Law, Science and Technology
MSCA ITN EJD n. 814177

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

Nadia Pocher
PhD Candidate at
Universitat Autònoma de Barcelona,
KU Leuven – CITIP and Università di Bologna

Mirko Zichichi
PhD Candidate at
Universidad Politécnica de Madrid,
Università di Bologna and Università di Torino

P2PFISY 2021 – December 1st, 2021

Outline and Objectives

1. **Background**
   - 1.1. Consumer Internet of Things
   - 1.2. M2M Communication
   - 1.3. Distributed Ledger Technologies
   - 1.4. (Retail) Central Bank Digital Currencies

2. **M2M Payments in Consumer IoT**
   - 2.1. M2M and the Economy of Things
   - 2.2. Cryptocurrencies applied to (C)IoT
   - 2.3. Programmability in M2M Payments

3. **Retail CBDC-based M2M Payments**
   - 3.1. E-fiat Money and the M2M Economy
   - 3.2. CBDCs and Programmable Micro-Payments
   - 3.3. Regulatory Methodology and Compliance
   - 3.4. Privacy-Transparency Trade-offs

4. **Integrating CBDCs and CIoT**
   - 4.1. The Role of CBDC Architectures
   - 4.2. A CBDC Wallet for a (C)IoT Device
   - 4.3. A CBDC Model Integrating CIoT and M2M
   - 4.4. Embedded Trade-offs

5. **Conclusions**

in this presentation

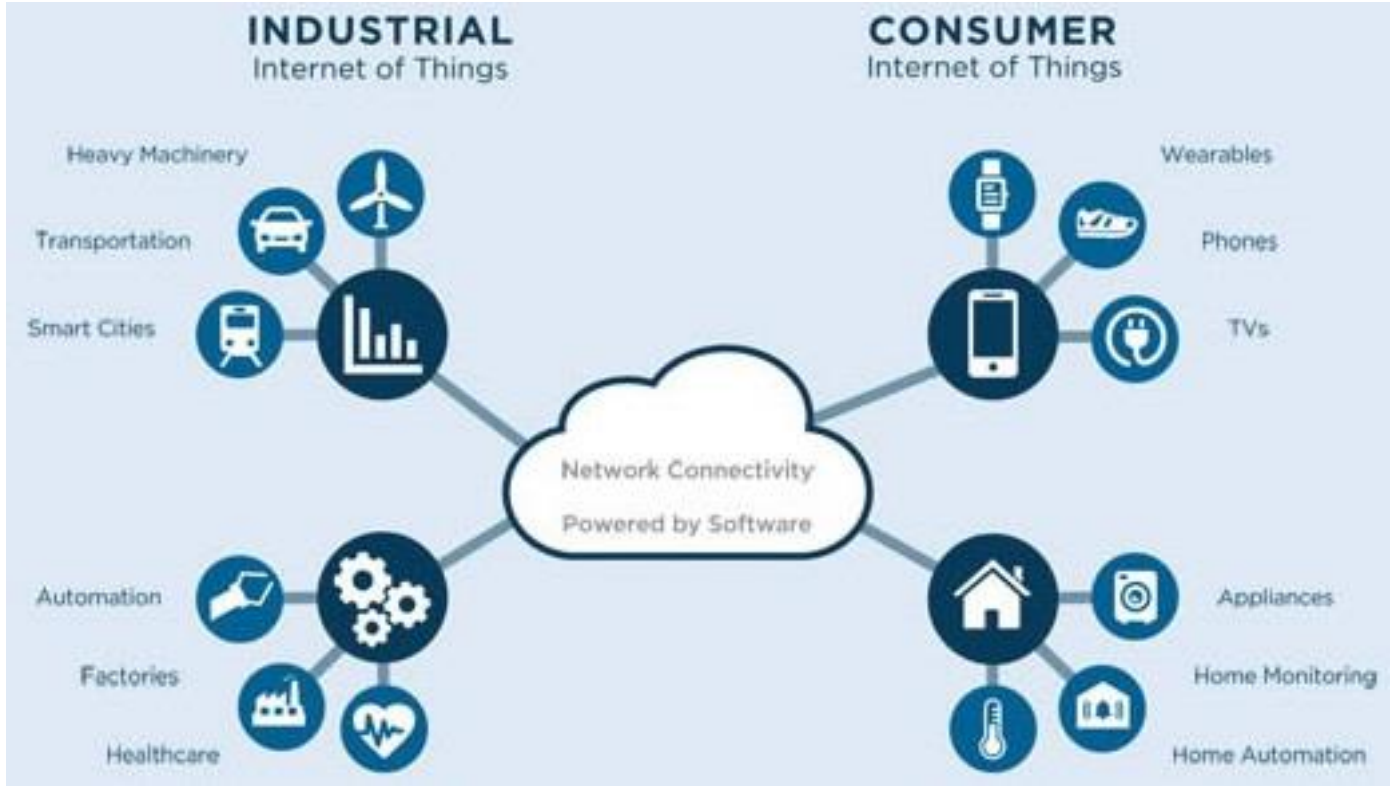
we explore the **emerging interaction** between the payment needs of the **M2M Economy** and the worldwide investigation into **digital fiat money**

we propose a **preliminary model of integration** between a **two-tier retail CBDC architecture** and **Consumer IoT**

Background
Consumer Internet of Things

Outline

- **Internet of Things (IoT)** -> objects embedding sensors and processing capabilities that exchange information with other objects, systems, people through the Internet, in order to provide a **new class of services** defined **"smart"**
- **Consumer IoT (CIoT)** -> subset of smart devices and IoT systems used by individuals that provide **personalized services**



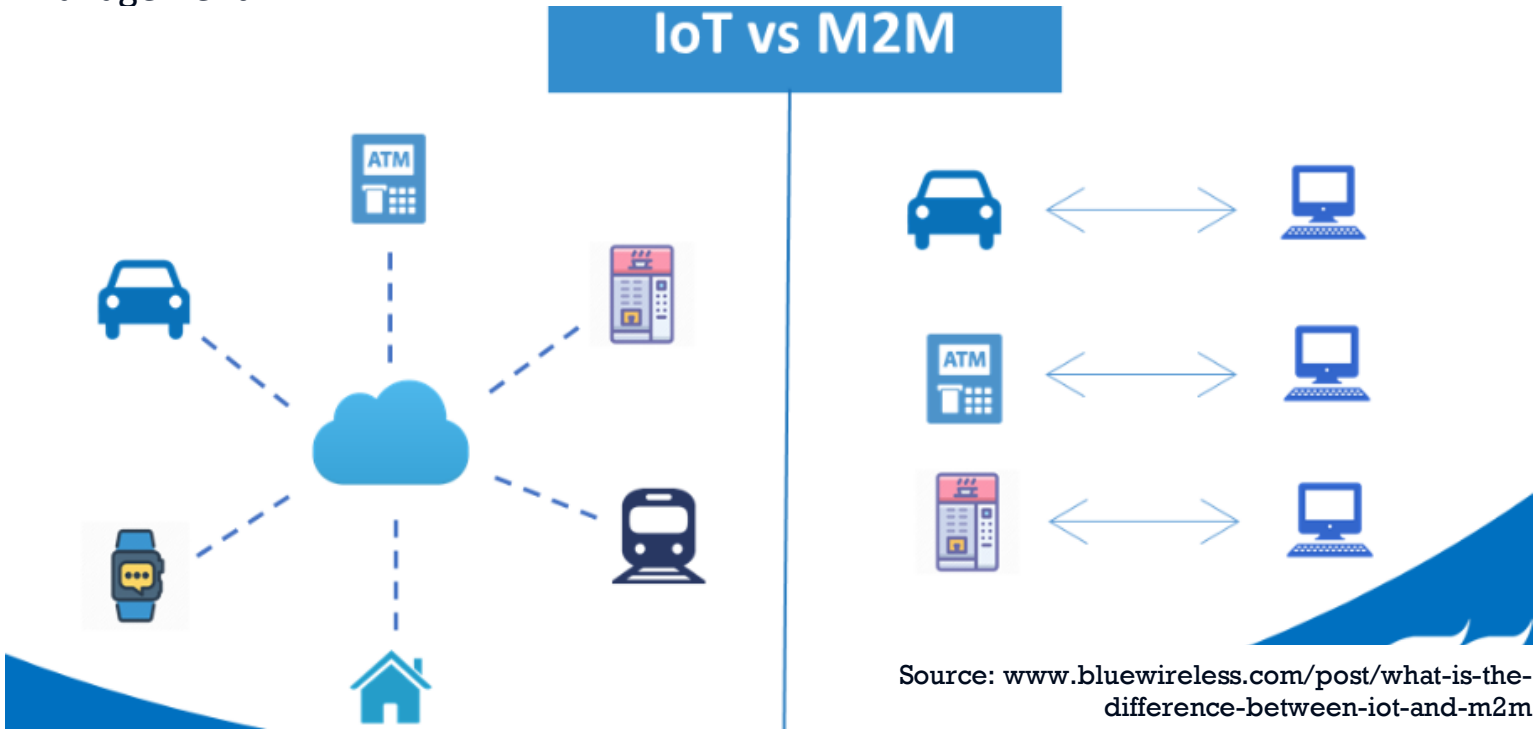
Source: pyxis.cat/internet-industrial-de-les-coses-iiot/

Background

Machine-to-Machine Communication

Outline

- **Machine-to-Machine (M2M)** techniques allow (C)IoT devices to **directly** communicate, or relay information, over a protocol.
- Communications -> **without or with limited human intervention**, between computers, embedded processors, smart sensors, actuators and mobile devices.
- **M2M + IoT** -> **machines (inter)acting autonomously** ->
  security monitoring, vehicle theft protection, mechanical maintenance, transport management…



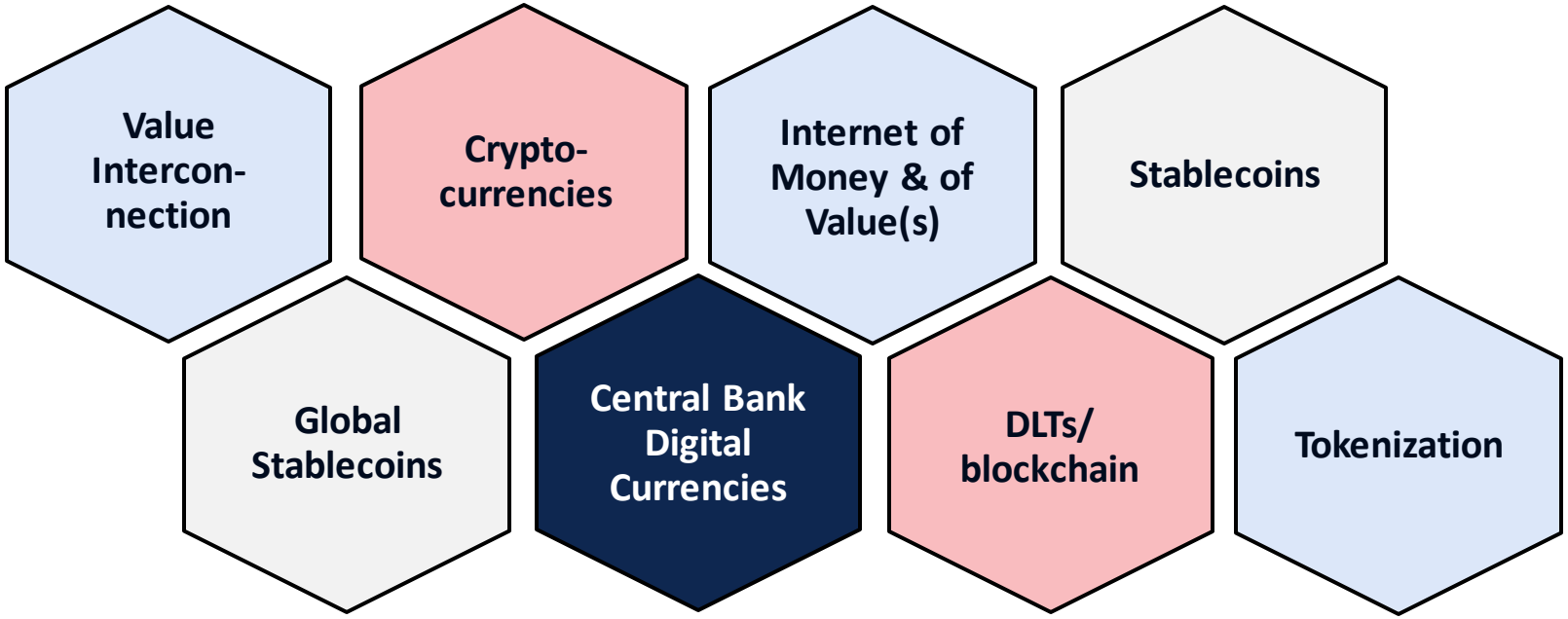
Source: www.bluewireless.com/post/what-is-the-difference-between-iot-and-m2m

Background
Distributed Ledger Technologies

Outline

strengths offered by recording information in a partially/fully **open**, **distributed** and **cryptographically constrained ledger**

- **Data integrity**
- **(Decentralization)**
- **Availability**
- **Automation**



Background

(Retail) Central Bank Digital Currencies [1/2]

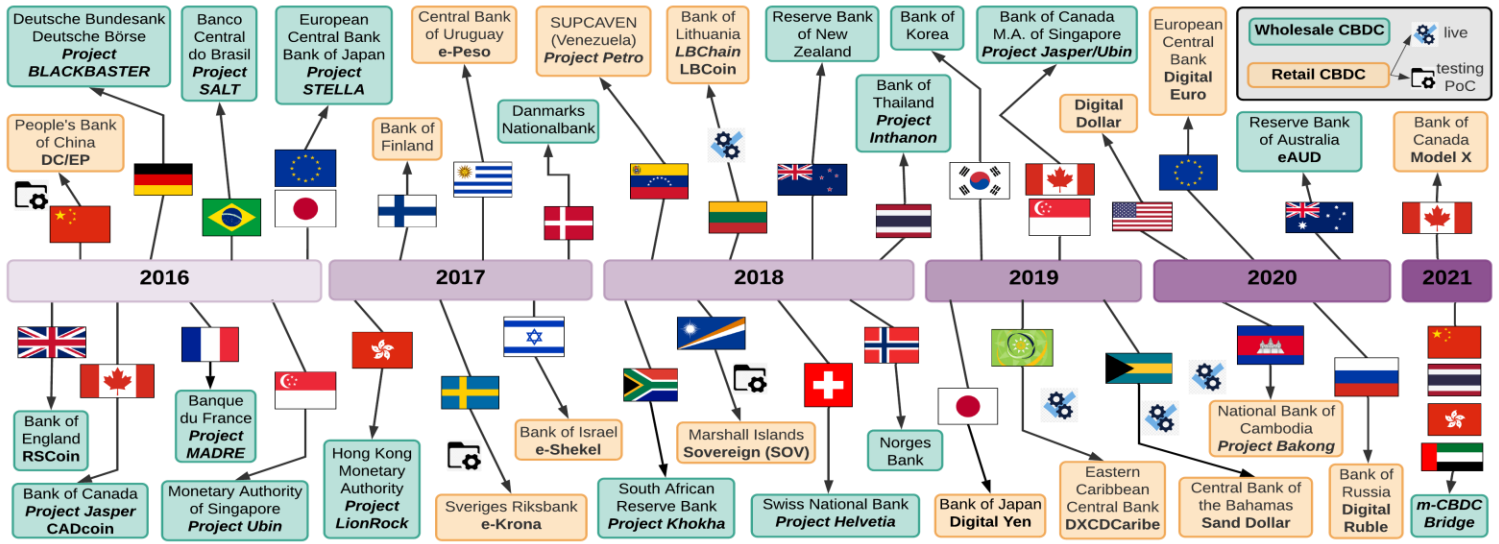
Outline

according to BIS, **86%** of **central banks** were exploring **CBDCs** at the beginning of 2021

- ***wholesale***
- ***retail / general purpose***

- **tokenized** and **natively digital** version of **fiat money**
- **sovereign currency, legal tender**
- available to the **general public**
- most **transformative** CBDC type
- "**digital cash**"

two types of CBDCs **<-> two** types of "*central bank money*"



Global roadmap on major *wholesale* and *retail* CBDC projects

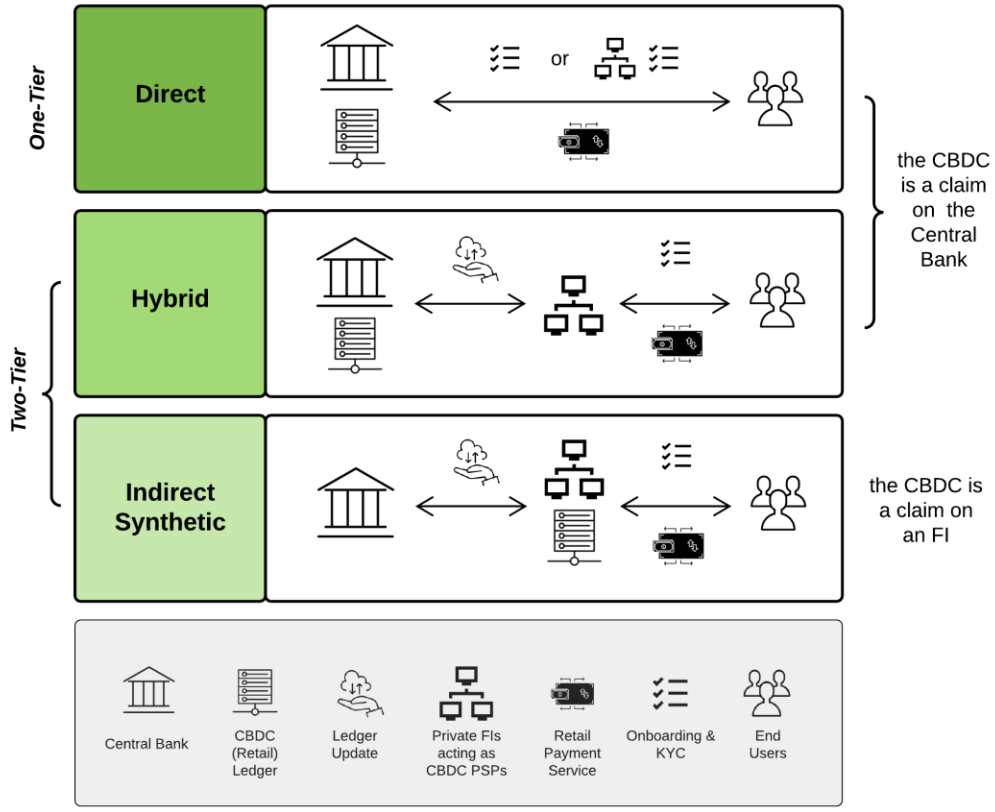
from: Pocher N, Veneris A (2021) *Privacy and Transparency in CBDCs: A Regulation-By-Design AML/CFT Scheme.* IEEE Transactions on Network and Service Management. Forthcoming

Background
(Retail) Central Bank Digital Currencies [2/2]

Outline

there is a **broad variety of CBDC designs** -> manifold techno-legal and standardization policy questions

- **one-layered** or **two-layered**
- schemes may involve **public** and **private stakeholders**
- **not all CBDC models are DLT-based**, but in our work we focus on DLT-based architectures
- **token-** & **account-based**
- **hardware-** & **software-based**
- **offline usability**
- **cross-border** and **cross-currency** projects (mCBDC bridge)



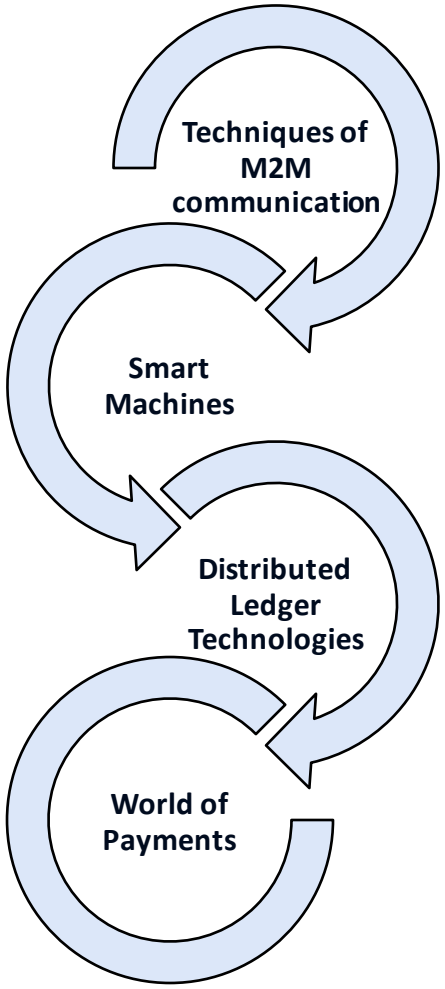
CBDC Architectures
from: *Pocher N, Veneris A (2021) Privacy and Transparency in CBDCs: A Regulation-By-Design AML/CFT Scheme*. IEEE Transactions on Network and Service Management. Forthcoming

M2M Payments in Consumer IoT

M2M and the Economy of Things

Outline

- a future may be envisioned where **"smart" machines (inter)act autonomously** from an **economic** perspective
- "**Machine Economy**", "**Economy of Things**", "**M2M Economy**"
- **e-devices exchanging data** and **services without** (or with limited) **human intervention** (*e.g.*, confirmation) -> the **need** emerges for **machines** to **handle payments**
- **M2M Payments** = integration of payment processes into an automated processing of business transactions
- a "M2M Economy" is **inherently decentralized** and based on the **autonomy of its participants**
- need of a **decentralized** and **self-managed payment system**
- **huge amounts** of **personal** and **sensitive data**
- **DLTs** and **smart contract-based programmability** aid the M2M economy to reach its full potential (*e.g.*, scalability; efficiency, security <- defined conditions for value transfers)

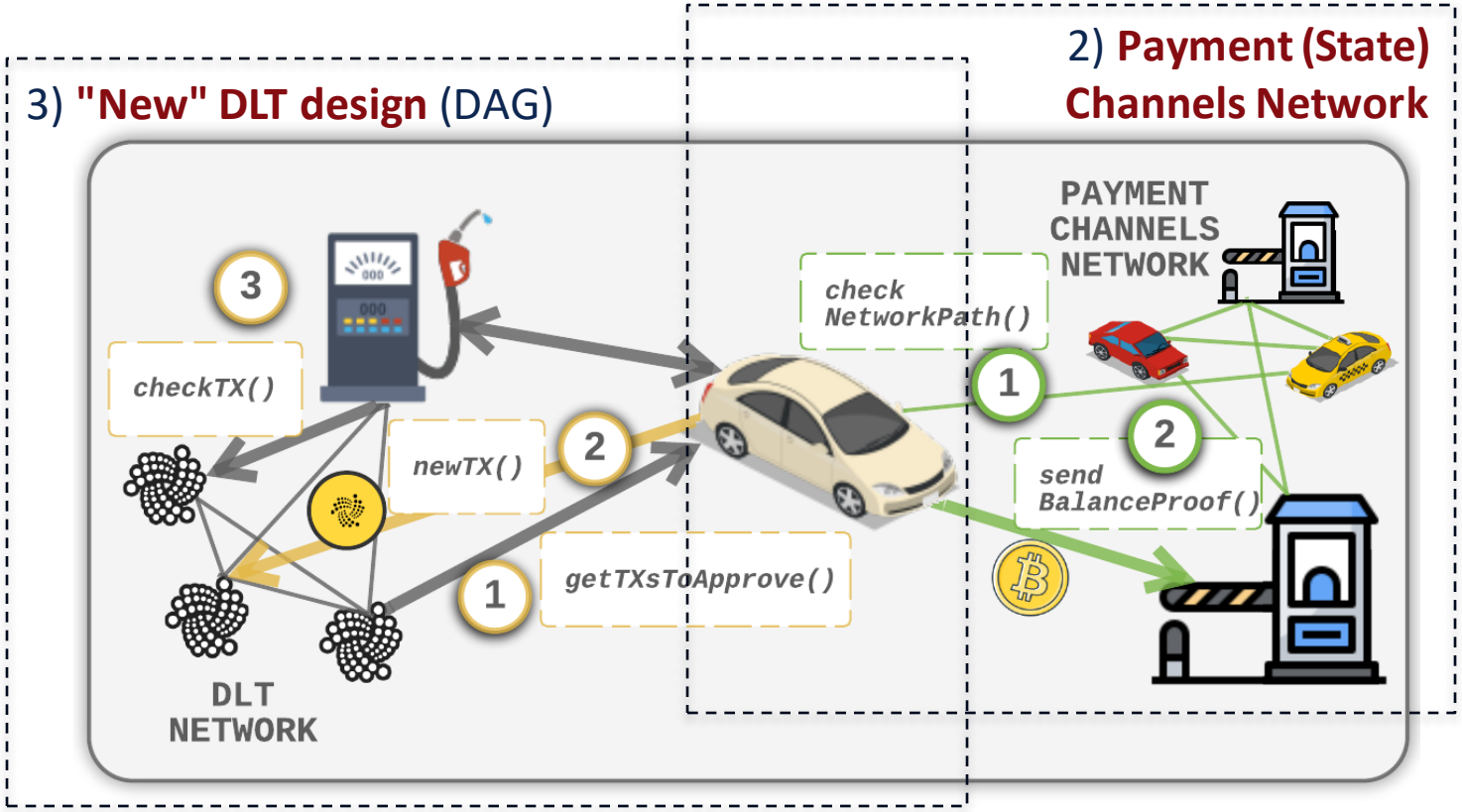


M2M Payments in Consumer IoT

Cryptocurrencies applied to CIoT

Outline

Cryptocurrencies applied to (C)IoT
from: *Pocher N, Zichichi M (2021) Towards CBDC-based Machine-to-Machine Payments in Consumer IoT*. Under Review. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3974838



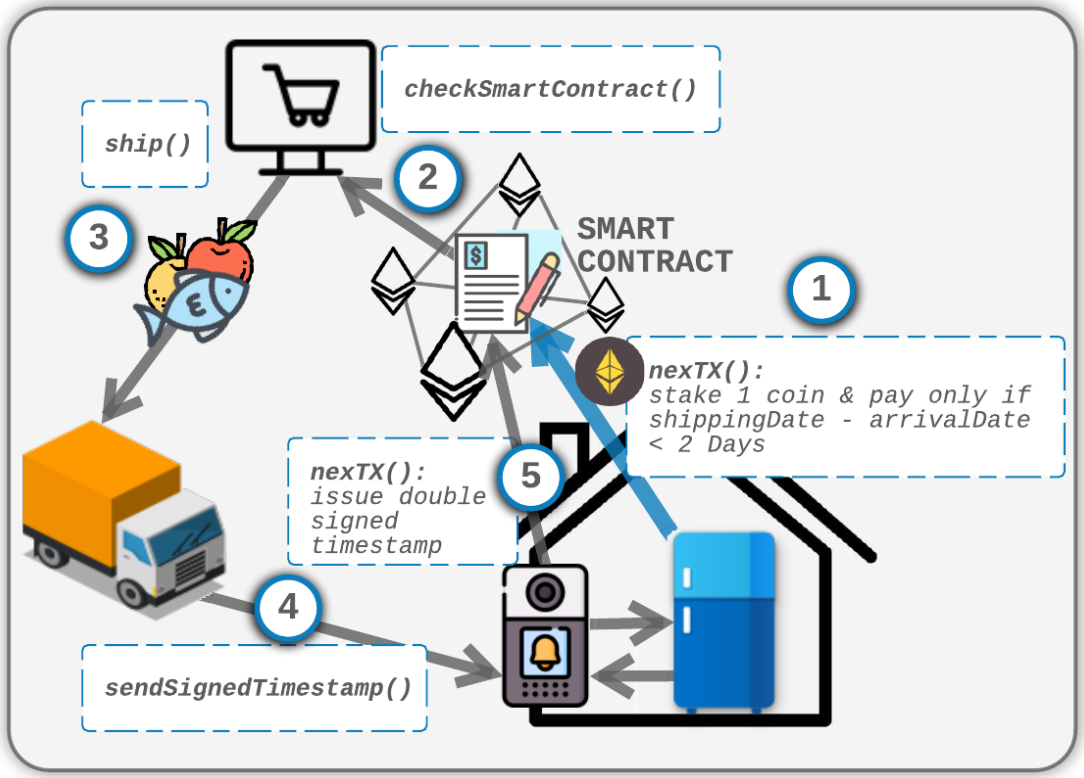
"weird" fact: CIoT and cryptocurrencies have largely developed in silos

M2M Payments in Consumer IoT

Programmability in M2M Payments

Outline

1) Direct Integration



Programmability in M2M Payments

from: *Pocher N, Zichichi M (2021) Towards CBDC-based Machine-to-Machine Payments in Consumer IoT.* Under Review. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3974838

Retail CBDC-based M2M Payments

E-Fiat Money and the M2M Economy

Outline

consumer/retail payments in CBDCs -> next major development in digital payments

key role of **decentralization** in the **M2M economy** and **(C)IoT** -> BUT in some scenarios it cannot be provided at the **governance level**

given the **stakeholders** involved in **CBDC schemes**, the tendency is to **centralize governance** while maintaining **decentralisation** of **systems** and **device communication**

CBDC research has pinpointed **policy objectives** -> some **core characteristics** that are a **priority for CBDC designs** seem to fit **CIoT** and the **M2M Economy**

- **trade-off** between (i) privacy and data protection and (ii) compliance with other sets of regulations such as anti-money laundering
- **universal & unrestricted accessibility** (*e.g.*, geographical location, means)
- **resilience**: providing continuous operation online and offline
- **security**: offering products/services resistant to cyberattacks
- **high performance**: ensuring scalability for daily use

Retail CBDC-based M2M Payments

CBDCs and Programmable Micro-Payments

Outline

limits of **traditional cryptocurrency designs** when applied to **micro-payments** in CIoT

consensus mechanisms (*e.g.*, PoW in Bitcoin) **VS. resource-constrained devices** -> scalability, transaction fees and block confirmation times

could specific CBDC models overcome these limits in (C)IoT scenarios?

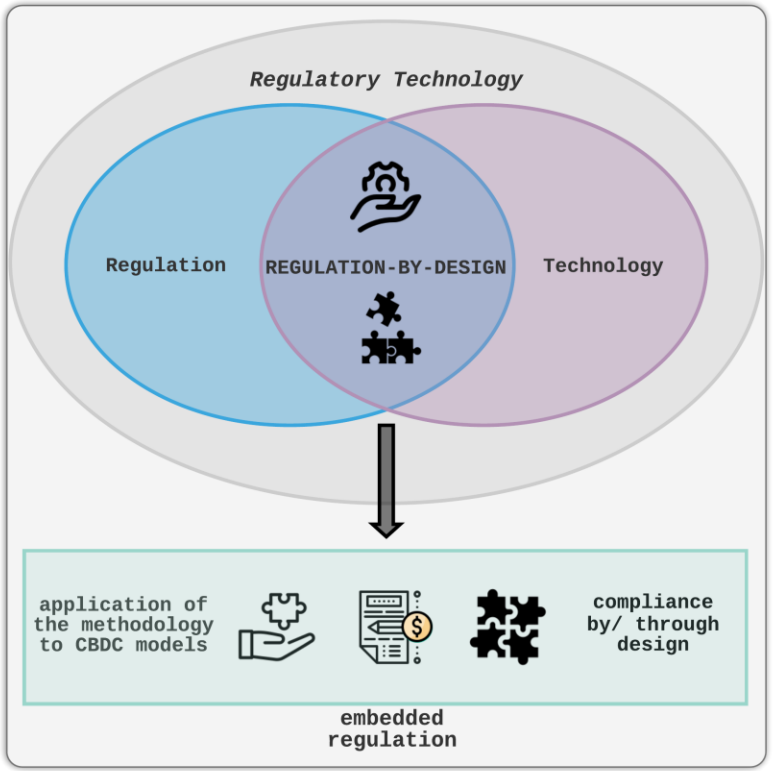
- could CBDCs **support micropayments** as required by **(C)IoT applications**?
- a **"native" instrument** integrated into the DLT platform -> **real-time settlement of payments** in (C)IoT scenarios
- **programmability**: **predefined payments** and **automated processing**
- a **DLT** as the underlying **platform for both the process and the payment**: delivery vs. payment
- use of **smart contacts**: P2P M2M low-value transactions when there is a **high third-party trust cost**

