The Case of Diem
A Distributed Ledger Technology-based Alternative Financial Infrastructure Built by a Centralised Multisided Platform

by **Golnaz A. Jafari and Malte-C. Gruber***

Abstract: In pursuing its declared mission "to enable a simple global currency and financial infrastructure with a safe, secure and compliant payment system that empowers billions of people," Diem has encountered apparent resistance from various social fields and politics. On the one hand, many critics recognise dangers to state currency sovereignty and the stability of the financial system; on the other hand, they fear negative developments regarding money laundering and the financing of terrorism. In addition, there are considerable concerns about an ever deeper erosion of privacy, consumer and data protection, which reaches a new dimension by linking such world currencies with already existing social networks governed and controlled by private entities. Under these circumstances, the chance of success of the Diem project clearly depends on the extent to which the aforementioned concerns can be dispelled and whether public trust can be established. Together with an overview of the developments of the Diem project since the inception of the underlying idea, the authors highlight the actors and their respective roles in an infrastructure primarily run and operated on distributed ledger technology (DLT), with computer nodes distributed across different jurisdictions. Moreover, it is argued that the level of control by end users over their digital representations and online footprints remains untested in the context of a worldwide digital financial infrastructure as proposed by Diem. The paper further elaborates and puts data protection and privacy of end users under scrutiny, outlining the need for a self-sovereign identity (SSI) management system in order to address the risks associated with correlation and profiling of individuals concerning their behaviour in payment systems.

Keywords: Libra; Diem; Facebook; Distributed Ledger Technology; DLT; blockchain; network governance; trust; digital identity; self-sovereign identity; SSI; central bank digital currency; CBDCs; crypto-assets

Recommended citation: Golnaz A. Jafari and Malte-C. Gruber, The Case of Diem: A Distributed Ledger Technology-based Alternative Financial Infrastructure Built by a Centralised Multisided Platform, 12 (2021) JIPITEC 301 para 1

A. Introduction

1 In order to achieve its set objective to design a location-independent alternative worldwide system for digital finance, Diem is set to be built on distributed ledger technology (DLT), and was initially structured to be governed by a Swiss based member association, the Diem[1] Association, and its subsidiary and primary operating entity Diem Networks. Diem Net-

* Golnaz A. Jafari, LL.M., is a doctoral researcher at Lucernaiuris, University of Lucerne, Switzerland, formerly a research associate at SOCAI, University of Würzburg, Germany & a research fellow at NRCCL, University of Oslo, Norway; Malte-C Gruber, Dr. iur., is a Professor of Legal Philosophy and Commercial Law with a focus on Intellectual Property Law and the Law of New Technologies at Lucernaiuris, University of Lucerne, Switzerland. The views and opinions expressed in this article remain those of the authors. Authors specifically thank Josephine Heinzelmann, and in particular, Dr. Steven Howe of Lucernaiuris as well as Pieter v Ysseldijk for their insightful comments.

works was designed to take the role of a regulated payment systems operator, activation of which required a payment systems licence from the Swiss Financial Market Supervisory Authority (FINMA). As of May 2021, the FINMA application for a payment systems licence has reportedly[2] been withdrawn in an attempt to limit the jurisdictional scope of the project to the United States of America (USA), at least during the initial phase. Nevertheless, both entities seem to currently hold active status on the Swiss commercial registries.

2 Against this background, one would also need to consider the possibility of central banks introducing central bank digital currencies (CBDCs). Once operational, Diem could presumably have an impact on the worldwide financial sector and further popularise the inception of CBDCs, most probably in a form consisting of public-private partnerships.

3 The paper will first provide an overview of the organisational structure of the Diem project as well as its technical typology in an attempt to define main actors and stakeholders, respectively to distinguish between the two phases of the project, namely Libra 1.0 and Libra 2.0, now known as Diem. In the subsequent section, attention is given to the definition of the fundamental legal nature of the Diem design, which took a two-fold form. The two-fold design model consisted of single fiat currency stablecoins and an intra-network Diem crypto token acting as a "digital composite" for some of the network's stablecoins. The digital composite would then be backed by a basket of fiat currencies and other assets. As for the project's initial phase, and with a primary focus to comply with the US regulatory landscape, Diem is set to take off in the form of a single US dollar -backed token.

4 Trust as the elementary fact of social life and, more specifically, as the central factor in the context of money creation as well as financial services, is addressed in the following section. Trust in the functioning of a given system would bear a direct link with the transparency of the system's governance. Here, the authors argue that Diem's chances for mass adoption would depend in particular on its prospects of gaining trust as a new and alternative digital form of *private* currency alongside the established monetary systems. This would require a number of constituents, such as comprehensive accessibility and trustworthiness based on legal certainty, clear attributions of responsibility, appropriate models of liability, and effective legal mechanisms of enforceability.

5 Trust and transparency are closely linked with consumer protection as well as compliance with end users' privacy and personal data protection. Identity management is therefore pivotal. In the final section of this paper, the authors argue that as it stands, despite minimal information being publicly available, Diem's identity management system would fail to give end users an effective control over their digital representation on its network. The paper concludes by highlighting the significance of recent technological developments in the digital identity sphere, whereby a standardised and interoperable self-sovereign identity (SSI) management could be a way forward in such network infrastructure.

B. The Case of Diem

I. Organisational Structure in a Nutshell

6 Initially branded as Libra 1.0, the project was incepted in June 2019[3] by the social network platform Facebook in an attempt to provide cross-border financial services enabled through the means of technologies such as distributed ledger technology (DLT).[4]

7 Headquartered[5] in Geneva, Switzerland, the Diem Association, previously known as the Libra Association, was formed in July 2019 as a non-profit (independent) membership association to be responsible for the development and governance

1 Announced by Libra Association, the name of the project has been changed from 'Libra' to 'Diem' in an attempt "to reinforce organisational independence"(1 December 2020) <https://www.diem.com/en-us/updates/diem-association/>; notably the name change has triggered the possibility for a legal action by a London based fintech company which operates finance application software also named Diem < https://cointelegraph.com/news/carpe-diem-lawsuit-threatened-over-facebook-s-libra-rebrand-plan>.

2 FINMA, 'Diem withdraws licence application in Switzerland' (12 May 2021) <https://www.finma.ch/en/news/2021/05/20210512-mm-diem/>.

3 Libra Engineering Team, 'Libra: The path forward' (18 June 2019) <https://www.diem.com/en-us/blog/the-path-forward/>.

4 The terms 'blockchain' and 'DLT' are often used interchangeably. The authors take the view that blockchain could be considered a subcategory of DLT, whereby entries to ledger (or chain) are primarily bundled in the form of blocks.

5 See entity registration in the commercial registry of the canton of Geneva (31 July 2019) <https://www.shab.ch/api/v1/publications/5626ee28-a9a2-4193-b05b-e5dc0679f155/pdf>.

of the project. Members of the association,[6] mostly businesses and enterprises, were set to be represented by one representative per entity with a right to one vote. These representatives would participate in the governance and key decision making areas of the project, develop its long-term strategy, and respectively validate all the transactions on the Diem network. The day to day management of the Diem Association would be carried out by its designated board of directors, with the association's operational leadership remaining in the hands of an appointed executive team.

8 As a subsidiary to Diem Association, Diem Networks,[7] previously known as Libra Networks, was registered in the form of a limited liability company (LLC)[8] by Facebook in Geneva in May 2019.[9] Initially a stakeholder of Diem Networks, Facebook Global Holdings II LLC later transferred its shares to the Diem Association in October 2019.[10] Diem Networks was founded to become a financial technology (fintech) entity, for the pursuit of a number of objectives. These include the development and production of software and infrastructure, particularly in line with investment activities, payment operations, financing, identity management, data analytics, big data, blockchain and other technologies. With the recent withdrawal from the FINMA application for a payment systems licence[11] which was submitted on the legal basis of the Swiss Financial Market Infrastructure Act (FMIA), the sister subsidiary Diem Networks US, Inc.[12] has recently been registered as money services business (MSB) administered by the Financial Crimes Enforcement Network (FinCEN) under the Bank Secrecy Act (BSA). Diem Networks US, Inc., wholly owned by Diem Association, has recently partnered with Silvergate Capital Corporation[13] whereby latter is set to be the exclusive issuer of Diem's single US dollar-backed token and the manager of the associated reserve.

9 Given the significant user base, global reach and network effect of Facebook and its associated group of entities, such as Instagram, WhatsApp and Messenger, with over a quarter of the world's population at its disposal,[14] the Diem project has, since its inception, been subject to extensive regulatory scrutiny from various jurisdictions including, but not limited to, the USA,[15] the European Union (EU)[16] and Switzerland. The project's potential effect on

6 See <https://www.diem.com/en-us/association/>; the membership profile of the association has changed since its inception in June 2019 with companies such as Visa, Mastercard, Paypal and eBay, among others, eventually opting out of the project.

7 See name change update in the commercial registry of the canton of Geneva (8 December 2020) <https://www.shab.ch/shabforms/servlet/Search?EID=7&DOCID=1005042618>.

8 LLC equals Société à responsabilité limitée (SARL) and Gesellschaft mit beschränkter Haftung (GmbH) in Swiss company law.

9 See entity registration in the commercial registry of the canton of Geneva (2 May 2019) <https://www.shab.ch/shabforms/servlet/Search?EID=7&DOCID=1004624965>.

10 See stakeholder update in the commercial registry of the canton of Geneva (21 October 2019) <https://www.shab.ch/shabforms/servlet/Search?EID=7&DOCID=1004742062>. Note: The shares have later been transferred from Diem Association to Diem GmbH, a new entity in Lucerne (01.02.2021) <https://www.zefix.admin.ch/de/search/entity/list/firm/1391882>.

11 FINMA, 'Libra Association: FINMA licensing process initiated' (16 April 2020) <https://www.finma.ch/en/news/2020/04/20200416-mm-libra/>. See n 2.

12 Diem Networks US, Inc. is incorporated in Washington (16 September 2020) <https://opencorporates.com/companies/us_va/11109939>.

13 On 12 May 2021 Diem announced its withdrawal from the ongoing FINMA application for a payment systems licence, bringing the project during its initial phase into the US regulatory perimeter. Diem Association's subsidiary and primary operating entity Diem Networks US has now partnered with Silvergate, a California based state-chartered bank, in a plan to first issue its US dollar-backed tokens. Diem's US dollar-backed tokens and the associated reserve is set to be exclusively issued and managed by Silvergate. <https://www.diem.com/en-us/updates/diem-silvergate-partnership/>. Note: no Diem tokens have been issued as of October 2021.

14 See Statista, 'Cumulative number of monthly Facebook product users as of 3rd quarter 2020' (4 November 2020) <https://www.statista.com/statistics/947869/facebook-product-mau/>; during the last reported quarter, Facebook stated that 3.21 billion people were using at least one of the company's core products.

15 'Facebook's Zuckerburg grilled by Congress on Libra – as it happened' (*Financial Times,* 23 October 2019) <https://www.ft.com/content/bf16f8ec-6897-38be-9ff4-0f40cc4c779d>.

16 European Council, 'Joint statement by the Council and the Commission on "stablecoins"' (5 December 2019) <https://www.consilium.europa.eu/en/press/press-releases/2019/12/05/joint-statement-by-the-council-and-the-commission-on-stablecoins/#>; "when an initiative has the potential to reach a global scale, the concerns are likely to be amplified and new potential risks to monetary sovereignty, monetary policy, the safety and efficiency of payment systems and financial stability can rise."

worldwide financial stability and state sovereignty in the control of money creation are placed at the centre of public discourse.[17]

10 Money[18] is seen as a *public good* that is built on *public trust* in order to carry out its socioeconomic functions. In this context, a distinction would need to be made between *account-based* and *token-based*[19] forms,[20] on the basis of their respective identification and verification requirements. The account-based form relies on the identification of the payer's identity, i.e. bank deposits. The token-based form depends on the verification of authenticity of the object that is being exchanged, i.e. physical cash, respectively cryptographically generated payment token models.

11 In this regard, the European Central Bank (ECB) made a reference[21] to Diem as an infrastructure for the creation of stateless money by conglomerates of corporate entities, with potential conflict of interests, whereby the entities would only be accountable to their respective stakeholders and members. Here, control over the distribution network would arguably be maintained by these entities "acting as quasi-sovereign issuers of currency,"[22] which would then exercise privileged access to user private data for, among others, monetisation purposes.[23]

12 As has been pointed out,[24] the technical protocol of Diem has made extensive references to the term 'account'[25], mostly leaving out the term 'token'. On the Diem network, the object to be exchanged would then take the form of a payment instruction that would need to be authenticated and processed in accordance with the applicable rules of the network. In this case, identity verification may not be necessary in order to process transactions. Nevertheless, as will be discussed in subsequent sections, the Diem network is set to put in place a strict identity verification procedure through its in-house digital wallet application. As a result, classification of the *private* currency designed by Diem as either account-based, or token-based, seems not to be a straightforward task.

13 Moreover, the concerns raised are arguably not immaterial, given, not least because of Facebook's business model as a for-profit multisided platform. This model enables the company to effectively govern the interactions among participants in its network, namely users, developers and marketers.[26] Here, users utilise the platform free of charge in return for their metadata which can contain behavioural information. This metadata is then used by Facebook for the generation of analytics, on the basis of which marketers place advertisements. On the other hand, developers are charged by Facebook in order to integrate and monetise their application software on its platform. Facebook therefore largely depends on its user volume and advertising revenue[27] for maintaining its operations.

17 ECB, 'Money and private currencies: reflections on Libra' speech by Yves Mersch (2 September 2019) <https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190902~aedded9219.en.html>.

18 In economic theory, a functional definition of money would consist of three elements of a) a unit of account, b) a means of payment (exchange), and c) a store of value. Money can either be physical (cash) or non-physical (scriptural or electronic).

19 See section C.1 for further details.

20 MK Brunnermeier et al., 'The Digitalisation of Money' (2019) NBER Working Paper Series nr. 26300, 4f.; CM Kahn et al., 'Should the central bank issue e-money?' (October 2018), 8-11 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3271654>.

21 ECB, 'Money and private currencies' (n 17).

22 Ibid.

23 V Khan & G Goodell, 'Libra: Is it really about money?' (August 2019) <https://arxiv.org/ftp/arxiv/papers/1908/1908.07474.pdf>.

