

The criminal usage of cryptocurrencies is constantly increasing. In addition to the use of cryptocurrencies for criminal transactions such as purchasing illicit substances, cryptocurrencies can be used for money laundering and terrorism financing. Currently, cryptocurrencies are not covered by EU-level money laundering legislation. Evidence of terrorist groups using cryptocurrencies already exists, and increasing use of cryptocurrencies for money laundering and terrorism is expected in the near future.[17]

4.7 Privacy

Since all parties are able to download the ledger (i.e. a record of all transactions) and given the permanent nature of the record this could raise concerns, especially in the context of the upcoming entry into force of the GDPR[18], which requires personal data to be deleted after it is no longer necessary. This possibly goes against the nature of cryptocurrency design and illustrates the difficulty of legislation addressing technology challenges.

4.8 Addressing future challenges such as quantum computing

The security of algorithms and protocols used for the Blockchain is dependent on effective cryptography. New cryptanalytical challenges such as developments in quantum computing could have an adverse impact on the security and functionality of the Blockchain model.

It is considered that asymmetric keys, which are widely used across the internet today, may become vulnerable due to the computing power of quantum computers. A strategy to mitigate this risk would be to further invest in research on post-quantum algorithms and to develop an effective strategy for switching to such algorithms in a smooth fashion if and when quantum computing becomes widely available.

[16] According to: P. Vessenes, *Ethereum Contracts are Going to be Candy for Hackers,* May 18th 2016.
[17] Europol, p. 51 *Internet Organised Crime Threat Assessment,* 2016.
[18] General Data Protection Regulation.

5. Policy context of cryptocurrencies in the EU

Some of the main challenges associated with cryptocurrencies can be summarised as follows:

(1) Key generation and key management addressing their use, strength, storage, loss and theft;
(2) Privacy/encryption related challenges to provide lawful access to transactions;
(3) Code review of Blockchain applications to include Software Development Lifecycles and penetration testing;
(4) Smart contract management by monitoring the behaviour of contracts and mitigating the risk of vulnerable contracts.

Keeping these core elements in mind, the section below explains and elaborates on various aspects of the policy context of cryptocurrencies in the EU.

5.1 Anti-money laundering and countering the financing of terrorism

At present, there is no specific EU-level legislation addressing cryptocurrencies. However, at the time of writing, discussions are underway in the Council and European Parliament for an amendment to the Anti-Money Laundering (AML) Directive.[19] The proposed amendment would bring "virtual currencies", including cryptocurrencies, into the realm of existing AML and Countering the Financing of Terrorism (CFT) legislation. Specifically, virtual currency exchangers and "custodian wallet providers", defined as "an entity that provides services to safeguard private cryptographic keys on behalf of their customers, to holding, store and transfer virtual currencies",[20] would become obliged entities under the Directive.

ENISA is of the view that aspects of the operation of cryptocurrencies *can* be regulated, such as legislating for their use as legal tender and conversion with fiat currencies. ENISA welcomes the effort of the Union to bring forward legislation in this area. By addressing the legal uncertainty surrounding cryptocurrencies, the provision of legal certainty may also help to give confidence to users of cryptocurrencies. However, it is necessary to ensure that relevant safeguards are in place, particularly where security and privacy is concerned. ENISA stresses the need for a proportionate regulatory approach,[21] in order to avoid imposing an excessive burden that would undermine the advantages and flexibility that cryptocurrencies appear to offer at present.

5.2 Minimum requirements for resilient consensus attack

Given the experience to date of consensus hijacking, it is recommended to have in place minimum requirements (i.e. security requirements for consensus protocol[22]) to minimise the risk of attacks including hijacking[23]. These minimum requirements should result in reducing the incentive to hijack the consensus protocol.

[19] Supra note 2.
[20] Included in the latest Council negotiating mandate (19th December 2016) and the text adopted in Committee at the European Parliament (9th March 2017).
[21] As recommended in the European Parliament Resolution of 26 May 2016.
[22] ENISA is of the opinion that no minimum security requirements have been defined for the use of consensus protocols.
[23] This risk was experienced by one cryptocurrency and was labelled a 51% attack.

5.3 Supervision and licensing of cryptocurrencies exchanges

ENISA is of the opinion that financial regulators at Union and member state level should consider some level of supervision and licensing of the operation of cryptocurrency exchange points as appears to be happening in Asia. The level of supervision and licensing should be adequate so as to protect consumers. To protect the European ambition of a digital single market, ENISA recommends that solutions are applied across all member states at the same time to avoid competition between member states and different rules applying.

5.4 Smart contract research and development

Given the potential to use Blockchain technology to execute smart contracts, users need to have full confidence that the computer code generated is fit for purpose and has been certified by a trusted authority at a European level.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu