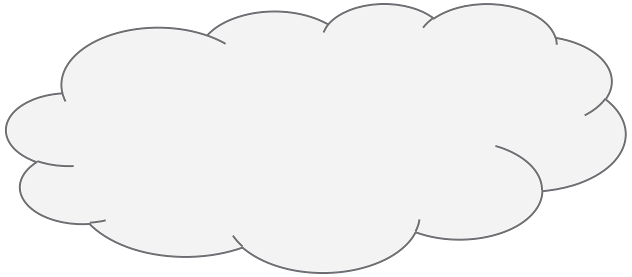
Mikolai Gütschow <mikolai.guetschow@tu-dresden.de>

Digital Payments for the Internet of Things

Towards E-Cash for Low-End IoT Devices

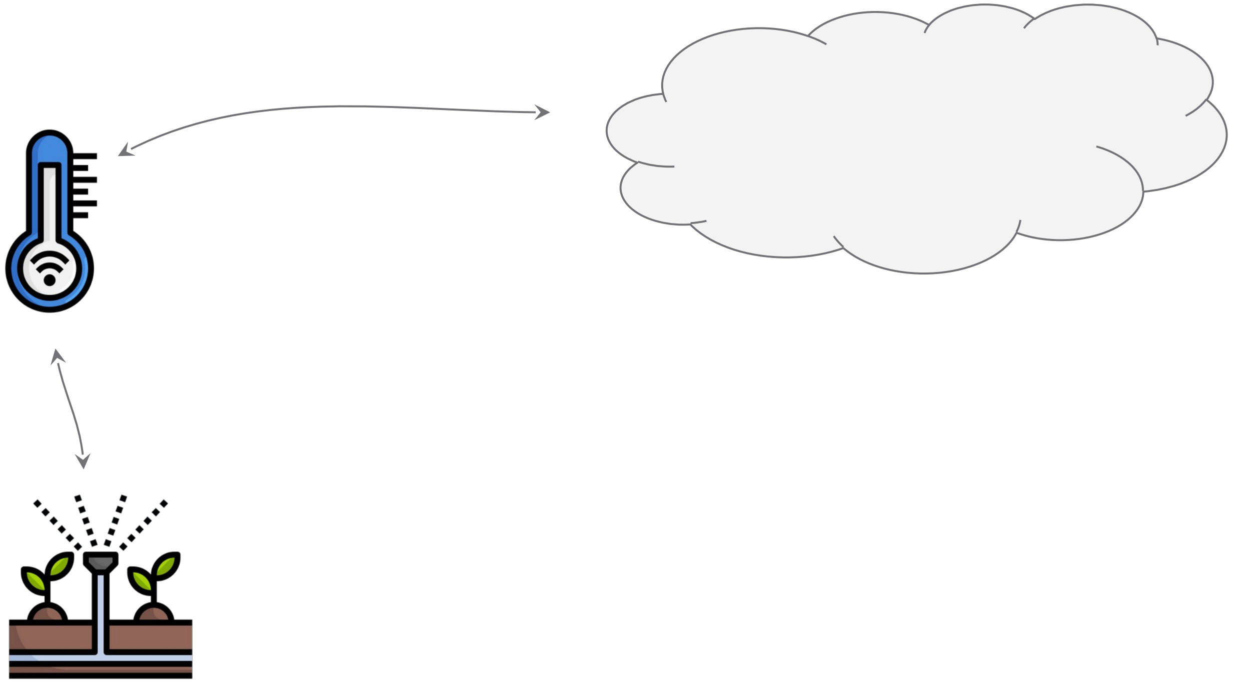
RIOT Summit // 2024-09-06

Internet of Things (IoT)



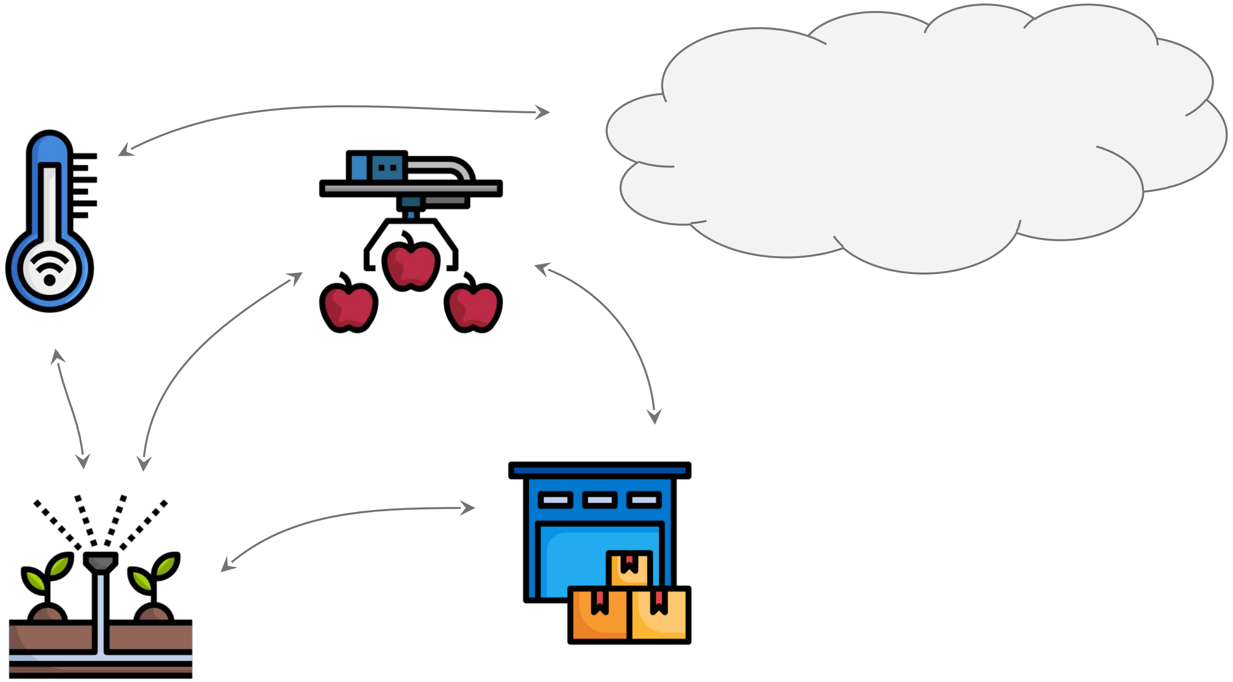
Internet of Things (IoT)

Smart Farming



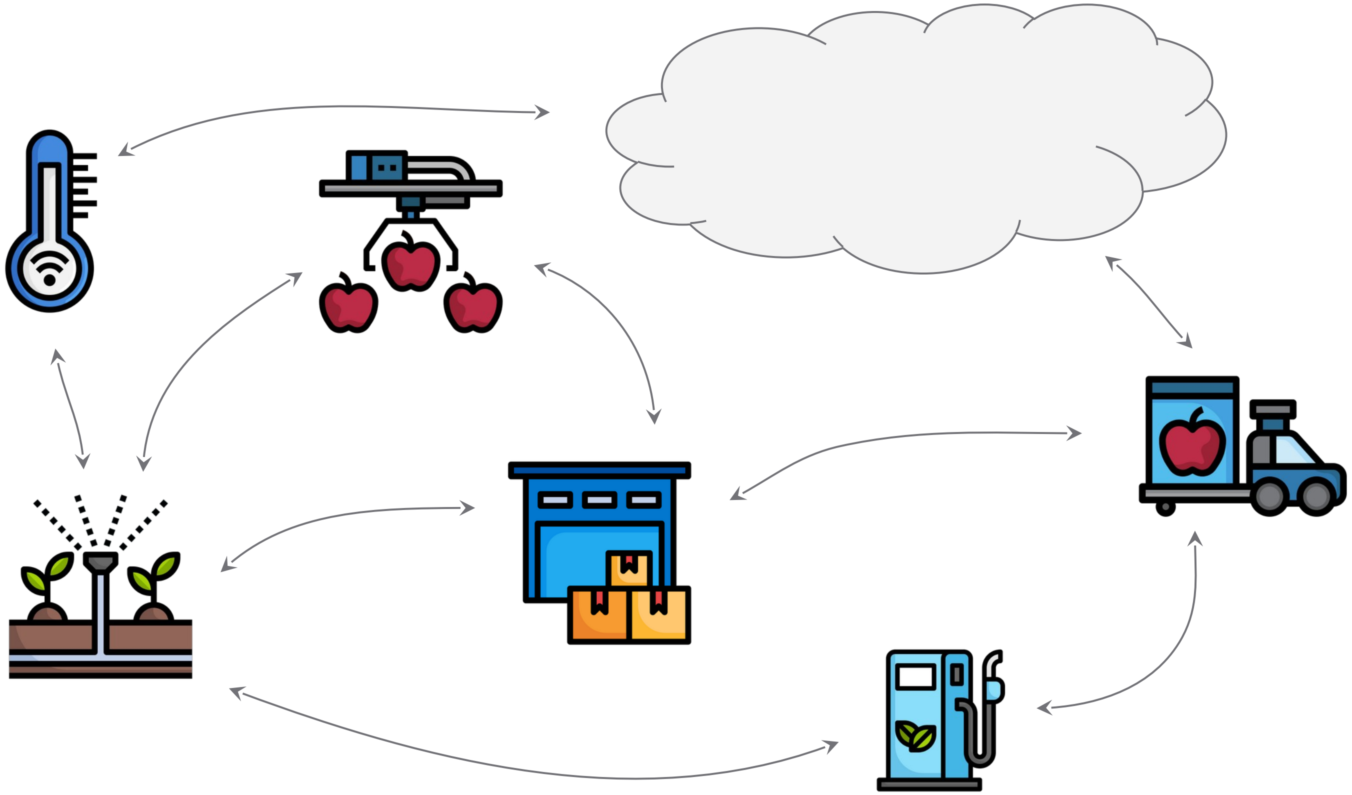
Internet of Things (IoT)

Smart Factory



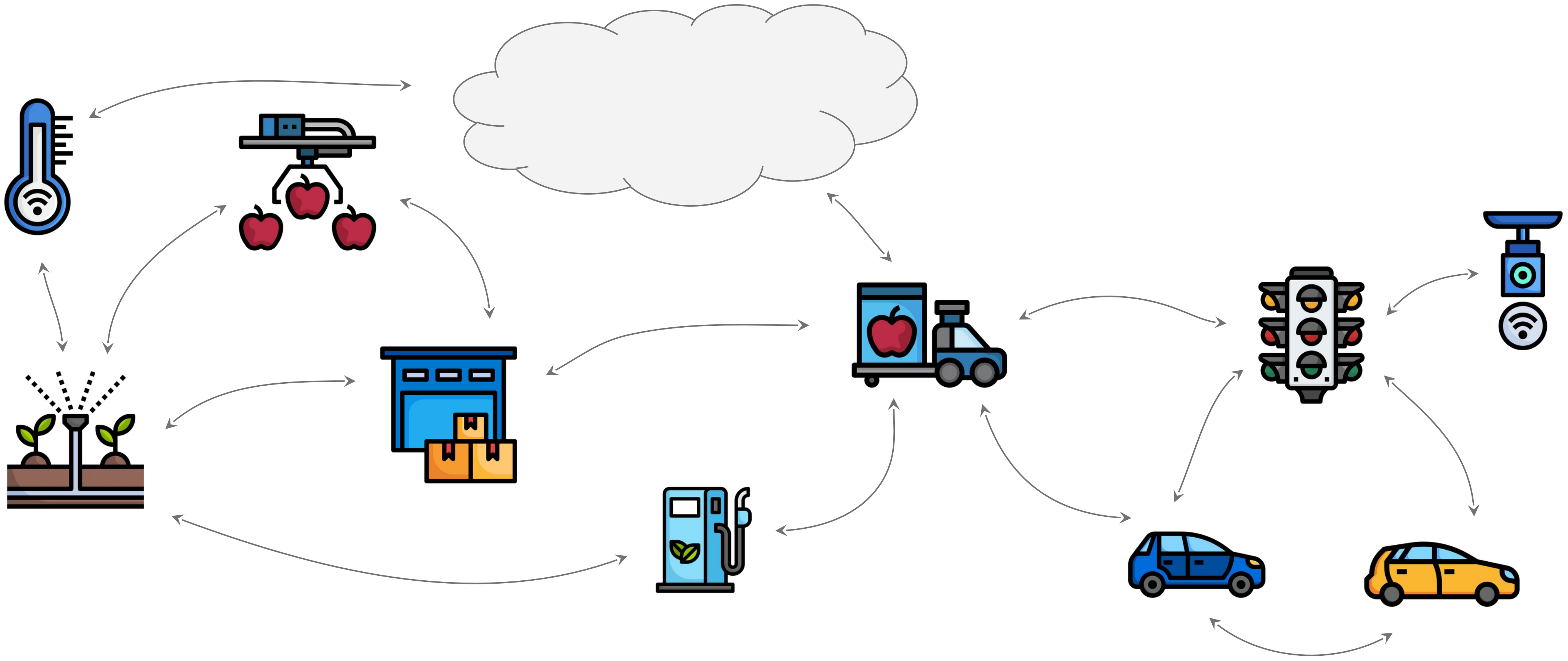
Internet of Things (IoT)

Smart Logistics



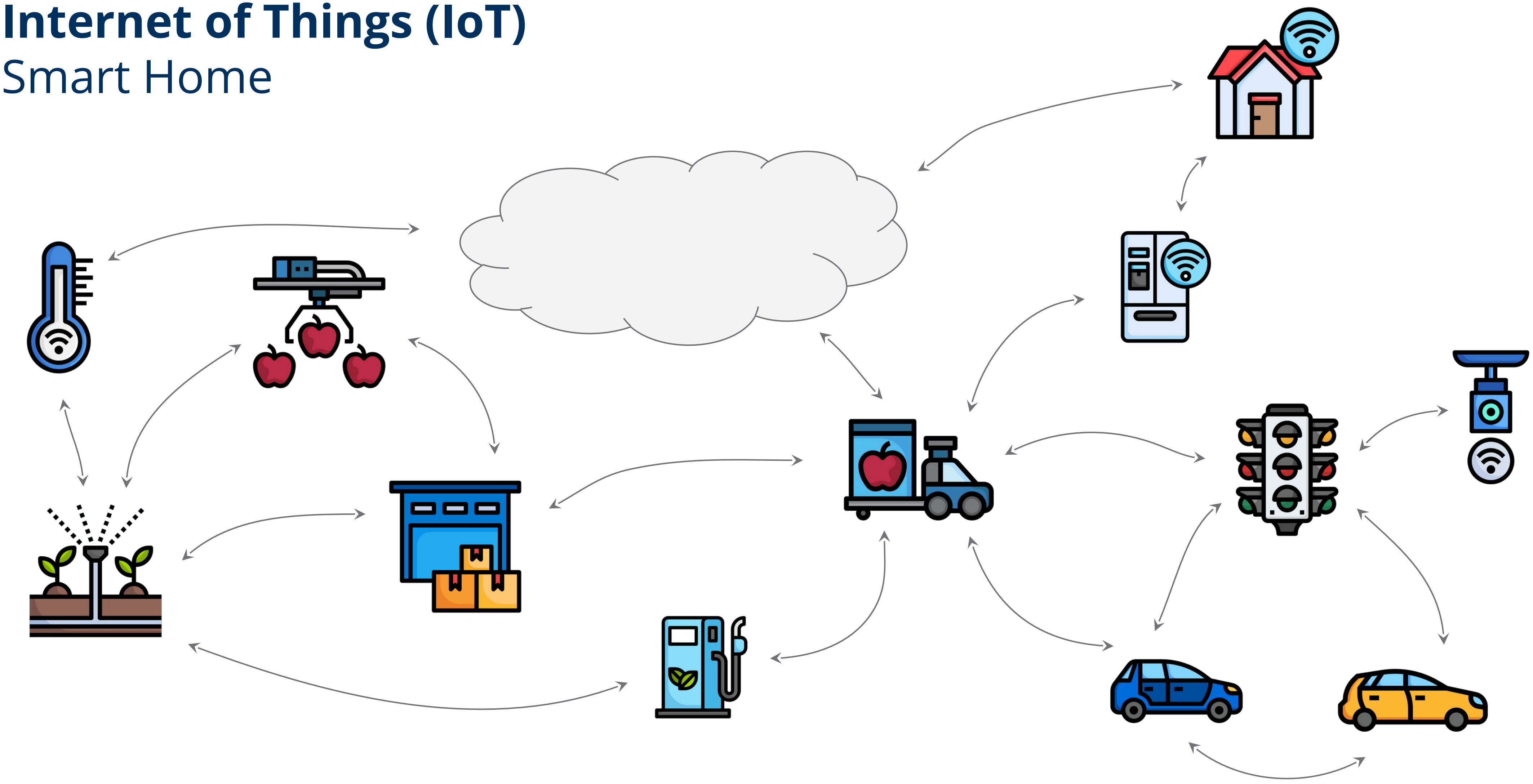
Internet of Things (IoT)

Smart City



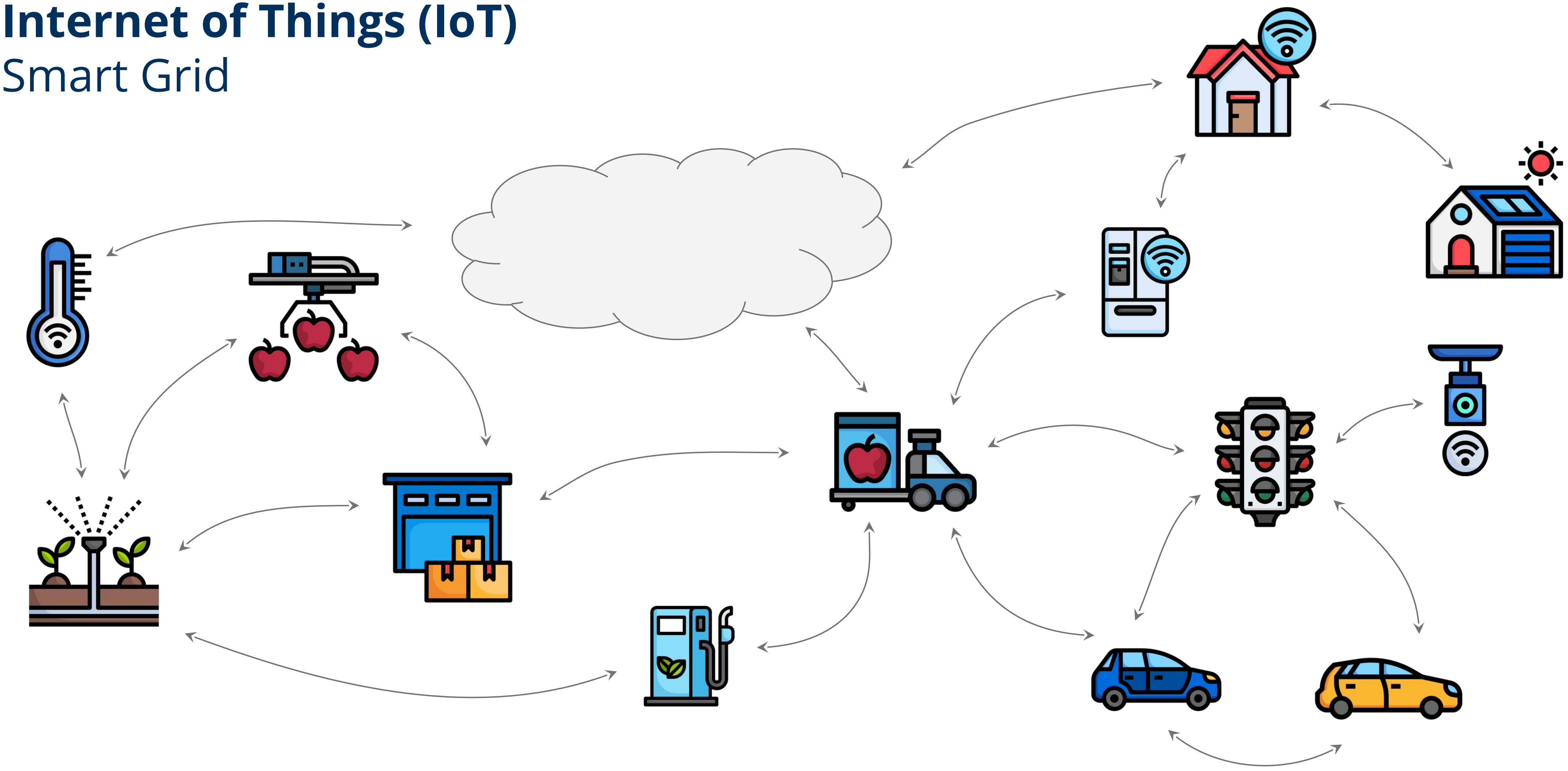
Internet of Things (IoT)

Smart Home



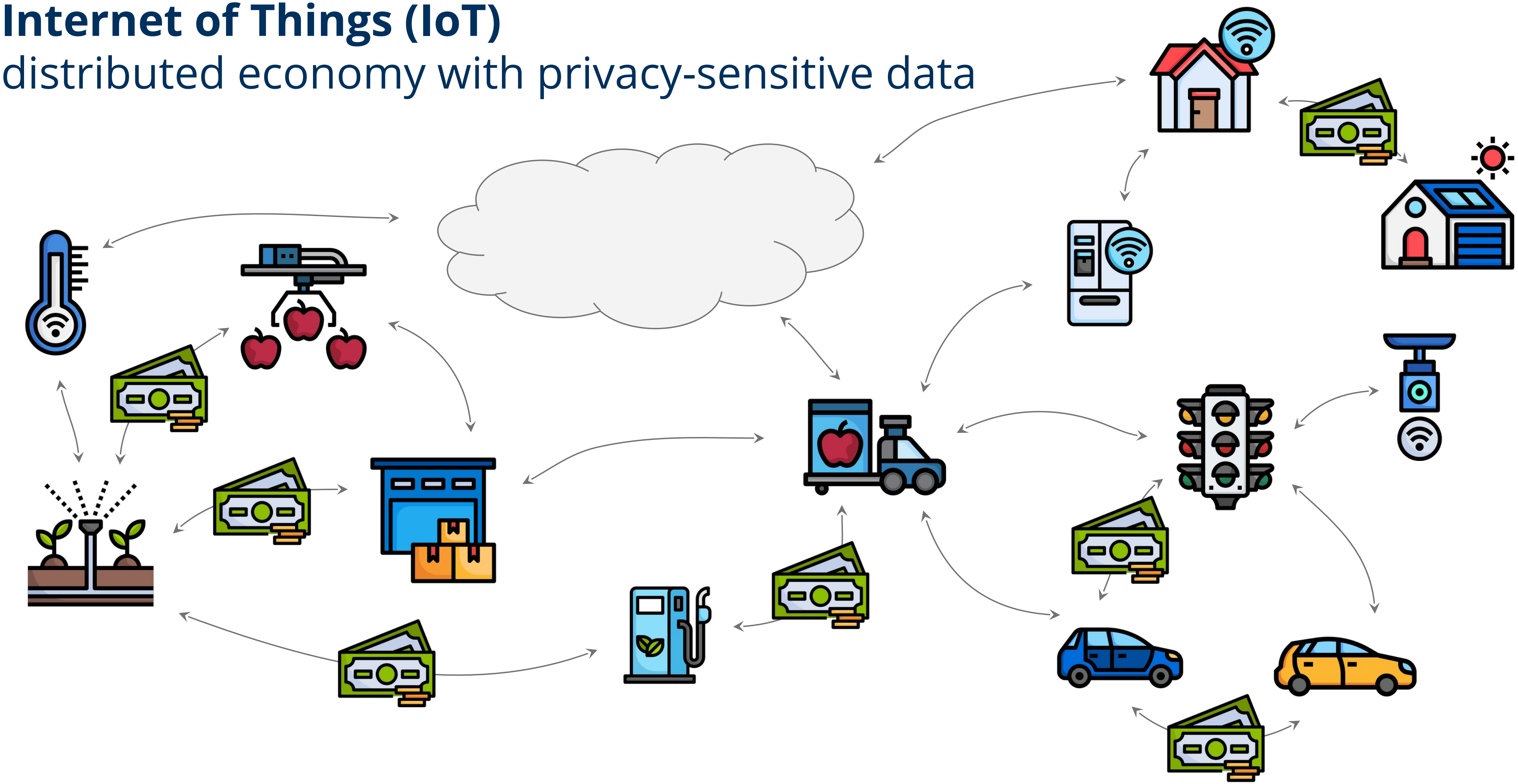
Internet of Things (IoT)

Smart Grid



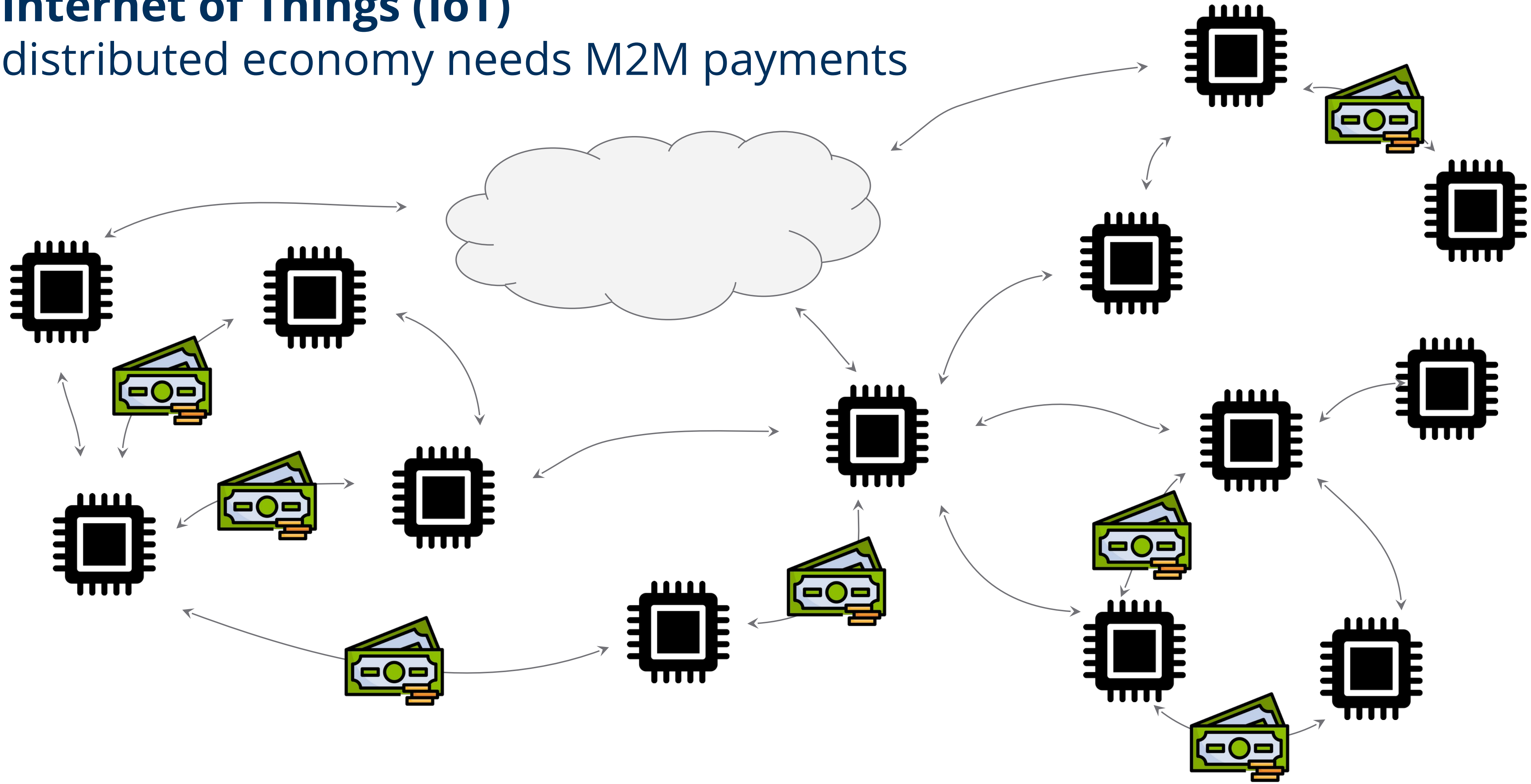
Internet of Things (IoT)

distributed economy with privacy-sensitive data



Internet of Things (IoT)

distributed economy needs M2M payments



Outline

Motivation: payments for a distributed IoT economy

The many faces of IoT

Suitable payment systems for the IoT

A typical e-cash scheme: GNU Taler

IoT e-cash wallet challenges and proposed solutions

The many faces of IoT
30 billion devices by 2030

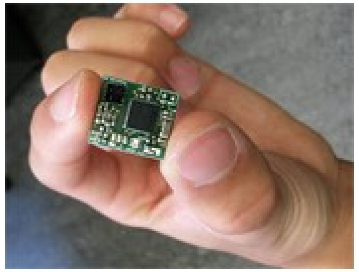
High-end IoT

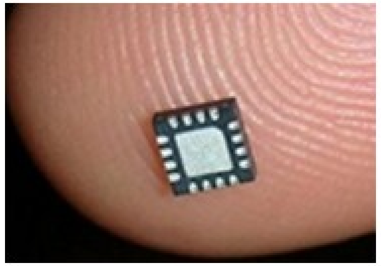
Linux

android

Processor: GHz, 32/64 Bit
Memory: MB/GByte
Energy: Watt
Network access: 5G, WLAN
Price: 10-100€

Low-end (or constrained) IoT



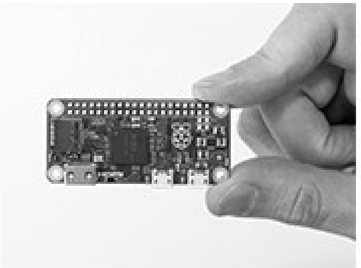


RIOT

Processor: MHz, 8/16/32 Bit
Memory: kByte
Energy: mWatt
Network access: 802.15.4, BLE
Price: 0,10-10€

The many faces of IoT
we focus on the challenging class of devices

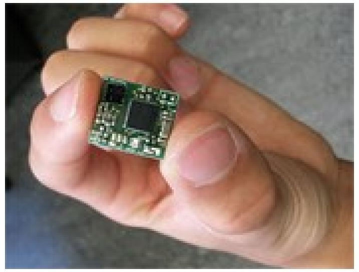
High-end IoT

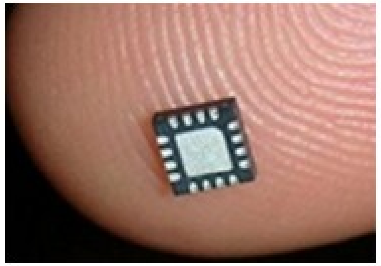


Linux android

Processor: GHz, 32/64 Bit
Memory: MB/GByte
Energy: Watt
Network access: 5G, WLAN
Price: 10-100€

Low-end (or constrained) IoT



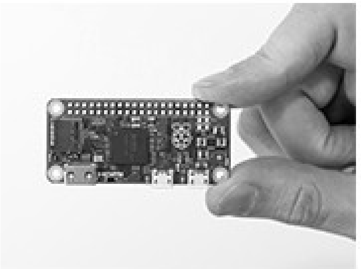


RIOT

Processor: MHz, 8/16/32 Bit
Memory: kByte
Energy: mWatt
Network access: 802.15.4, BLE
Price: 0,10-10€

The many faces of IoT
we focus on the challenging class of devices

High-end IoT

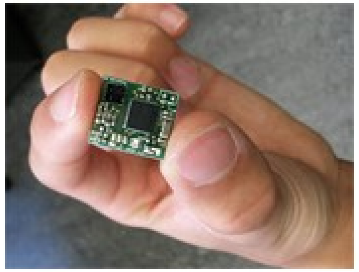


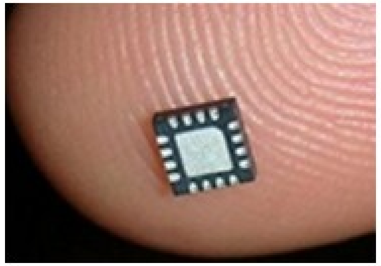
Linux

ANDROID

Processor: GHz, 32/64 Bit
Memory: MB/GByte
Energy: Watt
Network access: 5G, WLAN
Price: 10-100€

Low-end (or constrained) IoT





RIOT

high device heterogeneity

Processor: MHz, 8/16/32 Bit
Memory: kByte
Energy: mWatt
Network access: 802.15.4, BLE
Price: 0,10-10€

Digital Payments for the IoT
requirements on a payment system

resource demands as low as possible

autonomy: human-less operation for machine-to-machine payments

privacy: non-discriminating, privacy-preserving

micropayments: high amount-to-fee ratio even for small amounts

settlement as fast as possible to support high number of payments

Digital Payments for the IoT
using traditional payment systems?

✓ **resource demands:** negligible

✗ **autonomy:** identity-bound accounts

require human confirmation

✗ **privacy:** centralized, account-based systems

✗ **micropayments:** high fees

✓ **settlement:** instant

Digital Payments for the IoT
using cryptocurrencies?

- ✗ **resource demands:** expensive verification of distributed ledger
- ✓ **autonomy**
- ✓ **privacy:** at least pseudonymity
- ✗ **micropayments:** high mining fees
- ✗ **settlement:** delayed due to distributed consensus

Digital Payments for the IoT
using e-cash and GNU Taler!

- ? **resource demands:** more on that later
- ✓ **autonomy:** self-custody of tokens
- ✓ **privacy:** guaranteed thanks to blind signatures
- ✓ **micropayments:** low technical and operational costs
- ✓ **settlement:** instant

Outline

Motivation: payments for a distributed IoT economy

The many faces of IoT

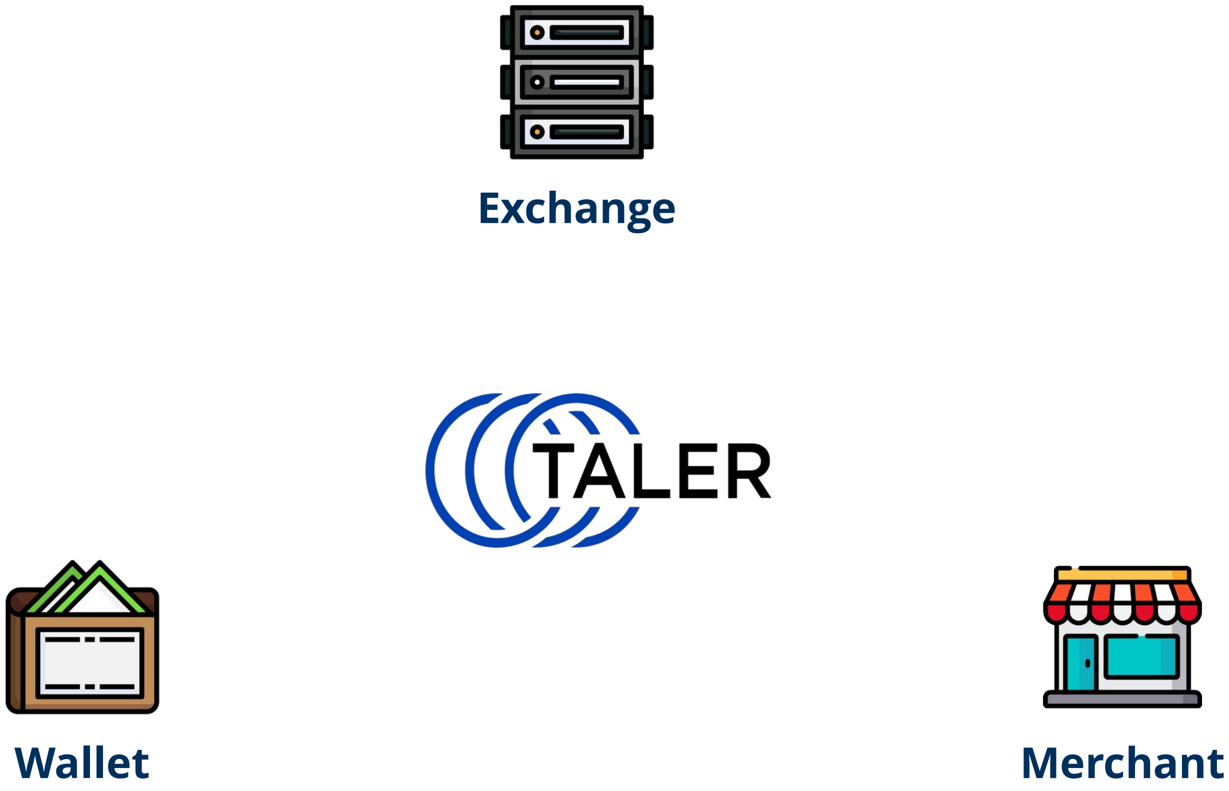
Suitable payment systems for the IoT

A typical e-cash scheme: GNU Taler

IoT e-cash wallet challenges and proposed solutions

GNU Taler

design and (non-)goals



representation of existing currency

***payer* anonymity**

- untraceable coins
- unlinkable payments

***income* transparency**

instant settlement

reliable contracts

micropayment support

online-only*

*at least one party needs to have internet connection

GNU Taler
centralized architecture

Exchange

central authority
liability
- signs coin
- holds actual value
- redeems merchant

TALER

Wallet

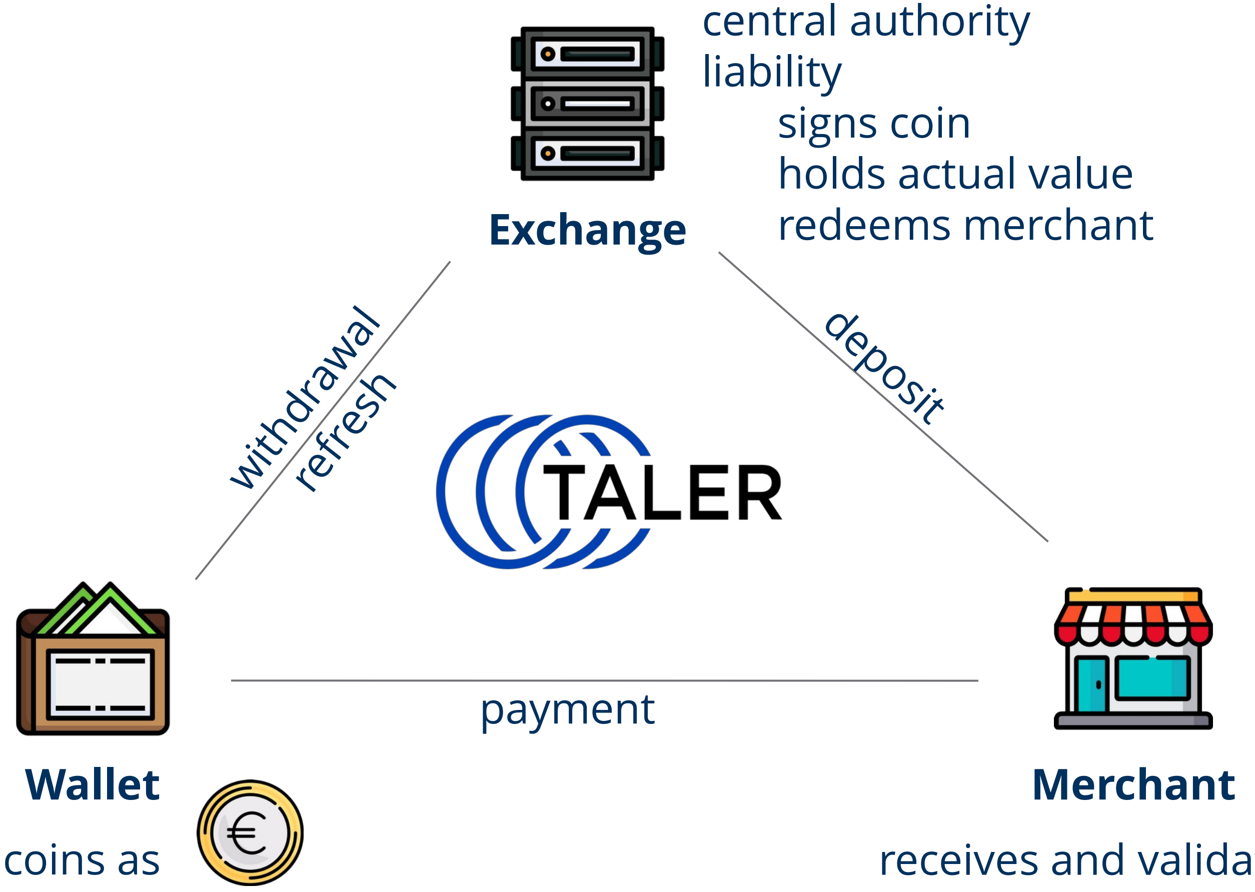
owns coins as
digital representation of
value in an existing currency