24 D Jackson, 'Global 'stablecoin' Challenges: Response to FSB Consultation Document' (12 July 2020), 3f. <https://www.fsb.org/wp-content/uploads/Dr.-Douglas-Jackson.pdf>.

25 'The Libra Blockchain' (23 July 2019), 15f < The Libra Blockchain>; "at the logical level, an account is a collection of resources and modules stored under the account address. At the physical level, an account is treated as an ordered map of access paths to byte array values. An access path is a delimited string similar to a path in a file system."

26 A Hagiu & J Wright, 'Multisided Platforms' (2015) Working Paper, Harvard Business School; notably, multisided platforms are distinguished from vertically integrated platforms in that the former do not exercise control over interactions but rather govern them; in 5, two features seen inherent in multisided platforms are "a) they enable direct interaction between two or more distinct sides & b) each side is affiliated with the platform."

27 S Ghosh, 'Understanding Multi-sided Platforms: Social Networks and more' (12 October 2015) <https://samghoshblog.wordpress.com/2015/10/12/understanding-multi-sided-platforms-social-networks-and-more/>.

14 By venturing into financial services, Facebook's potential expansion of access to users' financial and behavioural data in payment services would arguably aggregate the existing risks associated with the correlation of users' profiles to a wide range of their activities spanning from social networks to spending patterns and monetary transaction records.[28]

15 In light of Facebook's demonstrated pattern of failing to keep consumer data private,[29] risks associated with user data privacy in the context of the proposed Diem project have been subject to numerous Congress hearings[30] in the USA, primarily by the House Financial Services Committee.

16 In order to tone down the ongoing discussions, Facebook shifted away from Libra 1.0 and rolled out Libra 2.0,[31] now named Diem, with an updated whitepaper[32] on technical and organisational matters published in April 2020. The downgraded version of the project was initially expected to launch by January 2021,[33] pending an affirmative outcome of its licence application with FINMA. With the recent shift from its FINMA application for a payment systems licence in Switzerland to the MSB licence registry with FinCEN in the USA, the project's initial phase is yet to materialise as of the date of this writing.

17 Nevertheless, during the latest G7[34] (virtual) roundtable among finance ministers of participating states, central bank governors, the European Commission and the Eurogroup, hosted by the Treasury Secretary of the USA, the need for an effective regulatory landscape prior to inception of any such project was reiterated. Notably, the German representative[35] took the view that merely rebranding Libra would certainly not render sufficient the project's admissibility within the German as well as the EU markets.

18 In this context, Facebook's intention to expand its scope of activities to financial services worldwide is not restricted to its Diem project. It has recently launched[36] an electronic payments system for fiat currency[37] transfers via one of its core products, WhatsApp. The initiative is set to initially target the Brazilian market and is enabled through Facebook's in-house software application, Facebook Pay. The distinction between Diem and WhatsApp's electronic payments system rests on the nature of the particular currency in circulation. The former is built based on a cryptographically generated *private* currency model (otherwise known as cryptocurrency), whereas the latter integrates payments based on digital representation of underlying fiat currency that is both *public* and *private* money.

19 More importantly, Facebook's subsidiary Calibra was founded in June 2019[38] with the aim of providing in-house financial services, including digital wallet services, to the Diem network. Later rebranded as

28 See also DA Zetzsche, RP Buckley & DW Arner, 'Regulating Libra: the Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses' (2019), UNSW Law, 15f.

29 US House Committee on Financial Services, 'Waters Statement on Facebook's Cryptocurrency Announcement' Press Release (18 June 2019) <https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=403943>.

30 See S Hrg. 116-71, 'Examining Facebook's proposed digital currency and data privacy considerations' (16 July 2019) <https://www.congress.gov/event/116th-congress/senate-event/LC64460/text?s=1&r=2>.

31 Libra Association, 'Libra developers: The path forward' (16 April 2020) <https://www.diem.com/en-us/blog/libra-developers-the-path-forward/>.

32 Libra whitepaper v2.0, 'Cover Letter' (April 2020) <https://wp.diem.com/en-US/wp-content/uploads/sites/23/2020/04/Libra_WhitePaperV2_April2020.pdf>.

33 'Facebook's Libra currency to launch next year in limited format' (*Financial Times,* 27 November 2020) <https://www.ft.com/content/cfe4ca11-139a-4d4e-8a65-b3be3a0166be>.

34 US Department of the Treasury, 'Readout from a Treasury Spokesperson on Secretary Mnuchin's Discussion with G7 Finance Ministers and Central Bank Governors' Press Release (7 December 2020) <https://home.treasury.gov/news/press-releases/sm1203>.

35 'Facebook's renamed cryptocurrency is still 'wolf in sheep's clothing': German Finance Minister' (*Reuters,* 7 December 2020) <https://www.reuters.com/article/g7-digitial-facebook/facebooks-renamed-cryptocurrency-is-still-wolf-in-sheeps-clothing-german-finance-minister-idUSKBN-28H20B>.

36 WhatsApp Blog, 'Bringing payments to WhatsApp for people and small businesses in Brazil' (15 June 2020) <https://blog.whatsapp.com/bringing-payments-to-whatsapp-for-people-and-small-businesses-in-brazil>.

37 See the definition of fiat money (currency): one that is declared legal tender and issued by a central bank. Fiat money derives its value from public trust in central banks in order to maintain price stability.

38 Facebook, 'Coming in 2020: Calibra' (18 June 2019) <https://about.fb.com/news/2019/06/coming-in-2020-calibra/>.

Novi Financial[39] and headquartered in the state of California, USA, the entity has also been registered as MSB[40] by FinCEN which is passport-able among all states.

20 The first product of the company, the Novi digital custodial wallet, is set to be rolled out as a stand-alone software application, yet duly integrate-able in Facebook's core products of Messenger and WhatsApp.[41] In other words, operational interoperability would in principle be ensured between Diem, Messenger and WhatsApp infrastructures. The Novi wallet is a crucial element in the operability of the project given that it will serve as the main user interface upon which services would be built based on smart contract codes.

21 Furthermore, Facebook Financial (F2)[42] has been established as an internal group mandated with streamlining and managing Facebook's payments projects including Facebook Pay. The group will be led by the head of Novi Financial, who will also be involved in WhatsApp's electronic payment system initiative. Notably, Novi Financial is one of the members of the Diem Association.

22 As an interim remark, it has become increasingly apparent from the organisational breakdown of Diem, as it stands to date, that Facebook is arguably set to maintain a certain degree of governance and control, albeit indirectly, over the project. Through the bundling of its in-house software applications with the company's core products, the dynamics of user dependency seem to emerge, despite Facebook's absence from the membership of the Diem Association, respectively considering the fact that the company seems to no longer own stakes in Diem Networks in Switzerland and the USA. Once users would be enabled to engage in spending behaviour across Facebook's core products free of charge in return for their metadata, the company's advertising revenue would be set to experience an exponential growth.

II. Technical Typology & Taxonomy

1. Main Characteristics

23 The proposed Diem alternative financial infrastructure is set to be designed and built based on distributed ledger technology (DLT).

24 DLT could be defined as a shared database (or ledger) of records, distributed among computer nodes outside jurisdictional boundaries. A subset of involved interactions between these nodes is defined by consensus protocols. Every entry, update or transaction to the ledger would be time stamped, cryptographically hashed,[43] cryptographically signed[44] and authorised prior to its addition to the ledger.

25 An algorithmic consensus would represent the agreed-upon true state among all participants and stakeholders, which could either be reached on a system level or on an individual deal level, depending on the type of DLT deployed.

26 DLT can take various forms depending on the deployed participation and governance protocols, among which is a typical public and permission-less model. Here, the ledger would essentially operate on the basis of 'data broadcasting', where data is in principle broadcast to every single computer node on the ledger, irrespective of any associated interest or stake. DLT could also be designed in a hybrid public and permissioned format, or, in a rather stricter sense, in a private and permissioned format, or organised as a consortium.[45]

39 Facebook, 'Welcome to Novi' (26 May 2020) <https://about.fb.com/news/2020/05/welcome-to-novi/>.

40 See <https://www.docdroid.net/544Gxxg/calibra-msb-registration-pdf>; reference to FinCEN's definition of the term 'money services business (MSB)' as "a person wherever located doing business, whether or not on a regular basis or as an organised or licensed business concern, wholly or in substantial part within the United States, operating directly or through an agent, agency branch, or office, who functions as, among other things, a money transmitter." in FinCEN Guidance (FIN-2019-G001, 9 May 2019), 3.

41 Facebook, 'Welcome to Novi' (n 39).

42 'Facebook Financial Formed to Pursue Company's Payments Plans' (*Bloomberg,* 10 August 2020) <https://www.bloomberg.com/news/articles/2020-08-10/facebook-financial-formed-to-pursue-company-s-commerce-ambitions>.

43 A cryptographic hash function is a mathematical function used in cryptography. Typical hash functions take inputs of variable lengths to return outputs of a fixed length. A cryptographic hash function combines the message-passing capabilities of hash functions with security properties. Cryptographic hash adds security features to typical hash functions with stronger mathematical guarantees for collisions etc.

44 This process is made possible through the creation of encryption schemes such as asymmetric encryption or public key infrastructure (PKI) with public/private key pairs. Digital signatures are generated by private keys. Digital signatures are defined as "mathematical schemes for demonstrating the authenticity of a digital message."

45 For more on this see N Kannengisser et al., 'Trade-offs between Distributed Ledger Technology Characteristics'

27 In addition, from a legal and regulatory compliance perspective, in 'data propagation', as opposed to data broadcasting, transaction records would only be shared with nodes on a *need-to-know* basis depending on their stake, which would then enhance privacy and data protection thresholds. The form a DLT takes defines the scope of 'read' and 'write' privileges and restrictions granted to the network participants. The internal governance of a given DLT network would therefore be closely interlinked with the factual dynamics surrounding its nodes. Disintermediation associated with DLT effectively lays the ground for poly-directional relationships among nodes that are connected through software programmes.[46]

28 Notably, the choice of the architectural form of an underlying DLT would also have potential implications, directly or indirectly, in the way a smart contract code is defined and operated. A smart contract code is essentially a decentralised application running on a DLT network.

29 A smart contract code could be defined as a computer programme written based on a number of predefined terms and conditions as well as oracles. These programmes can facilitate, verify and enforce the negotiation and execution of legal contracts.[47] They can have interfaces to handle input from parties to contracts.[48] An oracle is an agent or an interface designed to verify external data and real-life occurrences. Upon satisfaction of the pre-defined terms and conditions, and the update of external data through the means of oracles, these programmes would change their state of information and autonomously self-execute[49] the predetermined outcome. Automation is, as a result, seen as an inherent and key feature of a smart contract code. Here, pre-defined terms and conditions as well as outcomes between *trust-less*[50] network participants, i.e. in the context of parties to a given transaction, would in principle be executed without reliance upon intermediation.

30 Furthermore, DLT enables the creation of native value[51] from scratch, which is intrinsically accrued from the rules of the system as well as network participation therein. Alternatively, a real world value can be collateralised and digitally represented in the form of a token appendable on DLT, otherwise known as asset tokenisation, with the end product often referred to as a crypto-asset.

31 Here, a token[52] is defined as a piece of information recorded on DLT, and takes the form of digital representation of value or asset, respectively a claim, ownership or access right. The terms token and crypto-asset are often referenced interchangeably in different jurisdictions. In the EU, preference is given to crypto-asset,[53] whereas in Switzerland the term token[54] is mostly utilised.

(2020) ACM Computing Surveys (CSUR), 53(2), 1-37.

46 P Paech, 'The Governance of Blockchain Financial Networks' (2017) Modern Law Review, 80(6) MLR.

47 M Wöhrer & U Zdun, 'Smart Contracts: Security Patterns in the Ethereum Ecosystem and Solidity' (2018) IWBOSE, IEEE, 2.

48 Ibid.

49 In this context, 'technical enforcement' is not synonymous to 'legal enforcement'.

50 Here the term 'trust-less' strictly refers to the absence of a concentrated single intermediary. In other words, in the DLT context there are mechanisms put in place that facilitate distribution of 'trust', whereby participants in the system, without necessarily trusting one another, are able to reach consensus as to a 'true state'.

51 Known examples are Bitcoin and Ethereum blockchain networks.

52 See Liechtenstein Tokens & Trusted Technology Service Provider Act "TVTG" (January 2020), Article 2 <https://www.gesetze.li/konso/2019301000>; for 2020 unofficial translation <https://www.regierung.li/media/medienarchiv/950_6_08_01_2020.pdf?t=2>; in a general technical sense: "tokens are classified as ordinary or delimiter tokens. An ordinary token is a numeric constant, an ordinary identifier, a host identifier, or a keyword. A delimiter token is a string constant, a delimited identifier, an operator symbol, or any of the special characters shown in the syntax diagrams", see <https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_73/db2/rbafzch2tok.htm>; in a DLT context: "token is a digital representation of value on a shared distributed ledger that is owned and secured using cryptography to ensure its authenticity and prevent modification or tampering without the owner's consent", see <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf>.

53 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA)', COM (2020) 593 final.

54 FINMA, 'Guidelines for enquiries regarding the regulatory framework for ICOs' (February 2018) <https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en>.

32 In this respect, a token or a crypto-asset[55] whose value is derived from an underlying asset that is considered stable, in order to limit price volatility, is also referred to as stablecoin.[56] The underlying asset can take various forms of one or more fiat currencies, one or more commodities, real estate as well as securities.[57]

33 Nevertheless, an algorithmic stablecoin[58] is denoted as one which aims at maintaining a stable value via protocols, whereby the supply of the crypto-assets would increase or decrease in response to changes in demand, and one which does not reference one or more other assets. Additionally, global stablecoin[59] refers to one that has a worldwide reach, is adoptable across jurisdictions and bears the potential to achieve significant volume. Such a tailor-made definition seems on face value to tie in with Diem. Nevertheless, as noted earlier and to be elaborated further in section C., it becomes increasingly apparent that such a classification may not be entirely accurate.

2. Version 1.0

34 Diem first issued its whitepaper version 1.0[60] in June 2019 with the objective to deliver on the promise of *the internet of money*. The initial approach of the project was a DLT-based financial system backed by a reserve of assets and governed by the Libra Association, now Diem Association. The token previously called Libra "LBR" was set to be backed by a basket of bank deposits and short-term government securities held in the Libra Reserve, which would be administered by both the association and its subsidiary Diem Networks, for every LBR created.[61] Both Facebook and Calibra, now Novi Financial, were among the founding members of the association. Also among the member entities was Breakthrough Initiatives, co-founded by Facebook's founder Mark Zuckerberg.[62] The final decision making, as is currently the case, was given to the association, while Facebook was to maintain leadership of the project during the project's inception year, 2019. Once launched, Facebook and its affiliates' role in governance were to be equal to other members.[63]

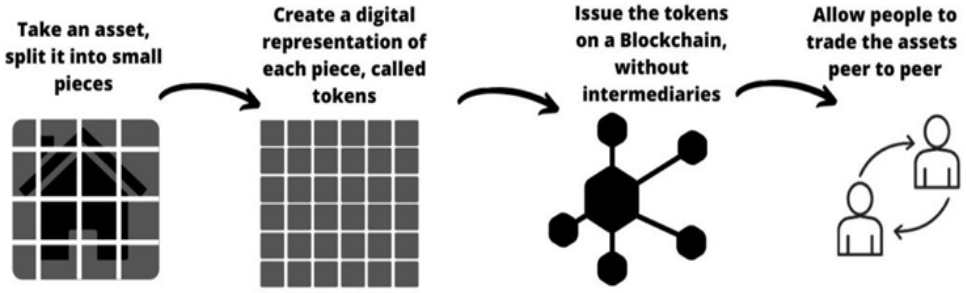

Figure i: simple example of asset tokenisation; credit: www.assetsonblockchain.com

35 The version 1.0 was set to be based on a permissioned DLT[64] with an aim to move towards a permission-less governance model. In both scenarios, the network's participation protocol was to be open access. Smart contract codes would be written based on the Move virtual machine programming language,[65] and the

55 A distinction can be made between fungible and non-fungible crypto-assets. A fungible crypto-asset can be replaced by an equivalent asset with similar market value. A non-fungible crypto-asset or token (NFT) is in principle uniquely identified to ensure its traceability and is generally irreplaceable.

56 FINMA, 'Supplement to the guidelines' (11 September 2019), 1-4, <https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-stable-coins.pdf?la=en>.

57 Ibid.

58 COM (2020) 593final (n 53) Recital 26; Financial Stability Board (FSB), 'Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements' (13 October 2020), 5, <https://www.fsb.org/wp-content/uploads/P131020-3.pdf>.

59 Ibid.

60 Libra whitepaper v1.0, 'An Introduction to Libra' (June 2019).

61 Ibid 3 &7; it is emphasised that LBR is not pegged to any single currency, and "...will not always be able to convert into the same amount of a given local currency. Rather, as the value of the underlying assets moves, the value of one Libra in any local currency may fluctuate"; Furthermore LBR was set to be interest bearing.

62 See <https://breakthroughinitiatives.org/board>.

63 Libra whitepaper v1.0 (n 60), 4.

64 Ibid.

65 Ibid 5 "...by making the development of critical transaction

consensus mechanism would be based on byzantine fault tolerant (BFT),[66] a variation of voting-based mechanisms, carried out by selected validator nodes, i.e. the members of the association who are publicly identified on the network. For this, validator nodes would process transactions and interact with each other in order to reach consensus on the state of the database (or ledger).[67] Notably, smart contract code risk control and management would be carried out by the Diem Association,[68] whereby only the association approved smart contracts were to be published and interact directly with the Diem payment system.

36 As an additional objective to develop and promote an open identity standard,[69] the network would enable pseudonymisation,[70] in principle allowing users to hold multiple addresses (accounts)[71] without risking correlation of these accounts with the holders' real world identities. This is made possible through generating multiple key pairs. On the other hand, a reference is made to the underlying DLT which is set to take the form of a single data structure which would record the history of transactions and states over time,[72] whereby through a unified framework applications could read any data on-ledger at any point in time for proof of integrity.

code easier, Move enables the secure implementation of the Libra ecosystem's governance policies, such as the management of the Libra currency and the network of validator nodes."; "It enables 'resource types' that constrain digital assets to the same properties as physical assets: a resource has a single owner, it can only be spent once, and the creation of new resources is restricted."

66 Ibid.

67 The Libra Blockchain (n 25), 1.

68 Libra whitepaper v2.0 (n 32), 8.

69 Libra whitepaper, v1.0 (n 60), 9.

70 Ibid 6; Regulation (EU) 2016/679 of the European Parliament and of the Council on the general protection of natural persons with regard to the processing of personal data and on the free movement of such data , and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)) (2016) OJ L119/1, Art. 4(5) on the definition of pseudonymisation: "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

71 The Libra Blockchain (n 25), 4.

72 Libra whitepaper, v1.0 (n 60), 6.

37 It consequently remains rather unclear as to how data visibility would be maintained on the network, which would then have direct implications regarding privacy.

3. Version 2.0

38 Shifting away from the version 1.0, version 2.0 was introduced with an update on the whitepaper in April 2020.[73] Diem would introduce multiple tokens, each backed by a single fiat currency, in the form of stablecoins. Each single currency stablecoin would then be fully backed[74] by the Diem Reserve, the administration of which is seemingly set to be transparent to the public.[75]

39 The project also seemed to perpetuate its original initiative of creating an intra-network token LBR, now Diem, in principle to be backed by a basket of multiple fiat currencies and other assets, acting as a "digital composite" of the stablecoins created on the network. This token would also be utilised as a means of settlement for cross-border transactions, in particular for jurisdictions where single currency stablecoins have not been introduced, and would be convertible to respective local currencies through third party service providers. The two-fold token model would collectively be referred to as Diem coins.[76]

40 The planned combination of a permissioned DLT platform with integrated smart contract code applications, and an intra-network Diem token together with a variety of single currency stablecoins, governed and supervised by a central authority, was intended to evolve into an ecosystem in the financial services sector, which a large part of the world's population could access via ordinary smartphones and edge devices.

41 Diem took a step further in its version 2.0 aiming at integrating central bank digital currency (CBDCs)[77]

73 See n31f.

74 Libra whitepaper v2.0 (n 32), 12; "full backing means that the Reserve will hold, in cash or cash equivalents and very short-term government securities, an amount at least equal to the face value of each Diem coin in circulation."

75 Ibid 13.

76 For taxonomic breakdown, see Jackson, 'Global 'stablecoin' Challenges' (n24), 6f; for the latest developments as to design of the Diem tokens during the initial phase of the project see n 13.

77 Libra whitepaper v2.0 (n 32), 2.

models once these begin to materialise. The initial plan of moving towards a permission-less DLT network has seemingly been omitted from the agenda of the latest version, governance of which now seems to take place collaboratively between the Diem Association and its subsidiary Diem Networks US, Inc. Facebook is no longer seen as a member of the association, without any special rights.[78] Novi Financial remains as a member together with Breakthrough Initiatives.

42 Diem Networks was mandated with the definition of policies and procedures for reconfiguring the Diem DLT network in case of critical errors, respectively in case of a need for upgrades.[79] The company would, based on contractual arrangements, mint and burn Diem tokens for the purpose of distribution to the market via designated entities called dealers, which would be regulated as financial institutions.[80] Diem Networks would therefore not enter into any contractual relationship with exchange platforms or end users, save for emergency operations.[81] Diem Association would exercise control over the process of minting and burning of Diem tokens, the mandate for which was given to Diem Networks. The association and its subsidiary, Diem Networks, would also operate a compliance infrastructure integrated in the form of a financial intelligence unit (FIU)[82] function, in order to monitor the network regarding any suspicious activity.

43 User interaction with the Diem DLT network was set to take place via regulated or certified virtual asset service providers (VASPs).[83] Alternatively, direct user access would also be made possible, albeit with limited transaction volume and account address balance, through Unhosted Wallets.[84] At protocol level, VASPs would be required to comply with the "travel rule" when transacting.[85] The travel rule[86] ensures that VASPs collect and exchange beneficiary and originator information with VASP counterparties for any transmittal exceeding USD 1,000. Under the travel rule, the required personally identifiable information (PII)[87] would include names, account numbers, physical addresses as well as unique identification numbers. In the course of facilitating transactions on behalf of users, VASPs would be given the possibility to record transactions off-ledger and internally in their respective books.[88]

44 In light of this requirement, it is arguable as to the manner in which Diem would effectively maintain user pseudonymity and respect correlation resistance between users' activities on the system and their real identities.

45 As mentioned, the Novi digital custodial wallet, which would most probably function as a hosted wallet, would act as the main user interface of the

78 Ibid 6.

79 Ibid 8; at the time of this writing Diem Networks referred to the subsidiary based in Switzerland which was the candidate for a payment systems licence application pending a decision by FINMA. At present, with the withdrawal of the FINMA licence application, Diem Networks US, Inc., a sister subsidiary wholly owned by Diem Association, has instead been registered as a money services business (MSB) licensee by FinCEN in the US.

80 Ibid 17.

81 Ibid 13f "In the context of a recovery and resolution plan, the association is considering whether to provide for two key components that could be implemented in severe stress scenarios in the unlikely case that the network is unable to convert the very short-term government securities in the Reserve into cash fast enough to satisfy all requests to burn Diem coins without incurring fire-sale losses: a) redemption stays which would delay Diem coin redemptions and allow for additional time to liquidate the Reserve's assets during a window of time without incurring large fire-sale losses, b) early redemption haircuts which would impose a fee for instant redemptions and require coin holders to internalise their negative externality (i.e., fire-sale losses) in a run."

82 The term financial intelligence unit (FIU) is defined as a "... central, national unit that is responsible for receiving and analysing information from private entities on financial transactions which are considered to be linked to money laundering and terrorist financing," see Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (4AMLD) (2015) OJ L141/73.

83 Financial Action Task Force (FATF), 'Guidance for a risk based approach: virtual assets and virtual asset service providers' (June 2019), 13 <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>.

84 Libra whitepaper v2.0 (n 32), 18f; Distinction between hosted and unhosted wallets lies in the exercise of control over private keys. In the case of hosted wallets, private keys are stored by third parties, whereas in unhosted wallets private keys remain in the control of users.

85 Ibid 20.

86 FATF, 'Guidance for a risk based approach' (n 83), Recommendation 16, 28 – 31.

87 The term 'personally identifiable information (PII)' is used interchangeably with the term 'personal data', which is used in the EU General Data Protection Regulation (GDPR).

88 Libra whitepaper v2.0 (n 32), 18.

network. In terms of user data privacy, account information and financial data would not be shared with Facebook and its core products, i.e. for the purpose of improving advertisement targeting, except in particular cases.[89] These include the prevention of crime, compliance with law, payment processing and service providers as well as in the case of data aggregation related to service performance and related products, with an in-built correlation resistance technique, details of which remain unclear.

46 The wallet would integrate an identity system named 'visual identity', with an obligatory identification of all users through government issued identities. Arguably,[90] the Novi wallet design would be implemented in the form of an off-ledger payment mechanism,[91] with Novi Financial acting as a VASP, for the provision of both exchange and custodial wallet services. Novi Financial would then "hold all Diem coin backing for Novi balances in its own accounts on the underlying Diem DLT network."

C. Legal & Regulatory Framework

I. Diem's Fundamental Nature

47 The legal and regulatory implications concerning the technical design of Diem are directly dependent upon the *substance* underlying such design. As mentioned earlier, there seems to be no clear-cut distinction to be made as to whether the intended design would fall under an *account-based*, or *token-based* private currency issuance. This distinction would be essential in understanding the applicable identification and verification requirements thereof.

48 In addition to the general civil law status of cryptographically generated tokens (crypto tokens) on DLT, it is essential to determine whether Diem could be considered *money* and in what way it will be comparable to currencies such as fiat money.[92] Not least, the question arises as to what extent an underlying *intrinsic value* could make a decisive difference in this equation.

49 In economic theory, a functional definition of money[93] generally consists of three elements of a) a unit of account, b) a means of payment (exchange), and c) a store of value. Money can either be physical (cash) or non-physical (scriptural or electronic).

50 More specifically, *public* money is distinguished from *private* money[94], whereby *public* money is defined as fiat money or fiat currency that is legal tender[95] and which is issued by central banks. *Private* money takes the form of fiat currency credit issued by licensed credit institutions such as retail and commercial banks. Fiat money derives its value from *public trust* in central banks which are primarily mandated to maintain price stability.

51 At first glance, the two-fold Diem design, in the form of single fiat currency stablecoins and an intra-network Diem token backed by a basket of multiple fiat currencies and other assets as the 'digital composite', seems to satisfy the three inherent constituents of money, albeit issued in the form of *private* currency. Here, it is pivotal to take account of the fact that the nature of Diem tokens as a *store of value* may be questionable with reference to the trust associated with the survivability of the Diem Reserve. Given the significant user base, global reach and network effect of Facebook and its associated group of entities, it would not be far-fetched to argue that the Diem design would satisfy the *means of payment (exchange)* element.

52 When defining the legal significance of crypto tokens and their classification, *substance* matters over *form*. As referred to in the preceding sections, DLT can enable the creation of native value from scratch through token representation. Such value would intrinsically be accrued from the rules of the system, network participation as well as the market response to those set rules. Here, the token is seen as an empty container.[96] Alternatively, real world

89 Facebook, 'Novi: Customer Commitment', 1f. < https://bit.ly/3826M16>.

90 Jackson, 'Global 'stablecoin' Challenges' (n 24), 22.

91 The Libra Blockchain (n 25), 22; it is anticipated that many payment transactions on Diem will occur off-ledger, for example, within a custodial wallet or by using payment channels.

92 On the regularly repeated functions of money, see eg K Langenbucher, 'Digitales Finanzwesen. Vom Bargeld zu virtuellen Währungen' (2018) 218 AcP 385, 388f.; L Müller & M Ong, 'Aktuelles zum Recht der Kryptowährungen' (2020) 29 AJP/PJA 198, 206ff.

93 See n 18.

94 See section D.III.

95 See the definition of the term 'legal tender' under Commission Recommendation on the scope and effects of legal tender of euro banknotes and coins (2010/191/EU) OJ L 83/70, para.1 regarding euro banknotes and coins "...where a payment obligation exists, the status of legal tender should imply three things: first, mandatory acceptance; second, acceptance at full face value; and third, the power to discharge from payment obligations."

96 As reflected in Liechtenstein TVTG Act (n 52).

value can be collateralised and digitally represented in the form of a token appendable on DLT. This is known as asset tokenisation, with the end product often referred to as a crypto-asset. Therefore, it is feasible to consider, and before any economic, sociological or legal classification, crypto tokens as semantic artefacts of network communication of digital platforms.

53 In this respect, initial, tentative approaches describe the likes of first category crypto tokens such as bitcoin, where value is created on DLT from scratch and maintained through the rules of the system, as "value-embodying data".[97] Here, it would certainly have to be asked whether the term *value embodiment*[98] is an oxymoron, which obviously presupposes an immaterial entity in which values could materialise. Above all, it has been argued that the monetary data value of such crypto token units should be considered distinct from the immaterial effects of data protection based on personal rights.[99]

54 There is widespread agreement in the so far sparse[100] civil law[101] literature only on what crypto tokens are not. Crypto tokens are not considered as things, since they are not separable, physical objects,[102] nor are they to be qualified as claims.[103] The latter would only be possible if a central institution owed the holders of crypto tokens a payment in the form of a contractual redemption right.[104] However, this prerequisite can not only be assumed for e-money, but also for e-money tokens, which will be discussed in the subsequent section. At best, a claim could then be derived from a relationship under corporate law between all users of a closed network.[105]

55 On the other hand, crypto-assets have been classified as property *sui generis* in a number of jurisdictions, in particular in common law systems such as the UK.[106]

56 Arguably, the lack of identifiability of a claim may lead to the assumption of an unplanned regulatory gap, which would have to be filled by analogy according to the rules of traditional legal methodology.[107] However, even the precondition of a regulatory gap can be doubted. This is because of the result of the underlying analogy, for example, an alleged equivalence[108] of crypto tokens in terms of property law, which is almost circularly based on the assumption of similarity with movable property or money.[109] Therefore, functional equivalences with traditional property ownership according to the standards of national property law provisions hardly lead any further.[110] Rather, they threaten to obscure the view of

97 Langenbucher, (2018) (n 92), 409.

98 Cf BV Enz, 'Die zivilrechtliche Einordnung von Zahlungs-Token wie dem Bitcoin als "Registerwertdaten" und deren Aussonderbarkeit im Konkurs de lege lata und de lege ferenda' (2020) 116 SJZ, 291, 294.

99 Cf S Omlor, 'Kryptowährungen im Geldrecht' (2019) 183 ZHR, 294, 311: "Such a personal rights component is missing from the sober transaction data on a payment blockchain".

100 Cf A Walter,'Bitcoin, Libra und sonstige Kryptowährungen aus zivilrechtlicher Sicht' (2019) 72 NJW, 3609 („shadowy existence").

101 See German Civil Code "BGB", Section 90; Swiss Civil Code "ZGB", Art. 641ff.

102 See n 99; see also B Beck & D König,'Bitcoin: Vertragstypologische Einordnung von kryptographischem Geld' (2015) 70 JZ, 130ff.; Langenbucher, (2018) (n 92), 405. In this respect, the German legal definition of the term "Sache" also corresponds to the Swiss private law doctrine on the interpretation of the Art. 641ff ZGB; see for instance Enz, (2020) (n 98), 293f; ibid, *Kryptowährungen im Lichte von Geldrecht und Konkursaussonderung* (Zürich 2019), paras.334ff.

103 Cf Langenbucher, (2018) (n 92) 385, 405ff; on the difficulties of classification from the perspective of U.S. law, see CS Goforth, 'U.S. Law: Crypto is Money, Property, a Commodity, and a Security, all at the Same Time' (October 25, 2018), Journal of Financial Transformation (forthcoming) <https://ssrn.com/abstract=3272975>.

104 See German Civil Code "BGB", Section 241(1) sentence 1.

105 Cf DA Zetzsche, RP Buckley & DW Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2017) 52 UNSWLRS, 26ff <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018214>; HC von der Crone, FJ Kessler & L Angstmann, 'Token in der Blockchain – privatrechtliche Aspekte der Distributed Ledger Technology' (2018) 114 SJZ, 340 f ("System agreement among all participants").

106 UK Jurisdictional Task Force (UKJT), 'Legal Statement on Crypto-assets and Smart Contracts' (November 2019); the UKJT statement has been endorsed by the English case law namely AA v Persons Unknown [2019] EWHC 3556, paras.57-59.

107 Cf Walter, (2019) (n 100), 3611ff.

108 Cf Walter, (2019) (n 100), 3613 ("Crypto tokens are supposed to correspond to cash in terms of their structure and thus to a movable thing").

109 For a critical view on such analogy conclusions from a Swiss perspective, see Enz, (2020) (n 98) 291, 293f; ibid, *Kryptowährungen im Lichte von Geldrecht und Konkursaussonderung* (Zürich, 2019), paras.345ff.

110 On Swiss property law, cf. B Graham-Siegenthaler & A Furrer, 'The Position of Blockchain Technology and Bitcoin in

the specific differences between the objects of two completely different media worlds.

57 In general, depending on the contingencies of the legal dogmatics of national legal systems, crypto tokens could be regarded as "other objects".[111] The conceptual commonality of "other objects" and things consists only in the fact that both types of legal objects are goods that differ precisely with regard to the characteristic of corporeality. As "incorporeal goods", "other objects" thus include all goods not covered by property law. These include, among others, intangible goods regulated by special law, but also unprotected inventions, technical know-how, as well as digital data and virtual goods.[112] In this respect, it appears obvious to also consider crypto tokens as "incorporeal goods",[113] which thus would find their place beyond objects and rights as legal objects *sui generis*.

58 Of course, this construction cannot hide the fact that the classification of property found in this way has its origin in legal relationships based on the law of obligations.[114] It would therefore be only logical that it is sometimes addressed with the rather vague term of "other property rights".[115] Thus, on the basis of "proven dogmatics", an attempt is made[116] to treat crypto tokens *de lege lata* in the context of claims under the law of condemnation as suitable objects of unjust enrichment[117]or as "other rights" protected in tort.[118]

59 Here, however, a clear distinction must be made between property law and personality law justifications of tort protection.[119] While the "guarantee of confidentiality and integrity of information technology systems" developed by the German Federal Constitutional Court[120] under personality law also forms a corporeal object of protection for tort law,[121] the more extensive classification of property-like rights of control over data or data files as "other rights" encounters some concerns.[122]

60 At the least, a corresponding protection of property-like data without attribution to personal rights requires an increased argumentative effort. Apart from the controversial discussion about a supposed new *right to one's own data*, it must be borne in mind that such *data ownership*[123] denotes something fundamentally different from data protection derived from personal rights. Even more far-reaching attempts to extend tort protection to individual units of crypto tokens may therefore seem rather far-fetched.[124] Such approaches, as well as the many other inadequate attempts at analogies, functional equations or equivalences, make clear that the current "private law system is completely undeveloped with regards to blockchain technology".[125] The widespread idea that civil law could also "keep up with the developments of modern technology"[126] in this respect would only appear as a continuation of the mantra constantly repeated in civil law that a mature jurisprudence will no longer be embarrassed by history.[127]

Swiss Law' (2017) Jusletter 8.5.2017, paras.42ff.

111 See German Civil Code "BGB", Section 453(1).

112 See, with further examples, A Peukert,'"Sonstige Gegenstände" im Rechtsverkehr' in S Leible, M Lehmann & H Zech (eds.), *Unkörperliche Güter im Zivilrecht* (Tübingen 2011), 95ff; referring to Beck & König, (2015) (n 102), 132f.

113 Cf Beck & König, (2015) (n 102).

114 In this respect, the Roman legal concept of *res corporales* (Inst. 2.2.; Dig. 1.8.1.) appears as a possible equivalent precisely because of its open inclusion of rights; differently Peukert, (2015) (n 112).

115 See Langenbucher, (2018) (n 92), 407; G Spindler & M Bille,'Rechtsprobleme von Bitcoins als virtuelle Währung' (2014) 68 WM, 1357, 1360.

116 Langenbucher, (2018) (n 92), 407ff.; Spindler & Bille, (2014) (n 107), 1363.

117 See German Civil Code "BGB", Section 812; Swiss Code of Obligations "OR", Art. 62ff.

118 See German Civil Code "BGB", Section 823(1); Swiss Code of Obligations "OR", Art. 41(1).

119 Equally unclear in this regard Langenbucher (n 92); Spindler & Bille, (2014) (n 115); cf. also G Spindler, 'Digitale Wirtschaft – analoges Recht: Braucht das BGB ein Update?' (2016) 71 JZ, 805, 813f.

120 German Federal Constitutional Court, BVerfGE 120, 274.

121 Cf M-C Gruber, *Bioinformationsrecht. Zur Persönlichkeitsentfaltung des Menschen in technisierter Verfassung* (Tübingen 2015), 158ff.

122 See eg A Spickhoff, 'Der Schutz von Daten durch das Deliktsrecht' in S Leible, M Lehmann & H Zech (eds.), *Unkörperliche Güter im Zivilrecht* (Tübingen 2011), 233ff, 243ff.

123 For a profound consideration based on legal theory, see M Amstutz, 'Dateneigentum. Funktion und Form' (2018) 218 AcP, 439ff.

124 In this sense Omlor, (2019) (n 99), 310.

125 See, with regard to German civil law, ibid; cf also Spindler, (2016) (n 119), 816.

126 Walter, (2019) (n 100), 3609.

127 Cf M-C Gruber, 'Futurities of Law. Versuche über die Zukunft

61 After the legal perspective of traditional legal doctrine has to give up its claim to develop the digital law of the future as the only authoritative perspective of observation, it will no longer be able to unilaterally determine the legal quality of crypto tokens. It would then no longer be necessary to ask primarily whether they correspond to (personal) property, whether they are similar to "coinage" or "cash", or even comparable to "forces of nature" or "energy", whether they are more like claims or securities, or to what extent they come closest to new types of intangible property.

62 Answers to the legal questions must therefore rather be sought where the new legal phenomena unfold, namely in the *second, digitalised* legal world itself. From such a perspective, primarily the specific characteristics of crypto tokens as to their substance ought to be worked out in order to draft the appropriate, independent standardisations on this basis.

63 In this context, a number of recent bespoke regulatory developments aim in principle at bringing clarity to crypto token legal classifications. Here, the new legal objects *sui generis* could be anchored, for instance, in separate civil law provisions as rival, exclusively assigned "register value data",[128] as "register value rights"[129] or as "property-like legal assets"[130], among others.

64 For the purposes of this paper, and in the context of Diem and alongside potential implications thereof, the recent regulatory developments in the jurisdictions of Switzerland, the EU and the USA have primarily been put under scrutiny.

II. Developments as to Classifications

1. Switzerland

65 The Swiss FINMA has categorised[131] crypto tokens in four groups of a) utility tokens, b) payment tokens, c) asset tokens and d) hybrid tokens. Payment tokens are means of payment, lacking any further function or link to any other development project, whereas utility tokens are those intended to provide digital access to an application or service. Asset tokens refer to underlying physical assets, company equity and rights such as dividends and interest payments, while hybrid tokens are a combination of any of the above. FINMA has also recognised[132] the emergence of stablecoin models, and in their classification, the authority has reiterated the view that *substance* matters over *form.*

66 At first glance, Diem would take a hybrid format seemingly catching features from at least two of the above categories, namely payment and asset tokens. The single fiat currency stablecoins would each be backed by a fiat currency, whereas the intra-network Diem token would act as a "digital composite" of some of those stablecoins, and would be backed by a basket of multiple fiat currencies and other assets. This would be in line with the definition of an asset token. Aimed as a complementary payments system, Diem's underlying purpose has been to provide for an alternative means of payment. Respectively, in order to be granted access to the Diem infrastructure and utilise its applications, end users would in principle need to acquire Diem tokens. Notably, purely utility tokens do not in general embody any financial purpose.

67 As a result, it seems that Diem's two-fold design incorporates characteristics from asset tokens, payment tokens and, partially, from utility tokens. In addition, Diem's two-fold design can be seen to derive its value from the underlying referenced fiat currencies and other assets. Consequently, Diem could be considered as a form of security under Swiss law, when defined[133] as a derivative or a financial contract, the price of which is set particularly according to a) assets such as shares, bonds, commodities etc., and b) reference values such as currencies, interest rates etc.

68 It can then be argued that the liability to comply with potential conversion claims by the token holders remains with the Diem Association and its subsidiaries. In this context, irrespective of contractual exonerations, it would be erroneous to consider intermediaries such as the third party service providers as independent actors, rather than agents.

69 Notably, Diem would only assume functionality by means of the underlying (implied) right to claim fiat currency or other assets. This in itself would then represent Diem as the effective embodiment of an

des Rechts' (2021) 107 ARSP (forthcoming).

128 Cf Enz, (2020) (n 98), 295.

129 See section C.II.1.

130 See, with regard to German civil law, Omlor, (2019) (n 99), 341, considering the insertion of a new Section 90b in German Civil Code "BGB".

131 FINMA, (2018) (n 54).

132 FINMA, (2019) (n 56).

133 Financial Market Infrastructure Ordinance (FMIO) (25 November 2015), Art. 2.2 (a)(b).

uncertificated security, issued by and subjected exclusively to the rules of the Diem network, thus rendering and mimicking a transfer system used for payment claims against debtors.

70 Recently, Swiss law has undergone a legislative reform process[134] that permits the exchange of asset tokens as uncertificated securities. This specific category of tokenised rights,[135] defined as uncertificated register securities,[136] and their legal transfer thereof, would therefore serve relevance in the context of Diem. The new laws will impose an obligation against the crypto token issuer, whereby holders would be given legal certainty in terms of the effect of disposal of the rights embodied in such tokens. Also, certain security standards by way of appropriate technical and organisational measures would need to be met by an underlying DLT system upon which the entries will be appended. The system would need to show resistance to manipulation, and be designed in such a way that no unauthorised intervention would be possible, in particular by the system operators and the third party service providers.

71 On the other hand, under Swiss law the validity of the underlying transaction is required in order for the disposal of a right or asset to have any legal effect. Under the principle of causality, therefore, Diem token holders would need to be able to demonstrate their legal status as holders, independently from any third party such as the third party service providers. This would imply the holder exercising a certain control over digital identifiers associated with the corresponding Diem tokens. Here, verification of such control would be available to any potential new beneficiary, without the need for the register on the Diem DLT network to be publicly accessible. This requires a particular identity management mechanism as addressed in the subsequent section.

72 The new laws in Switzerland also introduce a legal framework[137] for segregation of crypto-assets from third party service providers who provide custodial services. On the Diem network, dealers, VASPs and Novi digital custodial wallet must therefore undertake to keep the assets of third party clients available for those particular clients *at all times*.

73 Nevertheless, as mentioned, Diem Reserve seems to be fully backed by cash or cash equivalents and very short-term government securities, which can be assumed not to consist of segregated accounts specifically referring to identifiable token holders.

2. European Union

74 In the EU, the European Commission[138] has recently put forward a proposal for a Regulation on Markets in Crypto-assets (MiCA). Distinction is made between three sub categories of crypto-assets. These include a) utility tokens which provide digital access to a good or service, accepted only by the issuer of that token without a financial purpose and related to the operation of a digital platform; b) asset-referenced tokens which aim at maintaining a stable value by referencing several currencies that are legal tender,[139] one or several commodities, one or several crypto-assets, or a basket of such assets, often for the purpose of a means of payment to buy goods and services and to transfer value; and c) e-money tokens which are intended primarily as a means of exchange by referencing only one fiat currency that is legal tender, with a function arguably similar to that of electronic money (e-money).[140]

75 Notably, e-money tokens bear close similarities to e-money on the grounds that the holders of both

134 Swiss DLT Framework, parliamentary approval of 25 September 2020 <https://www.admin.ch/opc/fr/federal-gazette/2020/7559.pdf>; Note: The amendments to the Swiss Code of Obligations, the Federal Intermediated Securities Act and the Federal Act on International Private Law that are envisaged in the DLT bill have now enter into force from 1 February 2021. These provisions enable the introduction of ledger-based securities that are represented in a DLT. The remaining provisions of the DLT bill have entered into force as of 1 August 2021.

135 See Art. 973d – 973i, Swiss Code of Obligations (CO).

136 See reference to the term "Registerwertrechte"; CMS Law –Now, 'The new Swiss blockchain/DLT laws have been finalised and presumably entre into force early 2021' (15 October 2020) with reference to "uncertificated register securities have features largely analogous to traditional certificated securities. Any right that can be securitised also qualifies as an underlying right for uncertificated register securities, including asset tokens and utility tokens." < https://cms.law/en/che/blogs/law-now-blog/the-new-swiss-blockchain-dlt-laws-have-been-finalised-and-presumably-enter-into-force-early-2021>.

137 See the amended Art. 242a., Swiss Debt Enforcement and Bankruptcy Law (DEBL).

138 COM (2020) 593 final (n 53), Art.3; Recital 9.

139 See n 95.

140 In the EU, e-money is regulated under the Directive 2009/110/EC of the European Parliament and of the Council on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (e-money Directive) (2009) OJ L 267/7.

would by default be entitled to a claim[141] against the issuing institution. Specifically, subject to a contractual right, e-money and e-money tokens are redeemable at any given moment against fiat currency as legal tender at par value.

76 In this respect, MiCA further makes a specific classification of *significant* asset-referenced tokens and *significant* e-money tokens. For a crypto-asset to be considered significant,[142] a number of variables such as the underlying network's customer size, value or market capitalisation, number or value of transactions, size of reserve assets, significance of cross-border activities, as well as the interconnection with the financial system, would be decisive.

77 Furthermore, the ECB has taken a rather exclusive approach[143] by denoting a crypto-asset as "any asset recorded in digital form that is not and does not represent either a financial claim on, or a financial liability of, any natural or legal person, and which does not embody a proprietary right against an entity." With this take, the ECB seems to associate the risk profile of crypto-assets with the lack of an underlying claim or liability.

78 Whether the two-fold design of Diem would by default confer a redemption right at par value or a claim against the operating subsidiary, or the entity mandated for minting and burning Diem tokens, in favour of respective holders would play a decisive role as to the potential implications under MiCA, respectively the e-money Directive.[144]

79 Variables such as the potential customer size of the Diem network, its value and market capitalisation as well as the significance of its cross-border activities, among others, could render the project *significant* under the MiCA definition. Both Diem token models would by definition be caught under MiCA's two categories of asset-referenced tokens, respectively the e-money tokens.

80 Within the possible scope of applicability of the e-money Directive in the context of the Diem's single fiat currency stablecoins, the rules laid down in the Payment Services Directive (PSDII)[145] may also become increasingly relevant, in particular from the perspective of consumer protection as to, among others, the obligation to safeguard[146] end users' funds.[147] This obligation would be effective immediately on receipt of funds by payments institutions as well as e-money institutions.

81 In addition, it would be feasible to consider Diem under the PSDII definition of payment instrument[148] denoting a personalised set of procedures agreed between the payment service user and the payment service provider, used in order to initiate a payment order. This argument can be substantiated by the fact that the two-fold Diem design will be considered as a combination of *significant* asset-referenced and e-money tokens. As explained, the *significance* relates to the worldwide reach Diem will have based on the existing network built by its founding members. One of the consequences of this would be that with the identity management system deployed by Diem, there could be a competitive advantage in its favour in consideration of the account data portability[149] facilitated under PSDII.

82 On the other hand, any crypto-asset that would fall within the remit of the definition of a financial instrument would be subject to the EU Markets in Financial Instruments Directive (MiFID II).[150] A financial instrument[151] can take the form of, among others, a transferable security or a unit in a collective investment undertaking.

141 Ibid Art. 2(2); Art. 11; COM (2020) 593 (n 53), Art. 44.2, Art. 44.4.

142 Ibid Art. 39.1; Recital 41f; Art. 50.1; Recital 49.

143 ECB Crypto-Assets Task Force, 'Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures' (May 2019), 7f.

144 See n 140; for the latest developments see also n 13, 79.

145 Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market (PSDII) (2015) OJ L 337/35; Recitals 24-25; see also European Consumer Organisation (BEUC), 'Crypto-assets: BEUC response to the Commission's consultation' (13 May 2020), 7f.

146 PSDII (n 145), Art. 10.

147 See PSDII definition of the term 'funds' as "banknotes, coins, scriptural money or e-money within the meaning of the e-money Directive", Art. 4(25).

148 PSDII (n 145), Art. 4(14).

149 Ibid Art. 66 & 67.

150 Directive 2014/65/EU of the European Parliament and of the Council on Markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (MIFiD II) (2014) OJ L 173/349; European Commission has recently proposed a reform of the definitions of this directive in order to include those financial instruments that are issued utilising DLT; COM (2020) 596 final.

151 Ibid Art. 4.1(15).

83 Furthermore, from the perspective of the applicability of the EU anti-money laundering (AML) regime,[152] the definition of the term virtual currency becomes essential. Here, virtual currency is described[153] as a digital representation of value that is not issued or guaranteed by a central bank or a public authority, one that is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as means of exchange that can be transferred, stored and traded electronically.

84 Diem is likely to fall under the scope of 5AMLD, due to the fact that the form of attachment to "a legally established currency" would be dependent upon the governance of a private entity. Thus, any actor that provides custodial wallet services, safeguards private keys and engages in exchange services between Diem tokens and fiat currencies would fall under the category of obliged entities and be subject to due diligence, disclosure and supervisory requirements. These actors are Novi Financial and the associated designated entities, i.e. dealers and VASPs.

3. United States of America

85 In the USA, a draft federal bill was introduced in Congress, known as Stablecoin Tethering and Bank Licensing Enforcement or the Stable Act.[154] The term stablecoin[155] was defined as any cryptocurrency or other privately-issued digital financial instrument that a) is directly or indirectly distributed to investors, financial institutions, or the general public; b) is denominated in or pegged to the US Dollar (USD), or to any other national or state currency; and c) is issued with a fixed nominal redemption value, with the intention[156] of establishing a reasonable expectation or belief among the general public that the instrument will retain a nominal redemption value that is so stable as to render the nominal redemption value effectively fixed.

86 Given that the initial phase of the Diem project, once launched, would take the form of a single USD dollar-backed stablecoin, the extensive licensing regime set to be introduced by the Stable Act, if and once enacted, would therefore be relevant.

87 FinCEN has also proposed[157] implementation of stricter AML requirements for certain transactions that involve convertible virtual currency (CVC)[158] or digital assets with legal tender status (LTDA). Under the proposal, banks and MSB licensees would be required to verify the identity of their customers and keep record of transactions and counterparties in relation to transactions above certain thresholds that involve either a) unhosted wallets; or b) hosted wallets where a given transaction would be greater than USD 3,000.

88 As mentioned, Novi Financial is a US-registered MSB and would be the main user interface on the Diem network acting as a digital custodial (hosted) wallet. The Diem network would also support the integration of unhosted wallets,[159] albeit with limited threshold as to transaction volume and account address balance. FinCEN rules, if and once passed, would certainly have implications on Diem, in particular from the perspective of the network's identity management.

89 Moreover, regarding potential risks associated with DLT-based transactions involving digital asset securities, as well as custodial services in digital asset securities provided by dealers and brokers, the US Securities and Exchange Commission (SEC) has issued

152 In the EU, the anti-money laundering regime is regulated under the Directive (EU) 2018/843 of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (5AMLD) (2018) OJ L 156/43.

153 Ibid Art. 3(18).

154 116th Congress, 'Discussion Draft of 'Stablecoin Classification and Regulation Act of 2020" (19 November 2020) <https://tlaib.house.gov/sites/tlaib.house.gov/files/STABLEAct.pdf>.

155 Ibid Sec. 3(a)(aa)1.

156 Ibid "... or in such a manner that, regardless of intent, has the effect of creating a reasonable expectation or belief among the general public that the instrument will retain a nominal redemption value that is so stable as to render the nominal redemption value effectively fixed."

157 FinCEN, 'FinCEN Proposes Rule Aimed at Closing Anti Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions', Press Release (18 December 2020); Federal Register, 'Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets', Proposed Rule (23 December 2020).

158 See FinCEN's definition of the term 'virtual currency' as "a medium of exchange that can operate like currency but does not have all the attributes of "real" currency, including legal tender status; CVC is a type of virtual currency that either has an equivalent value as currency, or acts as a substitute for currency, and is therefore a type of "value that substitutes for currency.""; FinCEN Guidance (FIN 2019 –G001, 9 May 2019), 7.

159 See n 84.

a statement[160] relating to disclosure requirements in favour of customers, among others. In doing so, SEC has referred to the Rule 15c3-3[161] whereby segregation of customer securities (and related funds) would need to be ensured by dealers and brokers by maintaining physical possession or control over customer's fully paid and excess margin securities.[162] Establishing a control mechanism is particularly important in the context of digital asset securities that are issued and transferred via DLT. Such would take the form of effective maintenance of private keys and ensuring the authenticity of the recipient address prior to a digital asset transfer transaction via smart contract codes.

90 In the context of the Diem network, this control mechanism threshold would have significant implications for dealers, VASPs, and the Novi digital custodial wallet.

4. Public-Private Partnership

91 In the context of central bank[163] issued digital currencies (CBDCs)[164], these are kept specifically outside the scope of both legislative proposals, namely MiCA in the EU, respectively the Stable Act in the USA. Relevantly, the European Parliament[165] has reflected upon a need for public-private cooperation in the context of the future of money creation.

92 With reference to the concept of synthetic central bank digital currencies (sCBDCs),[166] the European Parliament takes the view that sCBDCs would have a number of advantages over CBDCs. These include[167] a) lower initial and maintenance costs, b) regulation of private stablecoin issuers by central banks, and c) lower reputational risk for central banks, given that central banks would continue focusing on their primary mandate, namely maintenance of price stability.

93 The European Parliament's stance on favouring public-private cooperation seems to tie in well with Diem's intention to eventually integrate CBDCs into its infrastructure.

D. Diem's Prospects of Trust

I. Digital Livelihoods in a "Vibrant Ecosystem"

94 If Diem's vision of *the internet of money* as a vibrant ecosystem is taken seriously, the requirements associated with it will also take on considerable significance. In this sense, digital living spaces are to be understood not only economically, but above all ecologically. What is required then, for one thing, is free and equal access to the global monetary and financial infrastructure, consequently conceived as a *public good*. And, secondly, it is of central importance to ensure the necessary trust in the functioning of the systems involved, which has a direct link to transparency in governance. From a legal perspective, therefore, what is needed is essentially the guarantee of legal certainty, the clear attribution of responsibilities, the determination of liability

160 SEC, 'Custody of Digital Asset Securities by Special Purpose Broker-Dealers' (23 December 2020) <https://www.sec.gov/rules/policy/2020/34-90788.pdf>; reference to the definition of the term 'digital asset' "...an asset that is issued and/or transferred using distributed ledger or blockchain technology ("distributed ledger technology"), including, but not limited to, so-called "virtual currencies," "coins," and "tokens."

161 Securities Exchange Act 1934, Rule 15c3-3 (Customer Protection Rule).

162 Ibid 17 CFR 240.15c3-3(b)(1).

163 Or any public authority acting in the capacity of monetary authority.

164 European Parliament, 'Public or Private? The Future of Money' Monetary Dialogue Papers (December 2019), 17, <https://www.europarl.europa.eu/cmsdata/207653/13.%20PE%20642.356%20DIW%20final%20publication-original.pdf>; "just like paper currency and coins, CBDC would be fixed in nominal terms, universally accessible, and valid as a legal tender for all public and private transactions. As with any public currency, the objective of the central bank would be that CBDC fulfil its efficiency as a medium of exchange, its security as a store of value, and its stability as the unit of account for economic and financial transactions."

165 Ibid 17f "...the main difference between CBDC and sCBDC is who maintains the end relationship with the customer: for CBDC, this is the central bank, while private entities maintain the end relationship with customers with sCBDCs."

166 T Adrian, T Mancini-Griffoli, 'The rise of digital currency' (9 September 2019) <https://voxeu.org/article/rise-digital-currency>; with reference to the proposed definition of the term 'sCBDC': "In the sCBDC model – which is a public–private partnership – central banks would go back to focusing on their core function: providing trust and efficiency by means of state-of-the-art settlement systems. The private sector – stablecoin providers – would be left to satisfy the remaining steps under appropriate supervision and oversight, and focus on their own competitive advantage – innovating and interacting with customers."

167 European Parliament (2019) (n 164),18f.

rules and, last but not least, the establishment of legal enforcement mechanisms *by design*.

95 The Diem Association justified its project with the noble goal of opening up access to financial services, especially for people in developing and emerging countries. However, this access will by no means be *free* in every respect. On the contrary, it will have its price.