Retail CBDC-based M2M Payments

Regulatory Methodology and Compliance

Outline

- the deployment of digital currencies in CIoT generates **manifold regulatory hurdles**
- **normative frameworks** for **device-to-device transactions**
- adequate **standardization**
- **legal effects** of smart communication & **frameworks** of **"machine identities"**
- unsuitability of **ordinary safeguards**: *e.g.*, two-factor authentication
- **interest in CBDCs** & opportunity to **define normative goals** at the **beginning** of the **process** -> **design-based techniques**
- **technical** and **legal aspects** tackled **jointly**, expert groups, standardization
- **inherent automation** of CIoT requires a **payment system compliant by design**



Regulation by Design
from: *Pocher N, Zichichi M (2021) Towards CBDC-based Machine-to-Machine Payments in Consumer IoT*. Under Review. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3974838

Retail CBDC-based M2M Payments

Privacy-Transparency Trade-Offs

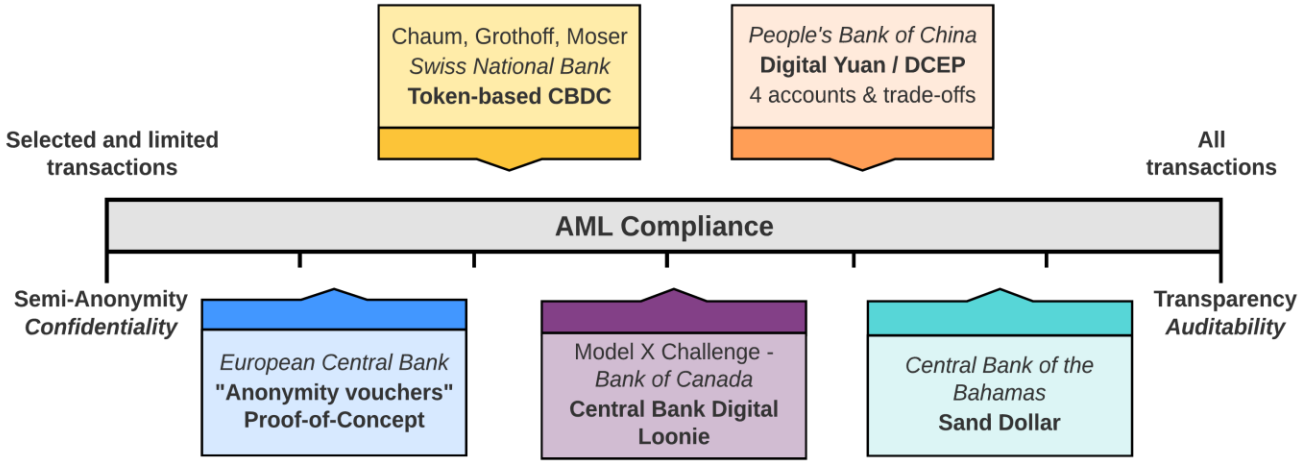
Outline

design choices are **never binary**

privacy vs. transparency is **not** a **zero-sum game**

trade-offs are found in **all means** of **payments**

digital currencies & **program-mability: new forms** of **control** and **disclosure**



Selected CBDC projects from an AML compliance standpoint, from *accountable anonymity* to *transparency*
from: *Pocher N, Veneris A (2021) Privacy and Transparency in CBDCs: A Regulation-By-Design AML/CFT Scheme.* IEEE Transactions on Network and Service Management. Forthcoming

main examples of specific trade-offs

- **fully-transparent CBDC** with real-world identity transactions fully visible to law enforcement
- **privacy without any limitation**: no information can be revealed, vulnerability to illicit misuse
- **nuanced solutions**: some privacy to consumers (*i.e.*, **confidentiality**) & some visibility to authorities (*i.e.*, **auditability**)

