Why blockchain technology can be useful for the processing of digital evidence?

The ubiquitous nature of digital devices such as smartphones, laptops and the IoT, makes digital evidences extremely relevant for criminal investigations on all kinds of criminal behaviour, including contraband, human trafficking, child pornography and murder. The LOCARD's holistic platform aims to ensure the chain of custody through the forensic workflow, by storing digital evidence metadata in a blockchain. Blockchain technology, which has boomed worldwide over recent years, employs cryptographic and algorithmic methods to log and synchronise data across the network in an immutable way. In this sense, the use of a blockchain within the LOCARD platform endows trustworthiness, integrity, authenticity and transparency throughout the entire forensic workflow, i.e. from the collection of digital evidences, going through the processing of the stored data to realise incidents reporting, to the final prosecution in a court of law. The blockchain's properties prevent disputing the chain of custody of digital evidences during a judicial procedure, a common challenge for many law enforcement agencies and forensic laboratories in spite of properly documenting the entire forensic workflows.

The recently approved LOCARD's D4.3 deliverable (see **HERE**) provides an extensive review of the state of the art on blockchain technologies, some of them implemented in the LOCARD platform. Moreover, it also describes how these technologies will mature and may be relevant to the LOCARD's needs.

The document sets the foundation of the distributed ledger technologies in Section **5**, being blockchain a particular type of data structure used in some distributed ledgers. Often wrongly understood, it is worth noting that not all distributed ledgers necessarily use blockchain technology, and conversely, blockchain technology could be used in other contexts. In this sense, Section **5.1.** recalls why both technologies are commonly mingled and describes the main similarities and differences between distributed ledger technologies and blockchain technologies. Contextualising the fact that a blockchain-based distributed ledger technology is used in LOCARD, Section **5.2.** provides an accurate definition and description of the main properties and applications of blockchain. To ease the understanding of the functioning of a blockchain, practical examples such as cryptocurrencies, a widely exploited blockchain-oriented market, are provided (also extended in Section **5.5.**). As all technologies, blockchains are not a silver bullet, and several advantages and disadvantages are discussed in Section **5.3.** Among others, properties, such as decentralisation, auditability, immutability, privacy, efficiency, resilience, cost, and hack susceptibility, are enumerated. With the aim to clarify the structure of a blockchain, Section **5.4.** elaborates on the most basic elements in a

LOCARD project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement nº 832735.

blockchain: the blocks, thus describing the different parts within each block and how are they related to each other to create the chain. More technically, Section **5.6.** addresses the main key features of blockchains, e.g., the distributed nature of the ledger, the mechanism to reach consensus in a network regarding the validity of new data, and public-key cryptography used in digital signatures and hash functions.

The broad use of blockchain enabled the appearance of several types of blockchains: Section **5.7.** details the most common types, namely public (or permissionless) blockchains with no access restrictions, private (or permissioned) blockchains with certain access policies and roles, and hybrid (or federated) blockchains that combine several design features from both public and private blockchains. In short, whereas public blockchains have a good security level, they lack speed and efficiency in crowded networks. On the other hand, private blockchains are faster and scalable solutions, although they are not fully decentralised. Federated blockchains overcome the shortcomings of the aforementioned blockchains, enabling more speed, scalability, lower transaction costs, lower energy consumption and more protection against certain attacks, to name a few. To compare several blockchains, Section **5.8.** focuses on four well-known blockchains, namely Ripple, Hyperledger Fabric, R3 Corda and Quorum. As blockchain technology is still evolving, Section **5.9.** presents several challenges that must be faced: including technological challenges (e.g., lack of maturity, scalability, transaction speed, interoperability, integration, cybersecurity, governance, and chain forking), legal and regulatory challenges (e.g., regulatory vetting, industry standards, legal clarity over ownership and jurisdiction, the Know-Your-Customer and Customer-Due-Diligence requirements in financial systems, and resource mechanisms), and other challenges such as privacy and environmental costs.

Blockchains have a huge potential in a wide variety of industries. Besides the financial purpose, the most popular through cryptocurrencies, Section **5.10.** enumerates numerous applications that can benefit from blockchain technology, such as the storage of electronic medical records within healthcare domains, the management of the supply chains in logistics, electronic voting systems and identity management systems. For the latter, Section **5.11.** describes how blockchain identity management could explore a self-sovereign identity management model, which enhances security and privacy levels. Smart contracts, another common buzzword, and their relationship with blockchains and distributed ledger technologies are explained in Section **5.12.**

Finally, Section **6** discusses the future of distributed ledger technologies as one of the most promising technologies to be applicable into many sectors. However, as already mentioned, the technology has to evolve to overcome current technological limitations, such as interoperability, scalability, and privacy, and to be a complete mature solution. Some of these limitations are to be researched during the execution of the LOCARD project (Section **7**) with a focus on the specific requirements for the LOCARD's blockchain (Section **8**).