96 As part of the digital, data-driven platform economy, as mentioned, Diem would contribute to an even further expansion of the Facebook empire. In Diem's single fiat currency stablecoin model, the value of which would be linked to single fiat currencies that are legal tender, identification of end users will be mandatory in numerous jurisdictions under the internationally established Know Your Customer (KYC) rules and national AML laws. In this way, mandatory legal standards would presumably help Facebook et al. to identify its now approximately 2.45 billion monthly active users and to track their business and social behaviour almost seamlessly.[168]

97 Finally, the effects of recent court decisions authorising Facebook to prohibit the use of pseudonyms[169] and thus to impose a real name requirement on its users are dramatic.[170]

98 The involuntary complicity of legislators and courts with Facebook does not only bypass privacy and data protection that is apparently considered obsolete. The consequences go much deeper, whereby the complete identification of all users and transaction information would create a comprehensive database to equip adaptive algorithms and artificial intelligence (AI) with the necessary training data and enable them to analyse, imitate and predict human behaviour. Therefore, it can be assumed that the Diem project is not primarily about building an efficient alternative financial system, but primarily about economic profit and further monopolisation of the data-driven platform economy.[171] Moreover, the suspicion is raised that Diem, as part of the digital platform economy, could be just another "colonisation project from Silicon Valley".[172]

99 Consequently, Diem's chances will depend in particular on its prospects of gaining trust as a new, alternative digital form of *private* currency alongside the established monetary systems. This would require a number of constituents, such as comprehensive accessibility and trustworthiness based on legal certainty, clear attributions of responsibility, appropriate models of liability, and effective legal mechanisms of enforceability.

II. Accessibility & Trustworthiness

100 The right to equal access to the global monetary and financial infrastructure presupposed by Diem serves not only as an individual fundamental right, but also, in an institutional sense,[173] as a necessary functional condition of social life in the digital medium. Comparable to other public goods and natural livelihoods, it presupposes the guarantee of a digital living space.

101 In order to enable action and decision making in this *bio-digital ecosystem*, it is generally necessary, as it corresponds to the *nature* of the world according to Niklas Luhmann, to stabilise behavioural expectations, i.e. to establish certainty of expectations and trust.[174] As "an elementary fact of social life",[175] trust creates the basis for "living and acting with greater complexity in relation to events":[176] "Where there is trust, there are more opportunities for experience and action".[177] In this respect, money is one of what Luhmann calls social mechanisms "that allow us to postpone decisions and yet already ensure them, that is, to live with a future of high, indeterminate event complexity".[178] Therefore, the stabilisation of such mechanisms depends on trust.[179]

168 Cf M Langer, 'Libra und des Pudels Kern' (2019) 14 IRZ 509f.

169 See n 70.

170 Higher Regional Court OLG München, Urteil vom 8.12.2020 (Az. 18 U 2822/19 Pre und 18 U 5493/19 Pre).

171 Cf Langer, (2019) (n 168), 510.

172 O Leistert, 'Hearing in the Digital Agenda Committee of the German Bundestag' (26.9.2019, hib 1052/2019).

173 Cf N Luhmann, *Grundrechte als Institution. Ein Beitrag zur politischen Soziologie* (6th ed. Berlin 2019).

174 See N Luhmann, *Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität* (4th ed. Stuttgart 2000), 1ff & 61ff; N Luhmann, *Soziale Systeme. Grundriß einer allgemeinen Theorie* (Frankfurt a. M. 1984), 179ff.

175 Ibid *Vertrauen*, 1.

176 Ibid *Vertrauen*, 18.

177 Ibid *Vertrauen*, 8.

178 Ibid *Vertrauen*, 19.

179 On the fundamental importance of trust for the stabilisation of monetary transactions, see G Simmel, *Philosophie des Geldes* (5th ed. Berlin 1930), ch. 2 III, 151ff, 164ff.

102 However, this is no longer primarily a matter of guaranteeing moral-individual trust in human persons, but rather of *system trust* in the depersonalised functionality and the regular course of communicative and technical processes. In this regard, the law has the special task of generating the necessary social trust in the functioning of information technology and, what is more, of digital institutions. Such a task can only be fulfilled by seeing the possibility of mistrust, likewise dispelling it with adequate model designs.

103 Consequently, the creation of such *socio-technical trust* is one of the most prominent objectives of the so-called DLT laws. For example, the Liechtenstein TVTG Act[180] aims "to ensure trust in digital legal communication, in particular in the financial and economic sector and the protection of users in TT Systems." The trustworthiness of DLT infrastructures does not primarily result from a central or superordinate authority, but from the reliability of the communicative operations in decentralised infrastructures themselves.

104 Hybrid tokens such as Diem's two-fold design would only have a chance of success if it is possible to guarantee a stable, uninfluenceable *source of truth* (beyond central state authorisation in accordance with financial market law)[181] using the means of distributed records. The actors involved in the network must all be able to rely on the fact that the traded crypto tokens are recognised as values in accordance with general expectations. Furthermore, they must be able to trust that all value transfer transactions are factually and legally executed.

105 In this respect, the same prerequisites basically apply to the functioning of hybrid tokens as to the *decentralising mechanism* of money in general, which Luhmann characterises in a corresponding way. According to Luhmann "the mechanism, however, presupposes for its functioning that money itself enjoys trust. The individual must be able to assume that with the money symbol he really holds in his hand the possibilities it promises, so that he can confidently postpone his decision on the final use of the money and enjoy or exploit the complexity of the possibilities represented in it as such in abstract form."[182]

106 In order to put this complexity of the economic and financial system literally into the hands of the participants, corresponding legal modelling is required in addition to technical designs. What is needed are legal models that support the trust of the participants in the sense of "trusting one's own expectations"[183] by mapping their underlying assumptions reliably and consistently, i.e. by making them legally secure.

III. Responsibility, Liability & Enforceability

107 The allocation of liability responsibilities is one of the remaining legal means by which access to the independent digital self-regulation processes can succeed in the form of an *exogenous* influence from outside.[184] As became apparent in the years following the subprime mortgage crisis, attempts to control the digital and financial sector through law have often proved ineffective, at least insofar as only single causal factors of undesirable developments have been made the object of control. Advanced legal concepts must therefore take into account the multiple dynamics, not least the diverse circumvention strategies of the actors involved in these sectors, to the extent that they focus on their "internal constitution".[185]

108 From the perspective of the new *lex cryptographia*, analyses and regulatory approaches of the financial sector come into consideration on the one hand, and, on the other, the specific inherent normativities of the relevant decentralised DLT networks are now to be included.

109 Especially against the background of the discussion in the preceding section as to the functional definition of money in economic theory, it seems apparent that the Diem hybrid tokens satisfy the three inherent constituents of money, albeit issued in the form of *private* currency. As pointed out, with regards to Diem tokens' nature as a *store of value,* such would be dependent upon the trust associated with the survivability of the Diem Reserve.

180 See n 52; the term 'TT Systems' refers to Trustworthy Technologies Systems within the meaning of the TVTG Act.

181 Cf C Zellweger-Gutknecht & RH Weber, 'Private Zahlungsmittel und Zahlungssysteme. Auf dem Weg zu neuen digitalen Geldordnungen' (2020) Jusletter 11.1.2020, paras.30ff.

182 Luhmann, *Vertrauen* (2000) (n 174), 63.

183 Ibid 1.

184 On the need for an externally compelled self-limitation of the "capillary constitution", see in particular G Teubner, *Constitutional Fragments: Societal Constitutionalism and Globalization* (Oxford 2012), 73ff.

185 See, especially with regard to financial crises, G Teubner, 'A Constitutional Moment? The Logics of "Hitting the Bottom"' in P Kjaer, G Teubner & A Febbrajo (eds.), *The Financial Crisis in Constitutional Perspective: The Dark Side of Functional Differentiation* (Oxford 2011), 3ff, 5ff.

110 Therefore, this form of *private* currency is clearly distinguished from the only forms of money creation in the traditional financial system, namely *public* and *private* money.[186] In all these forms of money in use today, there is already a lack of a separate purpose that could still convey a monetary value. Here, the value of money is derived solely from *socially constituted trust*. At the latest since the end of the binding of public money to the international gold standard,[187] i.e. the covering of banknotes issued by central banks by an adequate stock of gold reserves, it has become apparent in all clarity "how little money is bound in its innermost essence to the physicality of its substrate."[188] This early observation by Georg Simmel is also confirmed today in that money is "entirely a sociological phenomenon, a form of interaction among people". Therefore, "the more condensed, the more reliable, the more easily appealing the social connections, the purer its nature emerges."[189]

111 According to Simmel, it is "the solidity and reliability of social interactions, the consistency, as it were, of the economic circle, which prepares the dissolution of the money substance."[190] Only on this basis can the necessary confidence of economic actors emerge that in daily cash transactions they are not only dealing with pieces of mostly low-value metal alloys or paper, but can pay with them at a "nominal value" - "*non aes sed fides*".[191]

112 Today, the conditions of this confidence have long since ceased to be guaranteed unilaterally by individual state institutions such as central banks. The latter no longer obtain the cover required for the money in circulation only through corresponding gold holdings, but also, for example, through the acquisition of currency reserves, government bonds, securities or refinancing credits.[192] These means of monetary policy have proven to be precarious, especially in the recent past, which has been marked by financial crises.

113 The state as a money and value creator obviously lives on preconditions that it cannot guarantee itself. On the one hand, the central banks' large-scale open market operations are intended to serve them as indirect instruments of control in the sense of "interest rate policy", for example by providing the commercial banks with corresponding credits in the expectation of increasing the overall economic money supply.[193] On the other hand, they lead to the fact that today it is primarily the active commercial banks worldwide that are *de facto* engaged in money creation. In other words, "the widespread circulation of non-cash money in current accounts, the circulation of moneyless payment transactions, the new communication technologies, and - of particular importance - the globalisation of money and capital transactions, have prised the money-creating monopoly from the hands of the national central banks."[194] Here it becomes clear that an *intrinsic value* has long since ceased to be a prerequisite for the concept of money. On the contrary, privatised money creation has virtually developed into a "creatio ex nihilo".[195]

114 It is not possible to go into further detail here on how it comes about that these money creation mechanisms sometimes lead to fatal, crisis-like growth spirals, which are determined by harmful growth pressures, e.g. excessive growth pressures in the real economy on the one hand, and excessive speculative money creation in the financial economy on the other.[196] It should be noted, however, that in order to avoid such self-destructive growth excesses, it is important "to identify the dynamics that accelerate the growth spiral of a social sector to the point where it tips over into destructiveness by colliding with other social dynamics."[197]

115 As mentioned, the underlying value of the two-fold design of Diem hybrid tokens will be derived from the Diem Reserve, which is a reserve of fiat currencies and short-term government securities. But even with such securities, which certainly have complex risks,[198] the necessary mechanisms of currency supply control and guaranteed availability of a counter value backed by liquid assets are in principle safeguarded. The remaining risks of loss are to be reduced by means of a decentralised distribution of

186 See section C.I.

187 For a historical overview, see S Omlor, *Geldprivatrecht. Entmaterialisierung, Europäisierung, Entwertung* (Tübingen 2014), 22ff.

188 G Simmel, (1930) (n 179), ch. 2 III, 156.

189 Ibid.

190 Ibid, 155.

191 Ibid 164, with reference to such an inscription on Maltese coins.

192 Cf Langenbucher, (2018) (n 92), 385, 391.

193 Ibid.

194 See Teubner, (2011) (n 185), 6, with further references.

195 Ibid.

196 Ibid 6ff.

197 Ibid 10.

198 Cf Zellweger-Gutknecht & Weber, (2020) (n 181), para.28.

the assets to a geographically distributed network of custodian banks, which not least also spreads the associated responsibilities for risks accordingly.

116 In comparison, the establishment of the "consistency of the economic circle" in the sense of "solidity and reliability of social interactions"[199] in the crypto network appears to be conceptually more demanding. Here, beyond the *system trust* to be established technically, a fundamental *social trust* is still needed, which could not be replaced by the simple mechanics of a "crypto-proof".[200] However, the "trusted technology"[201] nature of DLT would be fundamentally misunderstood if it were to be reduced to its mathematical operations and *trust-less* characteristics as a "technology of mistrust".[202] Understood correctly, trust in DLT means guaranteeing the socio-technical conditions by means of adequate regulations in order to not only secure value and assets, but also to stabilise behavioural expectations among the acting actors. However, this cannot be achieved by means of state legislation alone.[203]

117 Legal norms should be used here to ensure that crypto tokens such as Diem establish internal self-restrictions in their technical medium that are oriented towards the aforementioned "internal constitution".[204] What this means is impressively summed up by Gunther Teubner. He stipulates that "just as in political constitutions power is used to limit power, so the system-specific medium must turn against itself. Fight fire by fire; fight power by power; fight law by law; fight money by money. Such a medial self-limitation would be the real criterion differentiating the transformation of the 'inner constitution' of the economy from external political regulation."[205]

118 Could these insights be transferred to the creation of a new crypto-constitution? How could the corresponding reflexive self-limiting mechanisms - for instance as limiting constitutional functions of a fight *crypto by crypto* - be set up? Certainly, it has to be kept in mind that money creation must not remain exposed to the unbridled addiction of the global banking market to non-cash money.[206] In this context, crypto tokens can make a productive contribution to the withdrawal of the addictive drug non-cash money by offering a better secured alternative to the *creatio ex nihilo* of current account credit.

119 However, the required security is not only guaranteed by the reserve of assets, which is always emphasised in the Diem project. A complete constitutional *crypto order* also requires the guarantee of autonomy, at least in three respects. These are a) self-regulation of the crypto sector without direct attempts at control on the part of state-institutionalised politics, b) avoidance of one-sided ties to individual forms of value or money of other monetary systems, and c) independence from individual technical operators as well as the infrastructure of social networks set up behind DLT.

120 This would by no means signify leaving the crypto sector to its own devices and placing it in a normatively unregulated state of total anonymity. No one needs to fear being afflicted by the "spectre of crypto anarchy"[207] as long as cryptographically generated value also lives up to its function as a *public good* and justifies the trust that must be presupposed. In addition to the stabilisation of value through an appropriately distributed reserve, this includes a further stabilisation of expectations through reliable allocation of responsibility and liability as well as corresponding enforcement possibilities vis-à-vis the various participating entities of the network.