Integrating CBDCs and CIoT

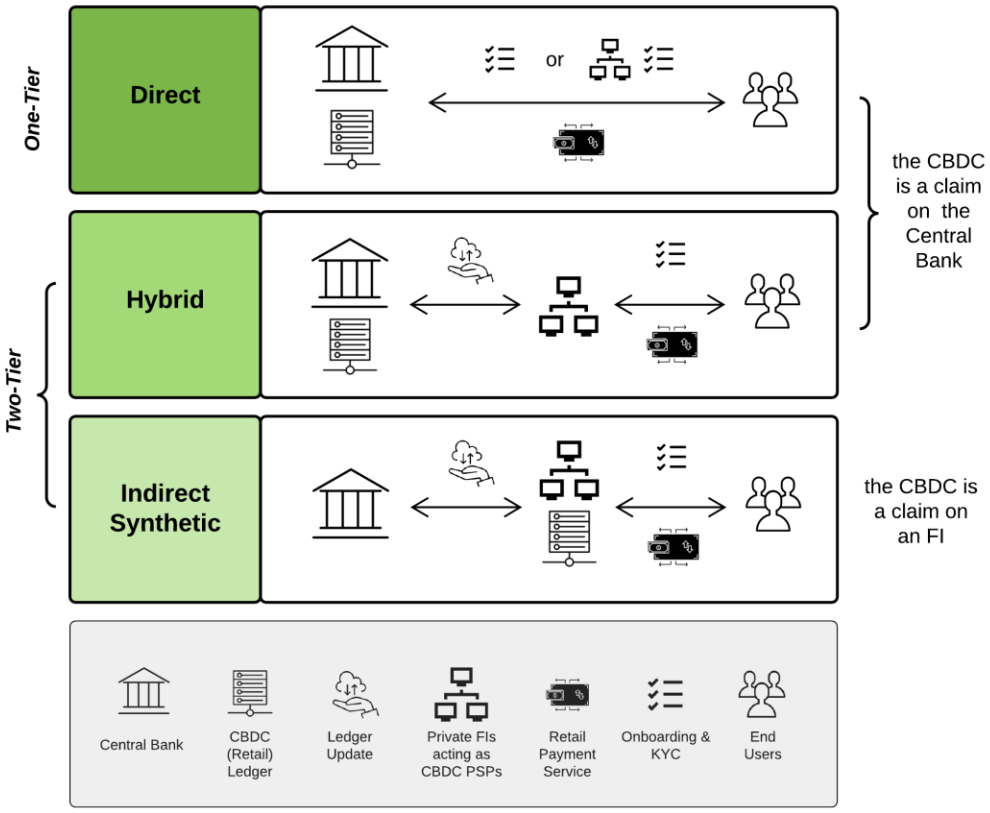
The Role of CBDC Architectures

Outline

Architectures from the perspective of the participating entities:

- **One Tier – Direct**: the model requires only the involvement of the central bank to offer retail services and manage client relationships
- **Requires central banks to initiate and continuously attend to the relationship with end-users** -> it falls largely **outside of their traditional competences**

- **Two Tier – hybrid, intermediated, synthetic**: cooperation with private financial institutions
- Users interact, e.g., open their accounts, with intermediaries
- **The ledger is maintained by the central bank (hybrid) or by financial intermediaries (synthetic)**



CBDC Architectures

from: *Pocher N, Veneris A (2021) Privacy and Transparency in CBDCs: A Regulation-By-Design AML/CFT Scheme*. IEEE Transactions on Network and Service Management. Forthcoming

Integrating CBDCs and CIoT

A CBDC Wallet for a CIoT Device

Outline

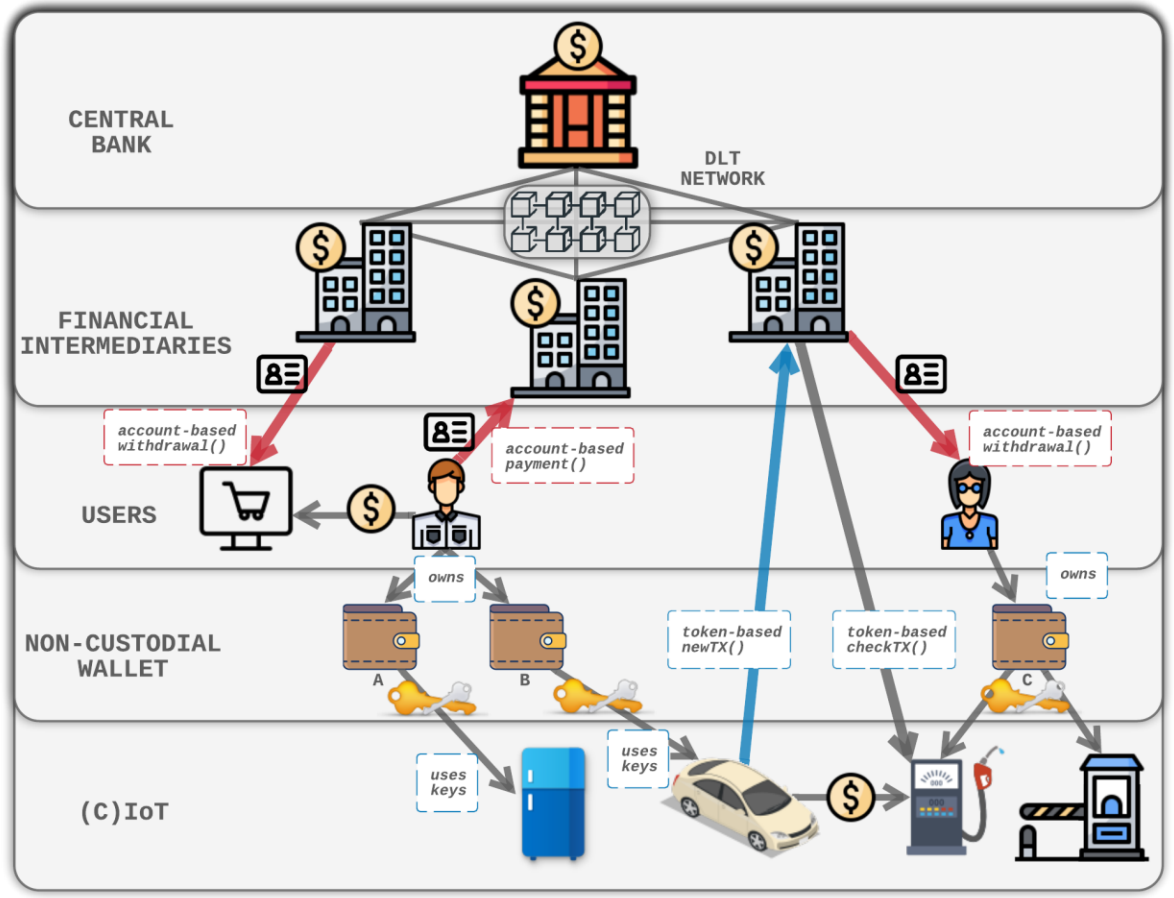
CBDC architectures can deploy **different types of wallets**, through which end-users' devices interact with the ecosystem:

- **Account-based vs token-based wallets** - account-based access is tied to an *identity system*; whilst token-based access is tied to a *cryptographic scheme*.
  M2M communication + account-based -> payment limited by the user authentication.
- **Hardware-based vs software-based wallets** – security based on the *technologies built in the device* making the payment vs. security based on *cryptography and sw protocols*.
  The choice depends on the operation scenario -> security vs. scalability.
- **Custodial or non-custodial wallets** – custodial means *third party operates the wallet* and holds the private keys, while in non-custodial *end-users hold the private keys directly*.
  Non-custodial wallets + CIoT devices -> for Payment Channels and New DLT Design
- **Parent wallets and sub-wallets** - holders can have a *main wallet* as parent wallet and *several sub-wallets* to set payment limits or conditions. **CIoT+sub-wallet -> autonomy**.
- **Offline usability** - *trade-off* between hardware/software *security, costs, and convenience*.
  Tamper-proof hardware for store small amounts of CBDCs?

