Towards CBDC-based Machine-to-Machine Payments in Consumer IoT

Towards CBDC-based Machine-to-Machine Payments in Consumer IoT

Nadia Pocher*
Universitat Autònoma de Barcelona
Law, Science and Technology RIoE EJD
nadia.pocher@uab.cat

Mirko Zichichi*
Universidad Politécnica de Madrid
Law, Science and Technology RIoE EJD
mirko.zichichi@upm.es

ABSTRACT

The technological advancement of the Internet of Things (IoT) is a well-known phenomenon that mainly affects industrial sectors but also consumers in everyday life. The use of Consumer IoT, *i.e.* CIoT, devices is increasing, and they are paving the way for a Machine-to-Machine (M2M) communication that could highly enrich consumer services. In this paper we position ourselves in the narrowing gap between the world of CIoT and the world of money, and we explore the emerging interaction between the payment needs of a M2M Economy and the "new ways of payment". Indeed, the advent of Distributed Ledger Technology and cryptocurrencies has introduced a tech-oriented dynamism in the monetary and financial sphere. Accordingly, central banks all over the world have started investigations into digital fiat money , *i.e.*, "retail" Central Bank Digital Currencies (CBDCs). Against this backdrop, we analyze the integration of retail CBDC models into M2M and CIoT dynamics, while heeding regulation-by-design and compliance-by/through-design methodologies, and we propose a preliminary model of integration between a two-tier retail CBDC architecture and CIoT.

CCS CONCEPTS

• **Networks** → **Peer-to-peer networks**; • **Applied computing** → *Law*; *Economics*; • **Human-centered computing** → **Ubiquitous and mobile devices**;

KEYWORDS

Central Bank Digital Currency, Machine-to-Machine, Internet of Things, Distributed Ledger Technologies

ACM Reference Format:
Nadia Pocher and Mirko Zichichi[1]. 2022. Towards CBDC-based Machine-to-Machine Payments in Consumer IoT. In *The 37th ACM/SIGAPP Symposium on Applied Computing (SAC '22), April 25–29, 2022, Virtual Event, .* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3477314.3507078

*This work has received funding from the EU H2020 research and innovation programme under the MSCA ITN European Joint Doctorate grant agreement No 814177 Law Science and Technology Joint Doctorate - Rights of the Internet of Everything.

SAC '22, April 25–29, 2022, Virtual Event,

ACM ISBN 978-1-4503-8713-2/22/04…$15.00
https://doi.org/10.1145/3477314.3507078

1 INTRODUCTION

At the end of 2021, swift societal digitization is hardly an unfamiliar concept. Over the past decade, Industry 4.0 has brought into our lives daily interactions with objects that use connectivity to provide a variety of services. In this respect, Consumer Internet of Things, or CIoT, is an interconnected system of digital devices whose use is steadily increasing by more and more consumers on a personal basis [30]. These "smart" devices range from wearable watches to voice assistants in our home, from smart vehicles to e-health devices. CIoT items are ubiquitous, and their market is expanding alongside their applications. Meanwhile, the advent of blockchain technology, cryptocurrencies, and more recently DeFi, has introduced another kind of tech-oriented dynamism in the financial and monetary sphere. Against such a backdrop of FinTech advancements, central banks all over the world have started investigations into digital fiat money, designed to be used by the general public, *i.e.*, "retail" Central Bank Digital Currencies (CBDCs) [5, 32].

While (C)IoT comprises interactive e-devices, Machine-to-Machine (M2M) techniques allow them to communicate, or relay information, over a protocol [35]. The integration of M2M and IoT provides invaluable services to humans, and a future may be envisioned with "smart" machines (inter)acting autonomously from an economic perspective [36]. Such a "M2M economy" is decentralized and based on the autonomy of its participants (*i.e.*, machines) Accordingly, studies have addressed the benefits of integrating DLTs/blockchain into (C)IoT projects [38]. While DLTs can improve scalability [9], smart contracts can increase efficiency and security in M2M communication by predefining conditions for data and value/asset transfers [38]. Arguably, DLTs and programmability enable the "M2M economy" to reach its full potential. Among the challenges arising from e-devices exchanging data and services without (or with limited) human intervention [36], the need emerges for them to handle payments [30]. In this way, M2M services could be billed as per the actual use [34], through very small transactions – *i.e.*, micro-payments – performed on an automated basis.

In this work we focus on retail CBDC research, in light of the narrowing gap between the world of e-devices and the world of money, whilst also considering the emerging interaction between the payment needs of (C)IoT and CBDC models. The integration of native digital fiat money into M2M dynamics may unlock a novel layer of socio-economic synergy, but also generates a variety of regulatory questions. While this contribution does not pursue a comprehensive account, it explores the deployment in CIoT projects of (i) regulation-by-design and compliance-by/through-design methodologies, (ii) decentralized infrastructures from a privacy and data protection perspective, to provide (iii) a preliminary model of integration between a two-tier retail CBDC architecture and CIoT.

Our intention is to put forward a specific proposal, among the many possible for CIoT and M2M payments. We exploit the use of DLT, albeit a CBDC is not necessarily based on this technology.

In developing this work we heed the following assumptions:

(1) As this paper investigates the interplay between CBDC models and CIoT, the focus is on *retail* CBDCs.
(2) We acknowledge not all CBDC models are DLT-based. Nonetheless, in our work we focus on DLT-based architectures.
(3) With regard to the integration between DLTs and M2M, we only address the M2M Economy from a payment standpoint.
(4) We do not address the security issues of CIoT devices. For our purposes, we assume it is guaranteed by design.
(5) We apply a context-neutral approach (*i.e.*, not jurisdiction-specific), and we place our arguments at a principle-level.
(6) Albeit the integration of CBDCs and (C)IoT generates many regulatory challenges, our objective is not to survey them.
(7) We do not address specifically the interplay between CIoT and cross-border CBDC interoperability.

The remainder is structured as follows. Section II offers background information and problem assumptions, while Section III the interplay between M2M , DLTs and payments. Section IV addresses the possible implementation of a CBDC-based retail M2M economy and its related regulatory questions. Section V explores the integration of CBDC and CIoT and Section VI concludes the paper.