121 It should be noted that this does not render the abolition of user anonymity. As mentioned, it is not clear as to whether Diem will be set up in the form of an *account-based* private currency issuance, respectively *token-based*. The original advantages of the token-based model could be maintained with the help of identity management that only ever reveals the partial identity of the *data person*, and only within the limited scope of a given transaction. Furthermore, responsibilities can be specifically linked to the corresponding roles of the (non-anonymous) responsible parties and collectives involved in the DLT network.

122 In the Diem network, the Diem Association has

199 Cf Simmel, (1930) (n 179), 155.

200 Cf Langenbucher, (2018) (n 92), 395, with particular reference to N Dodd, *The Social Life of Money* (Princeton & Oxford 2014), 362ff.

201 See n 52 & 180.

202 Cf Dodd, (2014) (n 200), 362; see also n 50.

203 A different view is held by Langenbucher, (2018) (n 92), 395, who sees the success of virtual currencies as "dependent on the societal-state underpinning of trust".

204 See also Teubner, (2011) (n 185), 15: "The task would, with a bit of luck, be to combine external political, legal and social impulses with changes to the internal constitution."

205 Ibid17.

206 See Teubner, (2011) (n 185), 16 ff, with resolute demands for a restoration of the money creation monopoly of the central banks.

207 Cf TC May, *The Crypto Anarchist Manifesto* (1988) <https://www.activism.net/cypherpunk/crypto-anarchy.html>.

been mandated with the general governance of the project. Its subsidiary Diem Networks US, Inc. could be seen as a "collegial institution" as it has been licensed and registered as a MSB by FinCEN, taking the primary operating role of the project at least during the project's initial phase.[208] As such, it could act as a "reflection centre", comparable to central banks in fiat money, in order to advance self-regulation in the sense of the self-rationality and self-normativity of the Diem network and to make it compatible with society.[209] However, this still requires a clear commitment to the function of the new monetary value as a *public good*, i.e. the decisive recognition of the users and other actors involved in Diem as the *public*. This does not mean, of course, that monetary value creation has to be a state matter at the same time. Rather, it belongs in the "public infrastructure of the economic sector" and is a "genuine component of the constitution of the economy because it takes part in determining the public function of the economy".[210]

123 The success of Diem will then depend above all on the extent to which it succeeds in providing forms of expectation, stabilisation and trust with liability and legal protection mechanisms set up specifically in the network, in order to do the best possible justice to the many participants in the network. At least at the beginning of the Diem project, trust will only be granted under legal conditions. This succeeds all the better as corresponding risk assumptions would be legally anchored in the form of liability guarantees. For Diem in particular, it will be crucial to define technical spheres of responsibility within clear boundaries. New liability constructions are required above all where no individually responsible person can be identified, because he or she no longer has sole control over the technical risks in the interplay of powerful artefacts and processes, i.e. where no individual can be expected to take a risk and bear responsibility for it.

124 For this reason, collective risk liability concepts corresponding to the associated network of risk-impacting actors and agents will increasingly come into consideration in the future.

125 What has to be considered then, are models of strict liability of the corresponding risk associations, which are composed, in particular, of the operators as jointly liable according to fixed shares. With its rather complex organisational structure, and as described in the preceding sections, the assignment of operating roles to the actors involved in Diem does not seem straightforward.

126 Overall, at least three spheres of responsibility come into view in Diem's case as far as can be seen from the current state of project planning. Each of these spheres is likely to be associated with different implications under liability law. These include a) *individual liability* of single corporate actors (e.g. designated dealers, VASPs, operators), primarily on the grounds of provable individual misconduct; b) *shared network liability* of validator nodes; and c) *collective fund liability*, governed by Diem Association with Diem Reserve managed by a network of worldwide institutional custodians.

127 Irrespective of how these spheres of risk and responsibility are ultimately structured in terms of liability law, it can at least be stated in general terms that suitable liability models should rely less on individual incentives for lawful behaviour or, in other words, less on negative (monetary) incentives through the threat of damages or compensation for infringing actions.

128 Instead of focusing on acting individuals, liability must also be directed primarily towards the risks of the socio-technical connections in whose interaction infringements of rights occur.

129 Liability responsibility is then no longer primarily based on culpable-causal acts of infringement, but on "infringement structures" that result from socio-technical connections in the sense of "risk associations".[211]

130 In this way, the multitude of damage risks[212] can finally be addressed in a differentiated manner, in particular the possible losses and damage as a result of price or monetary inflation, payment deficits, scarcity of currency, loss of liquidity, but also damages due to violations of the law through data protection breaches, money laundering, criminal financing or fraudulent activities.

131 But even in this respect it remains the case that

208 See Zellweger-Gutknecht & Weber, (2020) (n 181), paras.78ff; for the latest developments see also n 13, 79.

209 Cf Teubner, (2012) (n 184), 24.

210 Ibid 36.

211 For an exemplary legal reconstruction of different forms of risk associations on social networks and trading platforms, see M-C Gruber, 'Legal responsibility of AI in social media and algorithmic trading' in M Jankowska, M Pawełczyk & M Kulawiak (eds.), *AI: Law, Philosophy, and Geoinformatics* (Warsaw 2015), 90ff, 99ff.

212 For an in-depth consideration of these risks, see in particular Zetzsche, Buckley & Arner, (2017) (n 105); cf also DA Zetzsche, RP Buckley & DW Arner, 'Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses' (2019) 47 UNSWLRS, 10ff <https://ssrn.com/abstract=3414401>.

state law cannot directly bring about the changes necessary for enforceability in the information technology medium. It cannot determine, control or regulate the normative orders of the *internet of money*. The internet regulates itself. However, this self-regulation of information technology has its limits. In those cases in which, from an internal perspective, seemingly insoluble conflict situations arise between providers and users, so that the necessary trust in the functioning of information technology and even of the institution of information law appears threatened, the specific conflict resolution power of the law is required. Legal enforcement mechanisms ideally provide media feedback that serves the further development in the sense of a constantly improved *compliance by design*,[213] which also includes the well-known concept of *privacy by design* in favour of the users.[214] Furthermore, corresponding enforcement concepts of *liability by design* could be considered, which could be directly inscribed in DLT.

132 The clear allocation of responsibilities to the various actors, as well as the corresponding allocation of liability obligations and their enforceability, can become an existential question for DLT-based crypto tokens such as Diem.[215] To solve this, an identity management system would also be required which would meet legal requirements by technical means. Furthermore, such an identity management system would lay the foundation for technical isolation of the formal content of transaction data from the personal aspect of that data, with individuals and end users given the chance to control what to share, how much and for how long.

E. Identity Management

I. Digital Identification & Representation

133 Digital identification and representation lie at the core of a financial infrastructure operated on DLT, in particular when the primary aim of such an infrastructure is to bring about financial inclusion.

134 Identification is defined as "a process of recognising an entity in a particular domain as distinct from other entities."[216] Identification is seen as an essential process when requesting or accessing a service of any kind. While identity is "a set of attributes related to an entity,"[217] digital identity could simply be defined as "the digital representation of an entity detailed enough to make the individual distinguishable within a digital context."[218]

135 In the absence, and limited uptake of, effective standardisation as well as interoperability among diverse systems, digital identity has continued to be a fragmented development,[219] with pressing issues relating, among others, to security.

136 Digital identity management systems could in principle take various forms among which are centralised, federated, third party identity provider, user-centric and, more recently, self-sovereign identity (SSI). An identity provider[220] is "an entity that makes available identity information." Such information includes not only the creation, maintenance and management of credentials but also the provision of authentication services.[221]

137 With the consumer single sign-on (SSO) identity management of Facebook and its group of social network platforms, the data protection and privacy of end users seemingly remain untested. In the absence of an effective and secure identity management system, Diem, as a digital financial infrastructure, may further aggregate the risk of profiling end users' behaviour online by expanding the scope of reach to payment systems and spending patterns.[222]

138 Facebook's SSO is a common method of authentication of user logins whereby users could utilise their Facebook credentials and connect to other third party service providers. Such a scheme would argu-

213 For a similar concept of "embedded regulation", see DA Zetzsche, DW Arner & RP Buckley, 'Decentralized Finance' (2020) IIEL Issue Brief 02/2020, 51ff <https://ssrn.com/abstract=3539194>.

214 Cf Gruber, (2015) (n 121), 203.

215 Cf Enz, (2020) (n 98), 297.

216 International Organisation for Standardisation (ISO), 'IT Security and Privacy – a framework for identity management – part I: Terminology and concepts' (2019), ISO/IEC Standards No 24760-1.

217 Ibid.

218 International Telecommunication Union (ITU), 'Digital Identity Roadmap Guide' (2018), 4f.

219 See also EU Blockchain Observatory and Forum, 'Thematic Report: Blockchain and Digital Identity' (2019).

220 See n 216.

221 MA Lopez, 'The Future of Identity: Self Sovereignty, Digital Wallets and Blockchain' (2020), LACChain Global Alliance digital identity working group, 16ff.

222 See also Zetzsche, Buckley & Arner, (2019) (n 212), 22ff.

ably[223] increase the risks associated with the creation of a single point of failure. Facebook could therefore be seen as an identity provider with both centralised and third party provider management forms,[224] the latter in the context of Facebook's provision of authentication services through its SSO method.

139 In this respect, the Diem Association is committing itself to a long-term goal of developing and promoting an open identity standard,[225] pointing to *decentralisation* and *portability* of digital identity as prerequisites to financial inclusion and competition.

140 Here, decentralisation would mean that identity data of users, their attributes and identifiers, would be distributed among the running nodes of the Diem DLT network. Portability would mean that credentials and attributes could be moved from one place to another. Neither of these[226] would necessarily imply that users are to maintain effective control over the creation and management of their digital identities and representations. Notably, and in contrast with the open identity standard promoted by the Diem Association, the nodes running on Diem's permissioned DLT network would constitute a rather centralised structure.

141 As previously pointed out, Facebook's Novi as the digital custodian wallet would serve as the main user interface for the Diem network upon which services would be built based on smart contract codes. Novi as a hosted wallet will arguably function as an off-ledger payment mechanism with an obligatory identification system in place, called visual identification. Moreover, only those smart contract codes would be appended on the Diem network that would be pre approved by the Diem Association. The network would allow for pseudonymisation as part of its participation protocol, whereby users would be enabled to hold multiple accounts, which would in return avoid the risk of correlation as to users' activities and profiles. On the other hand, as mentioned, the underlying DLT is set to take the form of a single data structure which would record the history of transactions and states over time, providing for the possibility that all appended data on the network would in theory be visible to all applications.

142 One of the main objectives of Diem Networks as a subsidiary of the Diem Association was the provision of identity management. Furthermore, user interactions on the network would primarily take place through VASPs. These regulated entities would be bound by the travel rule as to beneficiary information disclosures, and would be permitted to record user transactions off-ledger and internally, presumably in their respective central databases.

143 In light of these developments, it would not be far-fetched to take the view that the identity management of Diem may not be of a nature to provide for an effective control in favour of end users as to the creation, management and sharing of their digital representations. Instead, despite the intended application of pseudonymity by the Diem project, going in clear contradiction with the role assigned to VASPs and the travel rule they are bound by, the establishment of correlation between such identifiers and real identities of end users, as well as network participants, would seem inevitable. This rhetoric seems to also tie in well with the growing pressure on social network platforms as to the identification of their users, particularly demonstrated in a recent German higher regional court's decision[227] to authorise Facebook to ban the use of pseudonyms on its platform.

144 Moreover, with regards to the *portability* element of the digital identity standard, put forward as a long-term goal by the Diem Association, such would involve cross-border transactions, including within the EU. Under PSDII,[228] explicit (contractual) consent from payment service users would be in principle required in order to request and obtain access to their transaction data and payment accounts with banks and financial service providers. This would serve relevance to the Diem project, in the context of smart contract code –enabled automated decision making, concerning user transaction data. Under the EU's data protection regime,[229] transaction data would be considered personal data where such information would be attributable to an independent individual. Transaction data could lawfully be processed[230] when necessary for the performance of a contract to which a data subject (payment services user) is a party. Furthermore, lawful processing of transaction data could be justified when necessary for compliance with a legal obligation,[231] laid down

223 See also LH Newman, 'Think Twice Before Using Facebook, Google, or Apple to Sign in Everywhere' (*Wired*, September 2020).

224 See Lopez, (2020) (n 221), 17f.

225 Libra whitepaper v.2.0 (n 32), 25.

226 See also I Allison, 'Buried in Facebook's Libra Whitepaper, a Digital Identity Bombshell' (*Coindesk,* 26 June 2019).

227 See n 170.

228 PSDII (n 145), Art. 64, 66 & 67.

229 See GDPR (n 70).

230 Ibid Art. 6(1)b.

231 Ibid Art. 6(1)c.

by EU law, respectively by the laws of Member States (MS) to which a data controller is subject, among which would be the requirements of the AML regime.

145 As seen, the notion of identity, in particular digital identity, clearly touches upon the legal and regulatory landscape in many respects. In the EU, next to the data protection regime, electronic identification and authentication is regulated under eIDAS[232] which, among others, recognises the use of digital signatures[233] for cross-border electronic transactions. Based on the principle of legally enforceable mutual recognition[234] between MS, eIDAS ensures interoperability by obliging public online services to recognise national electronic identification schemes for authentication purposes. Such has remained voluntary for private online services. With recent developments,[235] which particularly aim at extending the scope of application of eIDAS to the private sector, an EU digital identity scheme (EUid) is set to be introduced. EUid would act as a single sign-on, albeit entirely voluntary, harmonising access to online public and private services, and in principle facilitating anonymous authentication.[236] It is apparent that the relationship between personal identity and authentication[237] mechanisms is becoming increasingly important. In this respect, therefore, any entry appended on DLT would fall under the eIDAS definition of 'electronic document'.[238]

146 Under Swiss law, on the other hand, the Swiss banking sector is subject to compliance with FINMA rules[239] pertaining to the handling of electronic client data in order to ensure confidentiality. Moreover, the Swiss draft eID Act[240] was set to derogate from the traditional issuance of digital identities being conferred to state authorities only, permitting public-private partnership collaborations. In other words, the state would take the role of the issuer and verifier of attributes, whereas the task of authentication of eIDs would be given to the private sector under state supervision. The eID was seen as the key infrastructure element on which further digital services such as, among others, eBanking and eFinance could then be built.