Integrating CBDCs and CIoT

A CBDC Model Integrating CIoT and M2M

Outline



Preliminary integration scenario of CIoT and a two-tier retail CBDC system
from: *Pocher N, Zichichi M (2021) Towards CBDC-based Machine-to-Machine Payments in Consumer IoT.* Under Review. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3974838

Integrating CBDCs and CIoT

Embedded Trade-Offs

Outline

CBDC research

- **privacy-transparency trade-offs** -> "**mixed solutions**" with the goal of offering **anonymity** & a desirable level of **privacy**
  - **multiple wallet options** tailored to **different types of transactions**
  - **anonymity-oriented wallets** (usually *token-based*): transactions do not require identity information, **BUT** there are **limits** (*e.g.*, amounts & types of transactions) to mitigate the risks
- **users** shall have the option to **hold CBDC tokens outside of custodial relationships** + **tokens not linked** to **addresses** or **identifiers** <- **privacy-by-design**

this model + risk mitigation (*i.e.*, limits) appear **suitable to the needs of the CIoT** -> in a **scheme of tiered wallets**

Conclusions

Key Take-Aways

Outline

1. Background
2. M2M Payments in Consumer IoT
3. Retail CBDC-based M2M Payments
4. Integrating CBDCs and CIoT
5. **Conclusions**

☆ possible model for a **retail CBDC system** integrated with **M2M & CIoT dynamics**

☆ **regulation-by-design** & **compliance-by/through-design**

☆ integrating CBDCs, M2M payments & CIoT requires **multi-stakeholder-based standardization** -> **CBDC projects** **provide an invaluable opportunity**

☆ the deployment of **DLTs** is **conducive to embedding** desired **trade-offs**

multi-layered model of integration

two-tier CBDC architecture

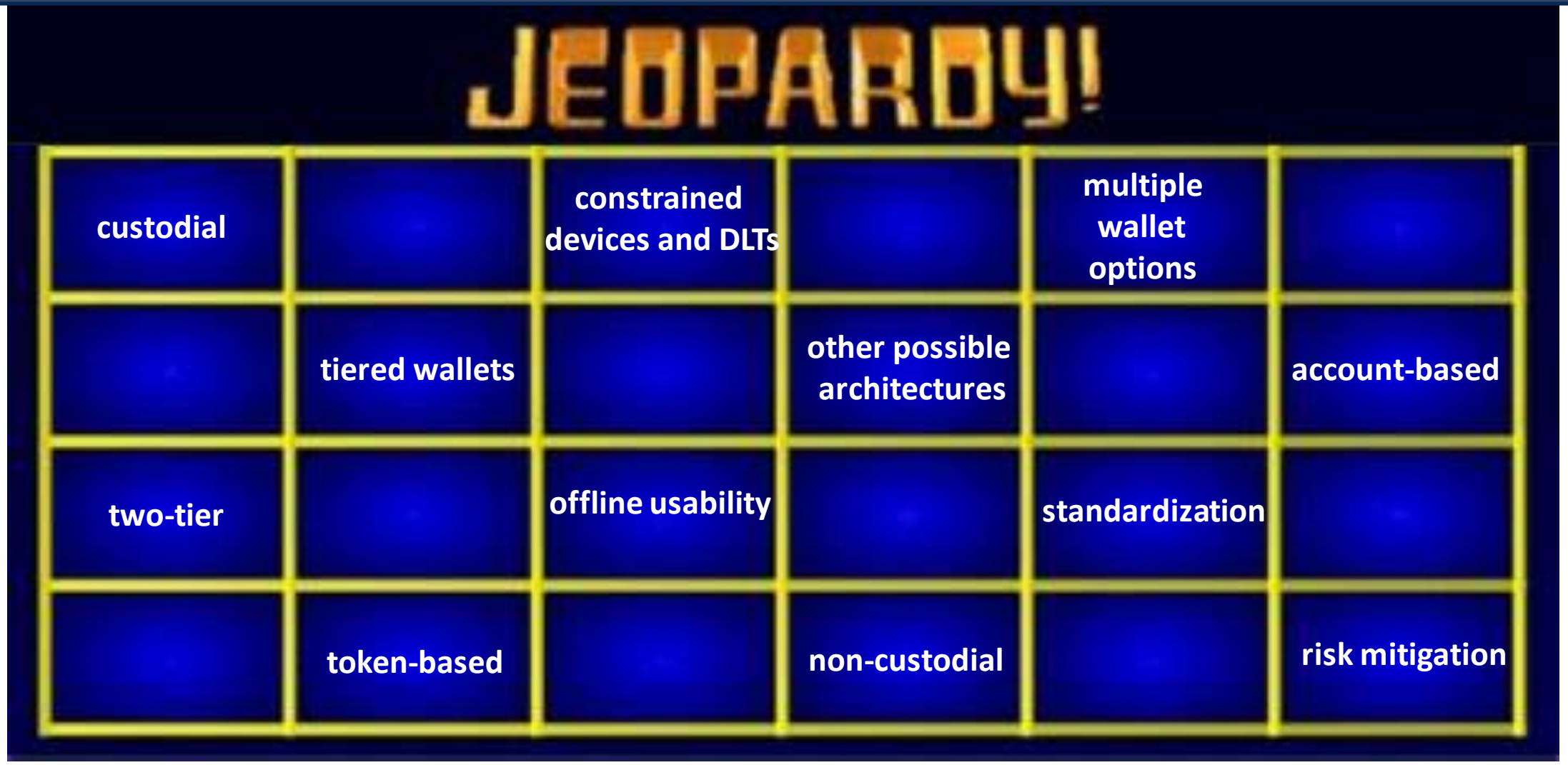
machines -> **non-custodial** **token-based** **sub-wallets** with a **given (limited) budget** -> smart devices can automatically and independently perform payments in native e-fiat money

end-users -> **custodial** **account-based** **parent wallets** that rely on authentication and **control the devices' wallets**

Thank you very much for your attention!

nadia.pocher@uab.cat
mirko.zichichi2@unibo.it

Open Issues


JEOPARDY!
custodial
constrained devices and DLTs
multiple wallet options
tiered wallets
other possible architectures
account-based
two-tier
offline usability
standardization
token-based
non-custodial
risk mitigation