2 BACKGROUND

2.1 Consumer Internet of Things and Machine-to-Machine Communication

The Internet of Things (IoT) can be seen as a people-to-people, people-to-things and things-to-things exchange of information via the Internet, for the purposes of providing personalised services such as smart homes, smart healthcare and smart transport to IoT system users [28]. The term Consumer IoT (CIoT) refers to the subset of smart devices and IoT systems that are (to be) used by individuals, for the sake of their convenience or lifestyle. They are opposed to smart machinery and systems designed for the benefit of factories and industries, labeled as Industrial IoT[30]. CIoT has a variety of applications in homes. Examples include surveillance, multimedia streaming and sharing, energy management systems for smart grid and healthcare. In the last few years, IoT is standard consumer electronics such as TVs, fridges, switches, bulbs, speakers, etc. Further, most CIoT devices can operate in mobility via cellular networks, *i.e.*, vehicle-to-vehicle applications, wearable devices, logistics and e-health are also enabled by M2M communication [3].

M2M refers to communications, without or with limited human intervention, between computers, embedded processors, smart sensors, actuators and mobile devices [15]. M2M suits applications such as security monitoring, vehicle theft protection, car sales, mechanical maintenance, transport management and many other smart city solutions in combination with IoT. Data can be transmitted via cable, wireless channel, mobile communication or other means [35].

2.2 Distributed Ledger Technologies

The opportunities created by the applications of DLTs are plentiful. The possibility to record information in an open, distributed and secure ledger shared among multiple parties efficiently and verifiably expressed a disruptive socio-economic change. In this respect, a distributed ledger is "*a type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner*" [26]. DLTs are cryptographically guaranteed to be tamperproof and unforgeable, and enable groups of nodes – *i.e.*, devices/processes participating in the network – to agree upon and record information without the need to rely on a trusted central authority. The use of Smart Contracts allows to employ DLTs to operate well beyond just currency transactions. Smart Contracts are instructions stored in the blockchain and automatically triggered once the default condition is met. For instance, the creation of smart services, based on Smart Contracts, may enable users to interact with devices/vehicles in smart transportation systems or to favor interoperability among devices and resources of smart cities [19, 44].

In light of the inherent features of DLTs – i.e. *data integrity*, due to the ledger tamper-resistance and *decentralization* – their combination with M2M communication entails a set of advantages: (i) *node autonomy*, as the network of nodes does not rely on a central authority; (ii) *availability*, as the append-only ledger and redundant data storage provide high availability of data and smart contracts provide high availability for services; (iii) *automation*, as smart contracts allow for autonomous execution of business logic and enforcement of agreements [25]. Overall, these features and the direction of future development of these technologies show a striking correspondence with M2M requirements [36].

2.3 CBDCs

After Bitcoin's launch in 2009, the prospect of devising an electronic version of cash has been considered with increasing fascination. The main promise was that of a more "democratic" and direct – *i.e.*, disintermediated – participation of citizens and businesses in the global economy. While cryptocurrency developments have heeded a token-based "Internet of Value(s)" [37] and an "Internet of Money", legacy financial institutions and the private sector have soon declared their interest in investigating decentralized "smart" – *i.e.*, "programmable" – money. Leveraging improvements in tokenization techniques, privately-driven projects of "(global) stablecoins" have reached the headlines – *e.g.*, Facebook's Libra/Diem.

Amidst this quest for value interconnection, sovereign monetary institutions have been leveraging technology not only to innovate payments and transmission channels, but also to rethink the essence of "physical cash" [2, 7]. Although their interest in digital money started emerging in 2014, most initiatives stepped into the spotlight over the last 2-3 years and explore the deployment of some sort of blockchain technology. At the beginning of 2021, 86% of central banks were reportedly exploring CBDCs [16].

Several definitions ground any CBDC-related discourse. First, there is an importance monetary distinction between

- *Central Bank Money*: includes A) physical money or cash, *i.e.,* general purpose money; and B) reserves or settlement accounts, issued to authorized institutions, *e.g.*, commercial banks and payment service providers;
- *Commercial Bank Money*: liabilities to the general public issued by a commercial bank, it consists of a claim against the issuer to pay central bank money.

As referenced in [32], CBDCs can be classified as follows:

- *Wholesale CBDC*: a settlement mechanism between financial institutions for inter-bank transfers between participants by Real-Time Gross Settlement Systems.
- *Retail CBDC*: offered to the general public. This is the most disruptive type of CBDC in terms of an evolution towards a more "democratic" monetary channel.

Recently, interest has focused on cross-border aspects, in terms of developing and surveying arrangements of multiple CBDC bridges [8].

The architecture of a CBDC can be designed in different ways, and may involve public and private stakeholders. Chiefly, the model can be (i) *one-layered*, under the sole management of the central bank (*e.g.*, distribution, KYC, settlement); or (ii) *two-layered*, where non-governmental financial institutions (*e.g.*, commercial banks, payment service providers) act as intermediaries for end-users. Accordingly, CBDC architectures are named *direct*, *hybrid*, *intermediated* or *indirect/synthetic* [7]. The *direct* structure is described as "one-tier", as only the central bank is involved (*e.g.*, it initiates/maintains the relationship with end-users, which is untraditional for central banks) and the CBDC is a direct claim of the public. On the contrary, *hybrid*, *intermediated* and *synthetic* CBDCs are "two-tier", thus resembling traditional mechanisms [6, 11].

Lastly, a CBDC can be (i) *account-based*, where users open a current account, or "e-wallet", usually following some form of KYC; and (ii) *token-based*, where the CBDC is a digital unit, such as a token stored in a physical device. This type of CBDC is a bearer instrument transferred with secure hardware/software units.

3 M2M PAYMENTS IN CONSUMER IOT

In this section, we explore the interplay between techniques of M2M communication, the advent of DLTs and the world of payments.

3.1 M2M and the Economy of Things

With regards to M2M, various stakeholders envisioned a future with "smart" machines (inter)acting autonomously and exchanging information also for economic purposes. As any economic system, this "machine economy" – also "economy of things" or "M2M economy" – has requirements to provide the expected added value to daily human activities. Arguably, one of the prerequisites is that the devices can autonomously issue invoices and make payments among themselves [34]. Without M2M payments – defined as the integration of payment processes into an automated processing of business transactions – (C)IoT would remain only a fragment of the bigger picture. Indeed, in the absence of M2M payments, information exchanges that should ideally take place without interruption would depend on, and should wait for, human actions such as a manual payment confirmation [34].

Ostensibly, this economic interplay would be grounded on different dynamics in comparison with the current centralized economy that relies on intermediaries. A "M2M economy" is inherently decentralized and based on the autonomy of its participants, *i.e.*, machines. The same ratio of M2M techniques draws from the observation that interconnected machines offer more value than isolated ones, and their interconnection can unlock the development of a wider variety of cheaper autonomous and intelligent applications [3, 15].

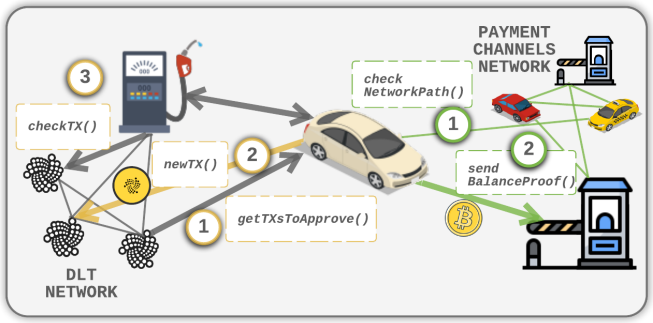

Figure 1: Cryptocurrencies applied to (C)IoT. Left is New Cryptocurrency Design (yellow payment). Right is Payment Channel Network (green payment)

Thus, it may be surprising that the development of CIoT and DLT-based payments – *e.g.*, cryptocurrencies – has largely occurred within detached silos. Albeit some exemptions exist, it can be argued that the possibility of their integration has so far failed to play a major role in the design phase of the two sets of projects. Even if the first and foremost application of blockchain technology was to facilitate payments, and even if the available cryptocurrencies now amount to more than 7,000 and can be deployed in relation to various services, their application to payments in IoT-related domains is reportedly uncommon and the scope of the research appears limited to few aspects, *e.g.*, privacy [27].

Nevertheless, all factors at play suggest that a future decentralized M2M economy will need to rely on a payment system that is decentralized and self-managed, which can give birth to an "economy of things" that is untethered from – and unconstrained by – human interactions [30]. Against this backdrop, cryptocurrencies seem to be a natural fit as they can provide decentralized management of "cash-like" assets. Concurrently, from a privacy and data protection perspective relying on a decentralized infrastructure, rather than on a centralized ledger, cannot only help distribute among users/devices computer power needs, but may also provide effective solutions for managing sensitive information [38].

3.2 Cryptocurrencies applied to (C)IoT

The vision of the M2M economy has driven investigations on how to integrate cryptocurrencies and (C)IoT. The amalgamation of the two concepts reportedly happens by enabling consumer devices to perform financial "micro-transactions" known as "micro-payments". Ideally, the significant number of expected transactions signals the need for scalable payment systems with almost non-existent fees. However, DLT architectures usually require significant resources to maintain security and decentralization, seemingly unfit for the constraints of smart devices. In this respect, [30] provides a taxonomy and a qualitative assessment of possible methodologies:

(1) *Direct Integration*: the (C)IoT device is connected to a major cryptocurrency network (*e.g.*, Bitcoin, Ethereum) via a trusted gateway. The e-device does not run a node itself, but is registered to a gateway – a "trusted (full) node" – that handles transactions. The cryptocurrency wallet is hosted

by the server, but transactions require the consent of the e-device/client. The communication between the smart device and the gateway is secured cryptographically. Alternatively, the use of "light clients" have been proposed.

(2) *Payment Channel Network*, *i.e.*, "second layer solution" or "off-chain transaction network": it allows instant off-chain transactions with minimal fees . It is based on smart contracts to avoid the need to record every transaction on the blockchain. Examples are Bitcoin's *Lightning Network* and Ethereum's *Raiden* for intra-chain transactions, and *InterLedger* and *Atomic CrossChain* for inter-blockchain operations [27].

(3) *New Cryptocurrency Design*: structures that are alternative to blockchain but still leverage a distributed architecture for the sake of scalability. They are DLT-based coins developed for IoT purposes, and the chief example is the structure implemented by IOTA, where a web of connections is enabled by the Tangle, a Directed Acyclic Graph [33]. In general, IoT cryptocurrency designs focus on the development of new algorithms that limit the computational cost of transactions.

Based on this taxonomy, our critical analysis of these methodologies is described in the following.

Direct integration to mayor cryptocurrency networks usually involve latencies that are not "(C)IoT-ready" – *i.e.*, (C)IoT devices usually require almost real-time operation [43]. For instance, Figure 1 depicts a smart vehicle that makes use of a petrol pump service and pays through cryptocurrencies (left side). Using DLTs such as Ethereum or Bitcoin could take from 30 seconds to several minutes to finalize the payment, mostly due to their consensus mechanism execution by a remote network node, *i.e.*, Proof of Work (PoW).

Making use of DLTs based on *New Cryptocurrency Design* such as IOTA the device on board of the vehicle can actively participate in the issuance of a new transaction by: (i) requesting autonomously past transactions to approve (i.e. tips) following the IOTA consensus mechanism [33]; (ii) executing the PoW or delegating it to a dedicated node and then broadcasting the newly made transaction to the DLT network nodes. This operation can take on average $\sim$ 20 seconds, that is still not a latency suited for real-time cases, but that would fit this scenario [43]. The petrol pump service device, then, only needs to check the validation of a new transaction.

More efficiency in terms of latency can be obtained using *Payment Channel Networks* in certain scenarios. For instance, Figure 1 shows a smart vehicle that pays a motorway toll and continues on his way (right side). In this case the $\sim$ 20 seconds of latency of IOTA are not suitable. Then one can make use of payment channels and be faced with two possible paths. First, if the vehicle and the tollbooth device have opened a payment channel in the past, the payment would consist of the vehicle sending a digitally signed message to the tollbooth showing the (updated) balance proof in their channel. Though a short range communication (*e.g.*, Wi-fi), maintaining this communication with real-time latency would be feasible [27]. Second, if the vehicle and the tollbooth device have no open payment channels, a path of open payment channels can be checked in the local payment channels network created through a Vehicular Ad-hoc Network among other vehicles and tollbooths in the same area [44]. This would increase the latency overall, but still be reasonable in such scenario [17].

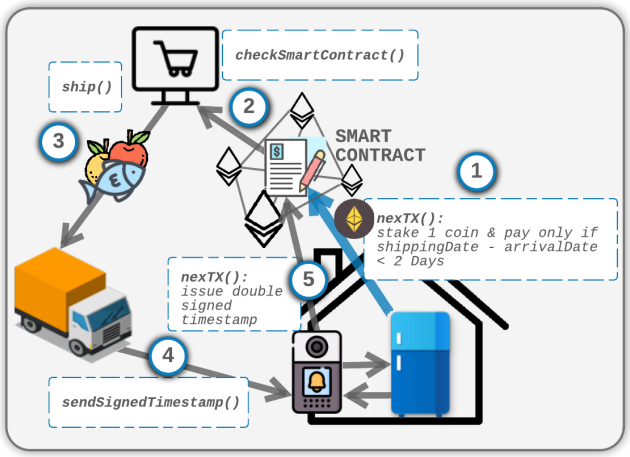

Figure 2: Programmability in M2M payments. A Direct Integration type of payment where a coin is stacked and released only if a condition is met, i.e. goods are delivered in time

3.3 Programmability in M2M payments

The idea of unlocking the M2M economy by integrating cryptocurrencies also leverages smart contracts to benefit from *programmability*, which is a requirement to provide the *automation* of the payment process. Nonetheless, the general debate tends to overestimate the role or DLTs and blockchains in this regard, as they are arguably not the only solutions for programmability [23].

There is, however, a difference between programmability of *money* and that of *payments*. Albeit often used imprecisely, "programmable money" features embedded rules that constrain its use, while "programmable payments" innovate the way to transfer money, thus offering functional benefits, new processes and business models [23]. Arguably, in a (C)IoT M2M scenario what is necessary is to have programmable *payments*. In this way, e-devices could be equipped with a payment system whose transactions occur at given conditions, thus enabling them to fulfill the entire cycle of a contractual relation.

In Figure 2 we depict a possible use case where a smart fridge, through a *direct integration* methodology, makes a programmable payment using an Ethereum smart contract. In this scenario, the smart contract is simply set up by an e-commerce platform to validate the freshness of its degradable products sold to clients, *i.e.*, "if" the difference between arrival date and shipping date is greater than 2 days "then" the coins deposited by the consumer at the time of purchase are returned (to be meaningful, this process would come at the end of a traced supply chain, but this falls outside the scope of this paper). Once submitted, smart devices in the same house can communicate M2M to further process the payment and its validity. For instance, the smart fridge can provide a payment secret value to a smart doorbell, that will be used by the delivery truck to authenticate itself to the doorbell. Then, different methods can be employed to validate the delivery timestamp – *e.g.*, a double signature (one from the delivery truck and one from the smart doorbell) on a timestamp value, attesting the delivery date. Such value can be issued to the smart contract to unlock the payment.

4 RETAIL CBDC-BASED M2M PAYMENTS

In this section, we investigate the prospective interplay between the M2M economy, retail CBDCs and regulatory questions.

4.1 E-fiat money and the M2M Economy

Even if the financial field is still largely based on traditional infrastructures, the advent of cryptocurrencies, FinTech and novel trends in tokenization has created a fertile ground for innovation. In this context, central banks have started their own investigations into sovereign frameworks of digital fiat money, and the introduction of consumer/retail payments in CBDCs is expected to be the next major development in digital payments [10].

We have argued so far that decentralization seems to be the most effective way to achieve an M2M economy in (C)IoT and we have seen how there DLTs offer several options in terms of interaction between systems and devices. Nonetheless, in some scenarios decentralization may not be provided with regard to the interplay between the entities at the governance level – *e.g.*, trivially, the difference between a public permissionless blockchain and a private permissioned one [26]. Generally speaking, governance can be regarded as the integration of norms and culture, the laws and the code, the people and the institutions that facilitate coordination and together determine a given organisation [20]. Given the stakeholders involved in CBDC schemes, the tendency is to centralize governance while maintaining the decentralisation of systems and device communication. It was argued the trend in central bank DLT systems is to move back to centralized but distributed systems, where network nodes are identified and accountable [2, 10].

At the earliest stages of CBDC projects the interest was mostly limited to transactions between financial institutions – *i.e.*, "wholesale" scenarios. In the last five years, research has increasingly focused on e-fiat money to be used by the general public, known as "retail" CBDCs [32]. In light of the target – *i.e.*, millions of people –, this tool could not only change the relationship between money and society but also the interplay between different sovereign frameworks, which prompted investigations into their interconnection, interoperability and standardization [8].

Against this backdrop, a series of core characteristics of CBDC systems seem to fit the M2M economy. CBDC research has pinpointed policy objectives [7, 39], and some features appear relatable to the CIoT sphere. For instance, CBDC designs shall heed:

- the interplay/trade-off between maximizing privacy and data protection and safeguarding compliance with other sets of regulations such as anti-money laundering;
- universal and unrestricted accessibility, disregarding geographical location and user's means and specific abilities;
- resilience: providing continuous operation online and offline;
- security: offering products/services resistant to cyberattacks;
- high performance: ensuring scalability for daily use, within the given jurisdiction and cross-border.

4.2 CBDCs and programmable micro-payments

Reportedly, consensus mechanisms of traditional cryptocurrencies (*e.g.*, PoW for Bitcoin transactions) are not suitable for micro-payments. This is especially true if they are performed by resource-constrained devices, due to elements such as scalability, transaction fees and block confirmation times [30, 43]. Albeit it is still not economically feasible to transfer small amount of money, which hampers the use case of streaming money [21], specific CBDC models could overcome the limits showed by cryptocurrency designs in (C)IoT scenarios. In this context, it was argued CBDCs could be divided to allow tiny transactions – *i.e.*, CBDCs models could support micro-payments as required by (C)IoT applications [18].