II. A Possible Way Forward: Taxonomy & Basic Definitions

147 The notion of trust as one of the central constituents of almost all industries, including digital financial services, is increasingly transitioning away from purely centralised intermediation by state authorities. As mentioned, in increasingly digitalised societies, the stance of trust as an elementary fact of social life has seen a shift towards augmented reliance on private sector actors.

148 In case Diem is to be eventually rolled out as a private cross-border infrastructure with the alleged aim of ensuring financial inclusion, it is inevitable that the

232 Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eIDAS) (2014) OJ L 257/73; ibid Art. 3(1): "electronic identification means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person"; ibid Art. 3(5): "authentication means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed".

233 See n 41; eIDAS (n 232) recognises 3 different signatures according to the degree of legal certainty which can be provided. As stipulated in Art. 3(10), (11) & (12) these are 'simple', 'advanced' and 'qualified' signatures.

234 eIDAS (n 232) Art. 6.

235 European Commission, 'Inception Impact Assessment for Revision of the eIDAS Regulation – European Digital Identity (EUid)', Ares (2020) 3899583 <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=cellar:35274ac3-cd1b-11ea-adf7-01aa75ed71a1>; European Commission, 'Proposal for a Regulation amending Regulation (EU) 910/2014 as regards establishing a framework for a European Digital Identity, COM (2021) 281 final.

236 For example, in cases where user identification is not required for the provision of services.

237 For a complete overview of eIDAS see IA Domingo (on behalf of European Commission), 'SSI eIDAS Legal Report: How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market' (2020) <https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf.>.

238 eIDAS (n 232) Art. 3(35): "electronic document means any content stored in electronic form, in particular text or sound, visual or audio visual recording"; ibid Art. 46 on legal effects of electronic documents: "an electronic document shall not be denied legal effect and admissibility in legal proceedings solely on the grounds that it is in electronic form".

239 KPMG, 'FINMA circular 2008/21 Operational Risks – Banks' (2014), Appendix III, 27.

240 Federal Act on Electronic Identification Services "eID Act/E-ID-Gesetz, BGEID" <https://www.admin.ch/opc/de/federal-gazette/2019/6567.pdf>; note: on the Referendum of 7 March 2021 the Swiss electorate rejected the proposal by 64.4%.

identity management scheme of the project requires a design that would ensure end users maintain an effective and sovereign control over their digital representations on the network.

149 As a result of technological advancements, reliance on third party public or private intermediaries for the provision of verification and validation services, in particular in the context of identity creation and the management of attributes, claims and credentials, could in principle become redundant. Disintermediation in the provision of identity services could therefore place individuals in the driving seat as identity providers.

150 Labelled as self-sovereign identity (SSI), this mechanism could be defined as a "digital movement that recognises an individual should own and control their identity without the intervening administrative authorities. SSI allows people to interact in the digital world with the same freedom and capacity for trust as they do in the offline world."[241] An SSI based identity management would imply a set of inherent principles.[242] These include a) access, b) consent, c) control, d) existence, e) interoperability, f) minimalisation, g) persistence, h) protection, i) portability, and j) transparency.

151 In other words, individuals (and entities) as the sole controllers of their digital identities must have access to their own data, exercise control and agree to its usage. The created identities must be long lived, widely available, usable and transportable. The rights of individuals must be preserved, respectively data disclosure must be minimised and done selectively on a *need-to-know* basis. The systems and infrastructures upon which SSI is built would need to be open and transparent as to their operation and management.

152 In this context, individuals (and entities) as their own identity providers are referred to as principal, subject or holder.

153 Central to the functionality of SSI architecture are decentralised identifiers (DIDs). A DID[243] is defined as a new type of globally unique identifier specification that is portable and rooted in a public source of truth such as DLT, a database, a distributed file system or a similar system. Such specification does not require a centralised authority to create, register, resolve, update or revoke the identifiers.[244] Ownership of DIDs could be authenticated and verified cryptographically, i.e. via digital signatures.[245]

154 As identifiers, DIDs do not carry information about the principal. Every DID is accompanied by a descriptor object known as a DID document or DDO. DDO is a machine readable document containing information about verification keys and proof of ownership of the associated DID, among others. Moreover, DID Methods are mechanisms by which a particular DID and its associated DDO is created and resolved.[246] Notably, DIDs are not always dependent on a DLT protocol for their creation. Depending on method specifications, DIDs could take the form of DLT agnostic, yet in principle interoperable with DLT infrastructures,[247] such as peer DIDs.[248] Peer DIDs could be "created and maintained for an entire lifecycle without any reliance on the internet, with no degradation of trust."[249]

155 Given that the principal or the subject would maintain control over the creation of their DIDs, it is in principle possible that multiple DIDs are generated by one principal or subject for different relationships, in turn providing for correlation resistance in the context of their digital representation.

156 DIDs could technically be created in different formats,[250] namely anywise, pairwise and N-wise DIDs. Anywise DID could be used with an unknown

241 Sovrin.org, 'What is self-sovereign identity?' (2018) <https://sovrin.org/faq/what-is-self-sovereign-identity/>.

242 C Allen, 'The Path to Self-Sovereign Identity' (2016) <http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html>; see also n 221, 26ff.

243 W3C, 'Decentralised Identifiers (DIDs) v1.0, Core architecture, data model, and representations' (2021), Working Draft 20 January 2021 < https://www.w3.org/TR/did-core/>.

244 R Soltani et al., 'A New Approach to Client Onboarding using Self-Sovereign Identity and Distributed Ledger' (IEEE Int. Conf. on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018), 1131ff.

245 See n 44.

246 See n 243.

247 This process is known as 'grafting'; in other words "...because peer DIDs are globally unique at the moment of creation, their numeric basis will not exist on any other blockchain unless someone copies it there. Blockchain-based DID methods can therefore (redundantly) register a peer DID doc using their own method."

248 W3C, 'Peer DID Method Specification, blockchain-independent decentralised identifiers' (2020), W3C Document 25 August 2020 <https://identity.foundation/peer-did-method-spec/#overview>.

249 Ibid.

250 Ibid.

number of parties, while pairwise DID would be used only between the principal and one other party. In N-wise format, the number of parties could be defined in accordance with a given context.

157 As mentioned, DIDs could be created via different method specifications defined in DID Methods. In order to ensure interoperability among these specifications, certain recent developments are of significance, namely the Universal Resolver[251] tool as a unified interface upon which any kind of DID could in theory be resolved.

158 With respect to the SSI identity management, DIDs are components of a larger picture. Here, claims and credentials play a crucial role as to individuals' digital representations and attributes. A claim[252] is defined as "an assertion made about a subject", and a credential is "a set of one or more claims made by an issuer." Credentials could be verifiable, self-asserted, as well as anonymous.

159 A verifiable credential is a data structure that is "tamper-resistant and cryptographically verifiable." In self-asserted credentials, the issuer is the same as the principal or the subject, whereas verifiable credentials are issued by a trusted third party entity

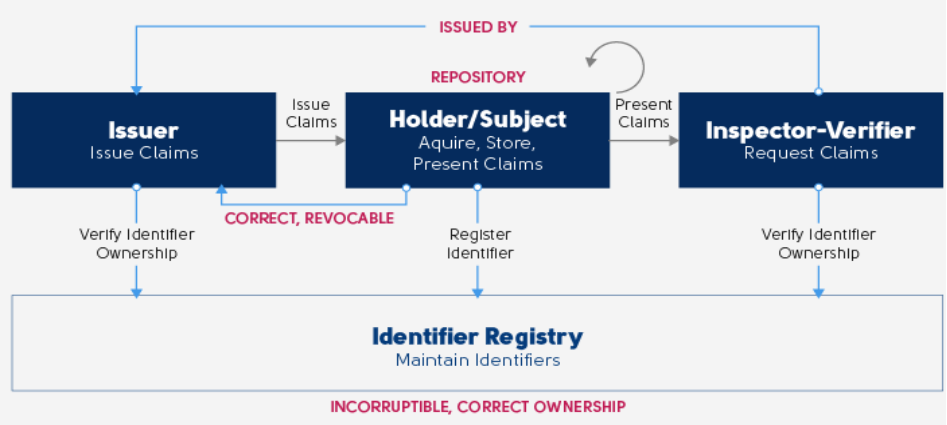

Figure ii: credit: www.luxoft.com/blog

such as a bank or a financial institution. Anonymous credentials[253] refer to data structures created through the means of an algorithmic protocol called zero knowledge proof (ZKP), whereby claims are proven without revealing additional information. This would arguably in return help maintain anonymity by not revealing the underlying identity related data.

160 In a simplified equation, there would be three parties, namely the principal or the subject, the issuer and the verifier. The communication between these parties would be facilitated through software programmes called user agents.[254] Both issuer and verifier are entities mainly responsible for the issuance of credentials requested from them and the reception of credentials presented to them.[255]

161 Verifiable data registry[256] is an underlying system upon which created DIDs are verified and exchanged between parties alongside verification keys and verifiable credential schemas. The Verifiable data registry could be based on a DLT network. Relevantly, a repository is a programme such as a storage vault or wallet which enables the storage of, and secure access to, the verifiable credentials of a principal or subject. Notably, verifiable credentials could be revoked by issuers, respectively deleted by principals or subjects.[257]

162 Digital representation of these actors would be facilitated and secured through encryption schemes such as asymmetric encryption or public key infrastructure (PKI). PKI provides for assignment of key pairs, public and private, to a principal or a subject, with public key being publicly visible and private key remaining under the control of the said principal or subject with which digital signatures would be generated for authorisation and validation

251 M Sabadello (on behalf of DIF), 'A Universal Resolver for self-sovereign identifiers on any blockchain or other decentralised system' (2017) <https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c>.

252 W3C, 'Verifiable Credentials Data Model 1.0, Expressing verifiable information on the web' (2019), W3C Recommendation 19 November 2019 < https://www.w3.org/TR/vc-data-model/#dfn-credential>.

253 See n 244, 1131ff.

254 See n 252.

255 Ibid.

256 Ibid.

257 Ibid.

purposes. In a PKI infrastructure, the identifier registry is generally managed by a centralised third party such as a certificate authority (CA), who can revoke certificates at any point in time, potentially increasing risks associated with a single *point of failure*. To address this, decentralised public key infrastructure (DPKI)[258] has been developed, whereby the identifier registry takes the form of key value data stores appended on a DLT network or similar systems. DPKI would allow for the principal's identifier to be securely linked to its associated public key.

163 In digital finance, strict KYC and AML requirements make the choice of the identity management mechanism pivotal to the functionality and operation of a given network. Through the means of uniquely assigned DIDs and verifiable credentials, an interoperable and standardised SSI mechanism would facilitate the portability of credentials leading to cost and process efficiency.

164 Furthermore, the personal data protection regimes in the EU, and that of Switzerland, pave the way for a more strict view of digital identity rights of individuals. Here, the principles governing SSI identity management seemingly correspond with the principles introduced by legislation such as, among others, the EU's General Data Protection Regulation (GDPR).[259] These include a) data processing in a lawful, fair and transparent manner, b) purpose limitation, c) data minimisation, d) data accuracy, e) storage limitation, f) data integrity and confidentiality, and more importantly g) data portability, to name a few.[260]

165 Consequently, it is only feasible that a large scale *private* digital financial infrastructure such as Diem implements an effective identity management mechanism, whereby individuals and end users are no longer seen as mere products or an extension of their digital footprints already created elsewhere. Technological developments allow for integration of mechanisms that would in principle limit the ever present collateral damage that is induced on end users by increasing digitalisation in societies.

166 An operational Diem network would be realistic as a complementary financial infrastructure only if its identity management system would provide for the integration of a secure and interoperable SSI mechanism where risks associated with profiling and correlation are minimised and individuals would maintain effective control and confidentiality in relation to their financial and spending behaviour.

F. Concluding Remarks

167 Diem is yet to become formally operational. Any analysis of its technical design and governance infrastructure would therefore need to be solely based on available information to date. Nevertheless, the Diem test network,[261] published late January this year, already documented the interaction of a significant number of addresses with unique identifiers on the network.

168 Diem aims at becoming an alternative worldwide system for digital finance, run and operated on DLT, in order to deliver on the promise of *the internet of money*. A breakdown of Diem's organisational infrastructure revealed that through the bundling of in-house software applications with Facebook's core products, the dynamics of user dependency would inevitably emerge, with Facebook maintaining a certain degree of (indirect) governance and effective control over the project. As argued, the aggregated risk of such a project could render further monopolisation of the data-driven platform economy, potentially leaving its primary purpose as an (efficient) alternative financial system in the cold. Furthermore, due to Diem's anticipated worldwide reach and its projected identity management system, the extent of the network's technological foundation, and its capacity to meet the regulatory obligations of different jurisdictions, in particular in the EU in consideration of the user account data portability facilitated by PSDII, a significant competitive advantage in favour of Diem would then be established. This would be even more prevalent once sCBDCs are introduced positioning Diem in a leading role in the dedicated public-private partnerships.

169 By taking a closer look at the *substance* of the two-fold Diem design and the associated legal implications, it seemed feasible to assume that the design would by definition embed a hybrid nature. Next to regulatory hurdles, as pointed out, the success of Diem will depend above all on the extent to which it succeeds in providing stability and trust with liability and legal protection mechanisms set up specifically in the network. Moreover, an identity management system would need to be in place, effectively meeting legal requirements by technical means. Such a system would then lay the foundation for technical isolation of the formal content of transaction data from the

258 C Allen et al., 'Decentralised Public Key Infrastructure, A White Paper from Rebooting the Web of Trust' (2015) <https://github.com/WebOfTrustInfo/rwot1-sf/blob/master/final-documents/dpki.pdf>.

259 See n 70.

260 See n 244, 1134f.

261 See <https://indiem.info/top#top=balance>.

personal aspect of that data, with individuals and end users given the chance to control what to share, how much and for how long.

170 In other words, for Diem to experience a realistic mass adoption and to serve as a complementary infrastructure to the established monetary systems, it must itself prove to be a constitutive part of the *lex digitalis*. Evolving into the *lex cryptographia*, it will depend on the *pouvoir constituant* of the digital world whether it succeeds in further developing a digital civil constitution in the medium of DLT. Such a constitution, not least with its respective identity management, will determine what human life will be like in a truly *vibrant ecosystem*.

Note: URL links have primarily been accessed within the period of 01.12.2020 - 09.02.2021, excluding those related to Diem's latest developments.