Further, experts have argued that in (C)IoT scenarios a tokenized and programmable version of fiat money issued directly on a DLT – *i.e.*, a "native" instrument integrated into the platform – would enable (i) real-time settlement, (ii) predefinition and automatic processing of payments, (iii) delivery-vs-payment transactions [21]. At the same time, in (C)IoT scenarios the programmability of a DLT-based e-fiat currency means it is possible to predefine payments and process them automatically, while delivery-vs-payment transactions are enabled by using a DLT as the underlying platform for both the process and the payment [21].

Nonetheless, it is the use of smart contacts in CBDCs that can prospectively allow to set up schemes of M2M transactions in a peer-to-peer fashion. This is because they allow to execute low-value transactions when there is a high third-party cost in terms of lack of trust.

4.3 Regulatory methodology and compliance

Deploying digital currencies in (C)IoT generates regulatory hurdles. A normative framework for device-to-device transactions is pivotal, yet it is still non-existent, and adequate standardization is needed. For instance, legal effects of smart communication need to rely on frameworks of "machine identities", while ordinary transaction safeguards may prove unsuitable – *e.g.*, two-factor authentication hampers the device from handling the settlement and debiting the amount without user confirmation [21]. We argue that the large-scale interest in CBDCs provides the opportunity to define normative goals at the beginning of the design process. Thus, technical and legal aspects can be tackled jointly, while institutions are setting up expert groups that could pursue standardization.

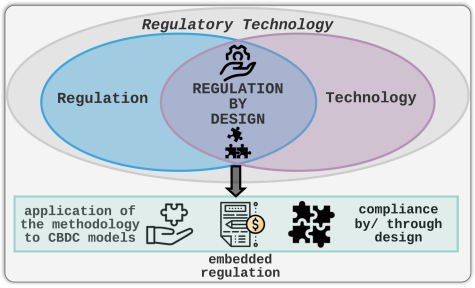

Figure 3: *Regulation by Design*

This approach is depicted in Figure 3 and replaces *command and control* regulatory techniques, based on prohibitions and sanctions, with a *design-based* methodology that views compliance as *embeddable* into technology [32, 41]. The idea that compliance *ought to* be streamlined into a design process developed from the concept of *privacy-by-design* [13], later evolved into *compliance by* or *through design* [12]. In turn, the concept of *embedding* law draws

from Lessig's "code is law" [29] – *i.e.*, cyberspace behavior can be controlled by code. Albeit hyperbolic statements shall not be interpreted literally, the methodology has informed valuable notions such as *embedded regulation* [42] and *supervision* [4].

Ostensibly, code can be leveraged to approach regulation and compliance in a proactive way, rather than reactively [31]. Building on RegTech, that uses technology to aid legal purposes (see Figure 3), *design-based* techniques act in a *forward-looking* manner with preliminary engineering and standard setting [32]. Meanwhile, cross-disciplinary tools are offered by legal informatics with *computational law*, trying to bridge the gap between legal knowledge/reasoning, natural language and machine-readable formats [14, 22]. Against this backdrop, we argue the inherent automation of (C)IoT requires a payment system that is compliant *by design*.

4.4 Privacy-transparency trade-offs

If design and code become regulatory instruments, when integrating (C)IoT and CBDCs the attention is drawn to the features to be tuned. Because (C)IoT devices are used in large economic sectors, and their core functionalities consist of sensing and collecting data [1, 30], vast-scale surveillance may arise if privacy is not safeguarded. At the same time, research on network formation and impacts on privacy is still insufficient [27]. If we add monetary transactions to the controversy, risks increase consistently.

CBDC research argues design choices are never binary and there are always compromises between different, often opposing, elements. An important trade-off relates to concurrent regulatory requirements concerning privacy and transparency – *e.g.*, data protection and anti-money laundering. On the one hand, privacy concerns emerge especially in two-layered CBDC structures that involve public-private partnerships and when a large number of stakeholders have access to personal information. On the other hand, techniques that leverage connectivity, micro-payments and programmability can also be seized by criminals [18].

The tension between privacy and transparency, however, is not a zero-sum game. A range of privacy/anonymity degrees are found in all means of payments, while digital currencies and programmability generate new forms of control and disclosure of sensitive information [2]. In this context, the added value of CBDCs is to embed from the start a specific trade-off. The main examples are [32]:

- fully-transparent CBDC with real-world identity transactions fully visible to law enforcement, in violation of privacy;
- privacy provided without any limitation, so that no information can be revealed about transactions, a solution that is vulnerable to misuse for illicit purposes;
- nuanced solutions, deployed by most CBDCs projects, offering some privacy to consumers (*i.e.*, confidentiality) and some visibility to authorities (*i.e.*, auditability).

5 INTEGRATING CBDC AND CIOT

In this section, we speculate on the elements at play when devising an integration between CBDC models and the CIoT environment.

5.1 The role of CBDC architectures

The publicly available technical specifications on ongoing CBDC investigations do not support a thorough analysis of the options to integrate the different designs with CIoT M2M dynamics. Nonetheless, in light of what we have outlined so far, we argue there is a set of elements that allow to depict a preliminary integration model.

To start with, we consider the available architectures from the perspective of the participating entities. As anticipated, when the model requires only the involvement of the central bank to offer retail services and manage client relationships, the structure is described as *direct*, or *one-tier*, or *one-layered*. On the contrary, when the system relies on the cooperation with private financial institutions – which happens in *hybrid*, *intermediated* and *synthetic* CBDC models – the architecture is defined as *two-tier* or *two-layered* [6, 11].

In this respect, the implementation of a *direct* model requires central banks to initiate and continuously attend to the relationship with end-users. These activities (*e.g.*, KYC, onboarding) fall largely outside the scope of their traditional competences, and would require them to provide a range of services already established in the daily operations of payment service providers. Clearly, such a "doubling" mechanism is hardly efficient. Hence, in our contribution we fall in line with the choice that informs most retail CBDC proof-of-concepts and pilots [40], and we consider a *two-tier* scenario where users interact (*e.g.*, open their accounts) with intermediaries.

5.2 A CBDC wallet for a (C)IoT device

All CBDC architectures can deploy different types of *wallets*, through which end-users' devices interact with the ecosystem. As with other digital wallets, they serve the function of authenticating the user and the transaction, and represent the interface to perform financial transactions [2]. In this respect, they store private and public keys used to sign transactions digitally. CBDC features are relevant to our discussion because the autonomy of (C)IoT devices and the decentralization of M2M communications shall be handled during the architecture design phase. Below we highlight five perspectives.

5.2.1 Account-based vs token-based wallets. While in *account-based* wallets access is tied to an identity system and authentication is performed via identity verification – *e.g.*, a security code sent to the user – in *token-based* wallets it is tied to a cryptographic scheme – *e.g.*, digitally signing a DLT transaction [7, 11]. If from the user's point of view there is little difference, in a M2M scenario an *account-based* wallet would limit the device's access to the payment process, as owner's authentication is required. Because devices need a (limited) degree of autonomy to reap the benefits of the M2M economy, the use of *token-based* wallets may be preferred, since only a digital signature is required to enable a payment. This relates precisely to the cryptocurrency payment methods shown in Section 3.2 for CIoT devices. However, it is not mandatory to use only one type of wallet, and different solutions can be tailored to different contexts. Hence, there is no need for a CBDC architecture to deploy only *token-based* wallets – *e.g.*, there could be an *account-based* main wallet and several *token-based* wallets dedicated to devices.

5.2.2 Hardware-based vs software-based wallets. The security of a wallet of the first type relies on chips and other technologies that are built in the device making the payment, while a *software-based* wallet makes use of cryptography and security protocols at the software level, which is more suitable for large-scale deployment [40].

In this case we believe the choice will depend on the operation scenario of the device storing the wallet and on the degree of security required. Indeed, the implementation of a hardware-based wallet might be more feasible for a CIoT device such as a smart vehicle's onboard computer than in a low-cost smartwatch.

5.2.3 Custodial or non-custodial wallets. Wallets are *custodial* when a third party operates the wallet and holds the private keys on the user's behalf, while in *non-custodial* wallets end-users hold the private keys directly. Non-custodial wallets offer cash-like features in digital transactions. While *token-based* CBDCs *can* be held by custodians on behalf of end-users, *account-based* CBDCs are *intrinsically* based on the relationship with a custodian [24]. We envision the use of *non-custodial* wallets for CIoT devices as it relates more with the use cases already deployed for DLTs, such as *Payment Channel Network* and *New Cryptocurrency Design*, shown in Section 3.2.

5.2.4 Parent wallets and sub-wallets. The distinction relates to authorization – *i.e.*, the holder can have a main wallet as parent wallet and open sub-wallets to set payment limits or conditions, personal privacy protection and other features [40]. A main parent wallet can be compared to today's generic bank account for the use of fiat currency, while sub-wallets would represent prepaid card linked to the account and with a limited amount of fiat. A CIoT device could use this type of sub-wallet to have autonomy in its payment.

5.2.5 Offline usability. A necessary requirement for CBDCs is to be usable even when their end-users are temporarily unable to access the Internet. Usually, the strategy is to devise solutions that allow to store small amounts of CBDCs that can meet the needs of daily and common transactions (*e.g.*, grocery shopping, petrol) even when connectivity to the network is not available. We argue CIoT devices are susceptible to run into the same circumstance on a daily basis – e.g., a smart vehicle needing to pay at a tollbooth but no Internet connection is available while it is passing through the gates. Hence, this can be easily linked to the state channel payment between CIoT devices shown in Section 3.2. Reportedly, possible strategies to solve the offline usability problem tend to result in a *trade-off* between hardware/software security, costs, and convenience. One way to implement offline transactions is via tamper-proof hardware. Alternatively, it is possible to issue CBDC-cards, loaded with a small number of CBDCs when the user's wallet is online [2, 39].

5.3 A CBDC model integrating CIoT and M2M

The deployment of blockchain/DLTs in a scenario populated by billions of economically autonomous devices was deemed conducive to handle techno-regulatory requirements [36]. Indeed, there would be no need to bridge the (C)IoT environment to the current SEPA system (*i.e.*, 'trigger/bridge solution"), an option that features considerable shortcomings for automatic payments because SEPA does not provide single-source-of-truth and machine identities functionalities [21]. Seemingly, native DLT-based means of payment can integrate payments into the CIoT and streamline the value chain. Going further, however, it is the nature of retail CBDCs as fiat money that can merge the physical and digital worlds seamlessly.

Against this backdrop, in Figure 4 we depict an overview of a *possible* model for a two-tier retail CBDC system based on a DLT.

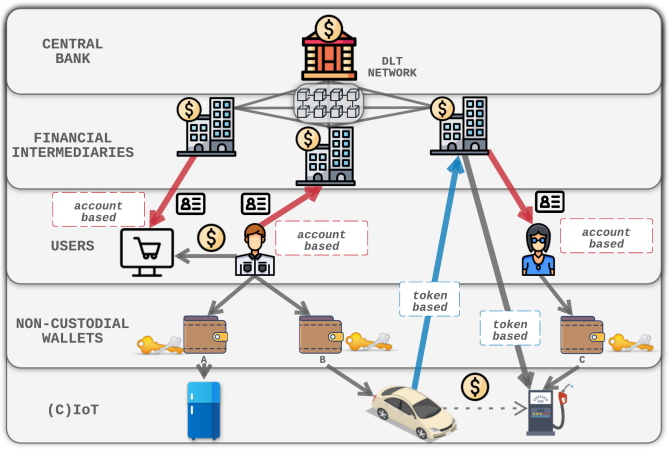

Figure 4: Preliminary integration scenario of CIoT and a two-tier retail CBDC system

In this model CIoT devices are equipped with token-based sub-wallets loaded with a given budget of CBDCs to enable machines to automatically perform payments in native e-fiat money. Such payments are triggered by the machines after a communication with another machine, *e.g.*, a vehicle and a petrol pump service device, and upon the verification of conditions predefined by the DLT protocol. This would complement the inherent capability of CIoT devices to execute processes independently – *i.e.*, with no human involvement – leveraging their interconnection [21]. Moreover, we integrate a layer in which users can authenticate themselves and pay through account-based custodial parent wallets with a layer in which CIoT devices have their own token-based non-custodial sub-wallets, that they use to pay "simply" by using a digital signature, as shown in 3.2. Such sub-wallets are prepaid, and their deployment allows not only to safeguard privacy more easily but also to design in a more flexible way the trade-off outlined below.

5.4 Embedded trade-offs

With regard to the embedded privacy-transparency trade-off, CBDC research is heeding "mixed solutions" as a way to offer anonymity while reaching a legally desirable level of privacy [32]. These models are designed to provide multiple wallet options tailored to different types of transactions – *e.g.*, they may allow higher degrees of anonymity for transactions of low values. To do so, they may offer specific anonymity-oriented wallets – *i.e.*, transactions may not require the acquisition of identity information on the payer or the payee – featuring limited amounts and allowing only certain types of transactions to mitigate the risks. This is the case of the Chinese e-CNY, where different types of wallets are assigned to consumers according to the strength of their personal identification, and different amount, per-transaction and daily limits are set [40]. Similarly, a proof-of-concept developed by Canadian universities adopts a mixed approach to provide untraceable offline transactions [39].

Ostensibly, an anonymity-oriented CBDC is usually token-based [24, 39]. In this respect, it was argued that users of retail CBDCs

should be able to hold CBDC tokens outside of custodial relationships, and that these tokens should not be forcibly linked to addresses/identifiers (to users or other tokens), thus applying *privacy-by-design* [24]. We argue that this model, together with its limitations in terms of amounts and types of transactions, appears suitable to the needs of the smart devices. Nonetheless, limiting our scope to a CIoT-specific scenario, we place it within a more comprehensive scheme of tiered wallets, comprising a main account-based wallet controlling token-based sub-wallets assigned to e-devices.

6 CONCLUSIONS

In this paper we have explored a preliminary techno-regulatory integration of the world of CIoT and M2M communication with the new frontiers of money. Thus, we analyzed a possible model of retail CBDC system to include M2M and CIoT dynamics, while taking into account regulation-by-design and compliance-by/through-design methodologies. Our findings show that the integration of CBDCs, M2M payments and (C)IoT requires multi-stakeholder-based standardization, and we maintain that CBDC projects provide an invaluable opportunity to develop it. Accordingly, we outlined the relevance of applying *by-design* techniques to address regulatory concerns (*e.g.*, in the spheres of data protection and misuse of the financial system), especially when they generate seemingly opposing requirements. In this context, we argued the deployment of DLTs in a CBDC design is conducive to reaching and *embedding* desired trade-offs, at least in our (C)IoT-specific scenario.

Against this backdrop, we put forward a preliminary model of integration between a two-tier retail CBDC architecture and CIoT. After tailoring a set of CBDC structural options to the needs and constraints of smart devices, we designed our multi-layered model to: (i) equip the machines with non-custodial token-based sub-wallets loaded with a given budget to automatically and independently perform payments in native e-fiat money by using a digital signature, while (ii) end-users can hold custodial account-based parent wallets that rely on authentication and control the devices' wallets.

REFERENCES

[1] B. Ahlgren, M. Hidell, and E.C.-H. Ngai. 2016. Internet of Things for Smart Cities: Interoperability and Open Data. *IEEE Internet Computing* 20, 6 (2016), 52–56.

[2] Sarah Allen, Srdjan Capkun, Ittay Eyal, Giulia Fanti, Bryan Ford, James Grimmelmann, Ari Juels, Kari Kostiainen, Sarah Meiklejohn, Andrew Miller, Eswar Prasad, Karl Wüst, and Fan Zhang. 2020. *Design Choices for Central Bank Digital Currency: Policy and Technical Considerations.* Technical Report 13535.

[3] Oluwatosin Ahmed Amodu and Mohamed Othman. 2018. Machine-to-machine communication: An overview of opport. *Computer Networks* 145 (2018), 255–276.

[4] Raphael Auer. 2019. Embedded supervision: how to build regulation into blockchain finance. (sep 2019).

[5] Raphael Auer, Codruta Boar, Giulio Cornelli, Jon Frost, Henry Holden, and Andreas Wehrli. 2021. *CBDCs beyond borders: results from a survey of central banks.* Technical Report.

[6] Raphael Auer and Rainer Böhme. 2021. *Central bank digital currency: the quest for minimally invasive technology.* Technical Report. BIS.

[7] Raphael Auer, Giulio Cornelli, and Jon Frost. 2020. *Rise of the central bank digital currencies: drivers, approaches and technologies.* Technical Report.

[8] Raphael Auer, Philipp Haene, and Henry Holden. 2021. *Multi-CBDC arrangements and the future of cross-border payments.* Technical Report. BIS.

[9] Alexandre C Barbosa, Thays A Oliveira, and Vitor N Coelho. 2018. Cryptocurrencies for smart territories: an exploratory study. In *2018 International Joint Conference on Neural Networks (IJCNN).* IEEE, 1–8.

[10] Ron Berndsen and Ruth Wandhöfer. 2020. *To Centralize or Decentralize: What is the Question? An Application to Digital Payments.* Springer Int., 105–118.

[11] Agustin Carstens. 2021. Digital Currencies and the Future Monetary System. *Hoover Institution policy seminar* 89, 1 (2021), 17.

[12] Pompeu Casanovas, Jorge González-Conejero, and Louis De Koker. 2018. Legal compliance by design (LCbD) and through design (LCtD): Preliminary survey. *CEUR Workshop Proceedings* 2049 (2018), 33–49.

[13] Ann Cavoukian. 2011. Privacy by Design. *Office of Inf. and Privacy Comm.* (2011).

[14] Luca Cervone, Monica Palmirani, and Fabio Vitali. 2020. The Intelligible Contract. In *53d Hawaii International Conference on System Sciences.*

[15] Min Chen, Jiafu Wan, and Fang Li. 2012. Machine-to-machine communications: Architectures, standards and applications. *KSII Transactions on Internet and Information Systems (TIIS)* 6, 2 (2012), 480–497.

[16] Boar Codruta and Andreas Wehrli. 2021. *Ready, steady, go? – Results of the third BIS survey on central bank digital currency.* Technical Report 114. 77–82 pages.

[17] Enes Erdin, Suat Mercan, and Kemal Akkaya. 2021. An Evaluation of Cryptocurrency Payment Channel Networks and Their Privacy Implications. *arXiv preprint arXiv:2102.02659* (2021).

[18] Yaya J. Fanusie. 2020. Central Bank Digital Currencies: The Threat From Money Launderers and How to Stop Them. *The Digital Social Contract: A Lawfare Paper Series* November (2020), 1–23.

[19] Pietro Ferraro, Christopher King, and Robert Shorten. 2018. Distributed ledger technology for smart cities, the sharing economy, and social compliance. *IEEE Access* 6 (2018), 62728–62746.

[20] Aron Fischer and María-Cruz Valiente. 2021. Blockchain governance. *Internet Policy Review* 10 (2021). https://doi.org/10.14763/2021.2.1554

[21] Maximilian Forster, Jonas Gross, Anja Kristina Kamping, Serkan Katilmis, Dr Mario Reichel, Prof Dr Philipp Sandner, and Philipp Schröder. 2021. The future of payments: programmable payments in the IoT sector. (2021).

[22] Michael Genesereth. 2015. Computational law: The cop in the backseat. *CodeX - The Stanford Center for Legal Informatics* (2015), 1–5. http://logic.stanford.edu

[23] Giesecke+Devrient. 2021. How to bring the benefits of program. to CBDC. https://www.gi-de.com/en/spotlight/payment/benefits-of-programmability-to-cbdc

[24] Geoffrey Goodell, Hazem Danny Al-Nakib, and Paolo Tasca. 2021. A Digital Currency Architecture for Privacy and Owner-Custodianship. *Future Internet* 13 (2021). https://arxiv.org/abs/2101.05259

[25] ITU-T FG DLT. 2019. *Distributed Ledger Technology Regulatory Framework.* Technical Report. https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d41.pdf

[26] ITU-T FG DLT. 2019. *Distributed Ledger Technology Terms and Definitions.* Technical Report. https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf

[27] Rateb Jabbar, Noora Fetais, Mohamed Kharbeche, Moez Krichen, Kamel Barkaoui, and Mohammed Shinoy. 2021. Blockchain for The Internet of Vehicles: How to use Blockchain to secure Vehicle-to-Everything (V2X) Communication and Payment? *IEEE Sensors Journal* 21, 14 (2021), 15807–15823.

[28] Dongyeon Kim, Kyuhong Park, Yongjin Park, and Jae-Hyeon Ahn. 2019. Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior* 92 (2019), 273–281.

[29] Lawrence Lessig. 2006. *Code v. 2.0.* Basic Books.

[30] Suat Mercan, Ahmet Kurt, Enes Erdin, and Kemal Akkaya. 2021. Cryptocurrency Solutions to Enable Micro-payments in Consumer IoT. *IEEE CEM* (2021).

[31] Hossein Nabilou. 2019. Testing the waters of the Rubicon: the ECB and central bank digital currencies. *Journal of Banking Regulation* 21, 4 (2019), 299–314.

[32] Nadia Pocher and Andreas Veneris. 2021. Privacy and Transparency in CBDCs: a Regulation-by-Design AML/CFT Scheme. In *Proceedings - 2021 IEEE ICBC.*

[33] Serguei Popov. 2016. The Tangle. https://iota.org/IOTA_Whitepaper.pdf

[34] PPI AG. 2020. Internet of Payments. https://www.ppi.de/en/payments/next-generation-payments/study-internet-of-payments-iop/

[35] Ramjee Prasad and Vandana Rohokale. 2020. Internet of Things (IoT) and Machine to Machine (M2M) Communication. In *Cyber Security: The Lifeline of Information and Communication Technology.* Springer, 125–141.

[36] André Schweizer, Patricia Knoll, Nils Urbach, Heiko Andreas von der Gracht, and Thomas Hardjono. 2020. To what extent will blockchain drive the machine economy? Perspectives from a prospective study. *IEEE Transactions on Engineering Management* 67, 4 (2020), 1169–1183.

[37] Don Tapscott and Jim Euchner. 2019. Blockchain and the Internet of Value. *Research Technology Management* 62, 1 (2019), 12–19.

[38] Josh Taubenheim. 2019. Integrating blockchain techn. into IoT: 3 vendor profiles.

[39] Andreas Veneris, Andreas Park, Fan Long, and Poonam Puri. 2021. Central Bank Digital Loonie: Canadian Cash for a New Global Economy. (2021). https://ssrn.com/abstract=3770024

[40] Working Group on E-CNY People's Bank of China. 2021. Progress of Research and Development of e-CNY in China. (jul 2021).

[41] Karen Yeung. 2017. 'Hypernudge': Big Data as a mode of regulation by design. *Information Comm. and Society* 20, 1 (2017), 118–136.

[42] Dirk A Zetzsche, Douglas W Arner, and Ross P Buckley. 2020. Decentralized Finance. *Journal of Financial Regulation* 6, 2 (2020), 172–203.

[43] Mirko Zichichi, Stefano Ferretti, and Gabriele D'Angelo. 2020. Are Distributed Ledger Technologies Ready for Intelligent Transportation Systems?. In *Proc. of the 3rd Workshop CryBlock 2020, co-located with MobiCom 2020, ACM.* ACM, 1–6.

[44] Mirko Zichichi, Stefano Ferretti, and Gabriele D'Angelo. 2020. A Framework based on Distributed Ledger Technologies for Data Management and Services in Intelligent Transportation Systems. *IEEE Access* (2020), 100384–100402.