Merchant

receives and validates
coin deposit permission
at exchange

GNU Taler

centralized architecture



Exchange

central authority
liability
signs coin
holds actual value
redeems merchant

withdrawal
refresh

deposit

payment

Wallet

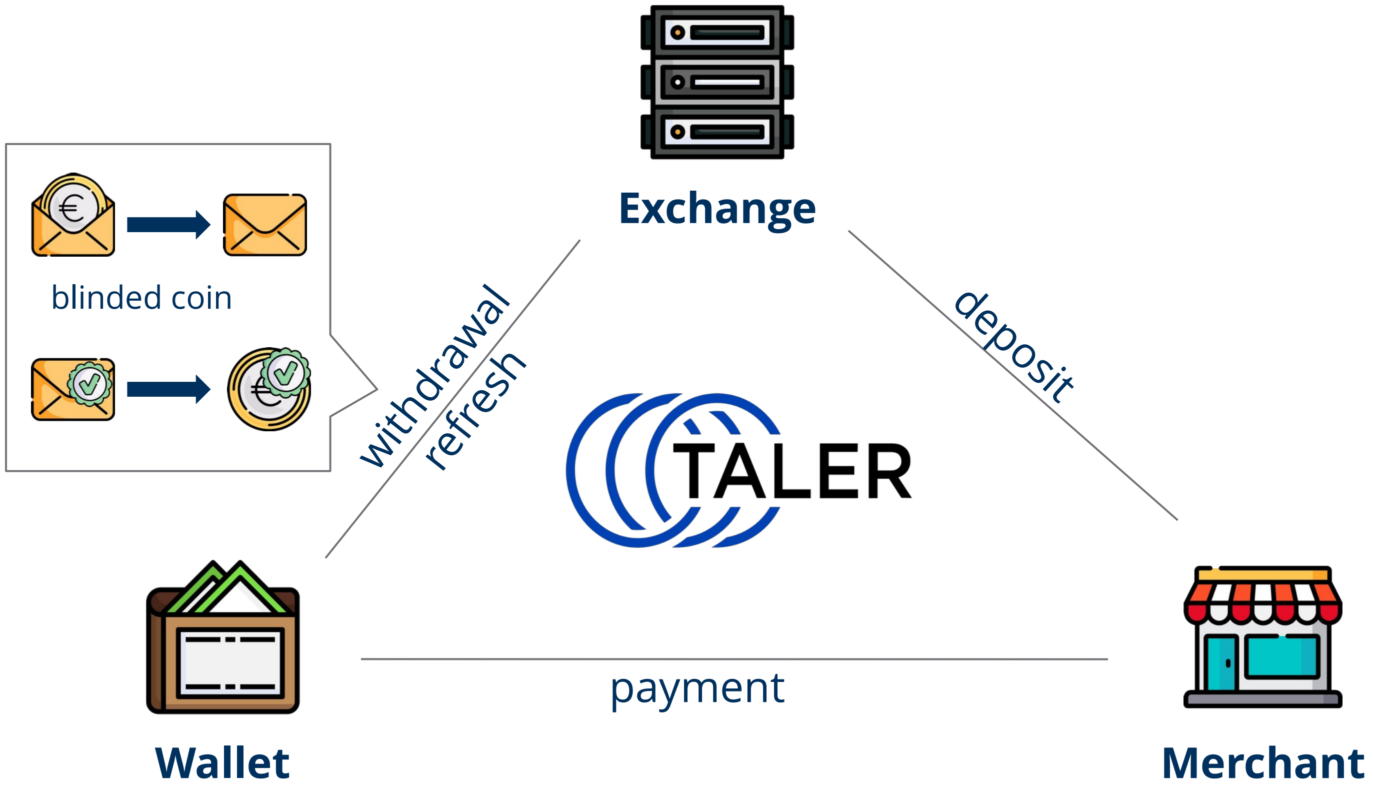
owns coins as
digital representation of
value in an existing currency

Merchant

receives and validates
coin deposit permission
at exchange

GNU Taler

distributed cryptographic protocol



€ = **Ed25519** keypair

ownership = private key

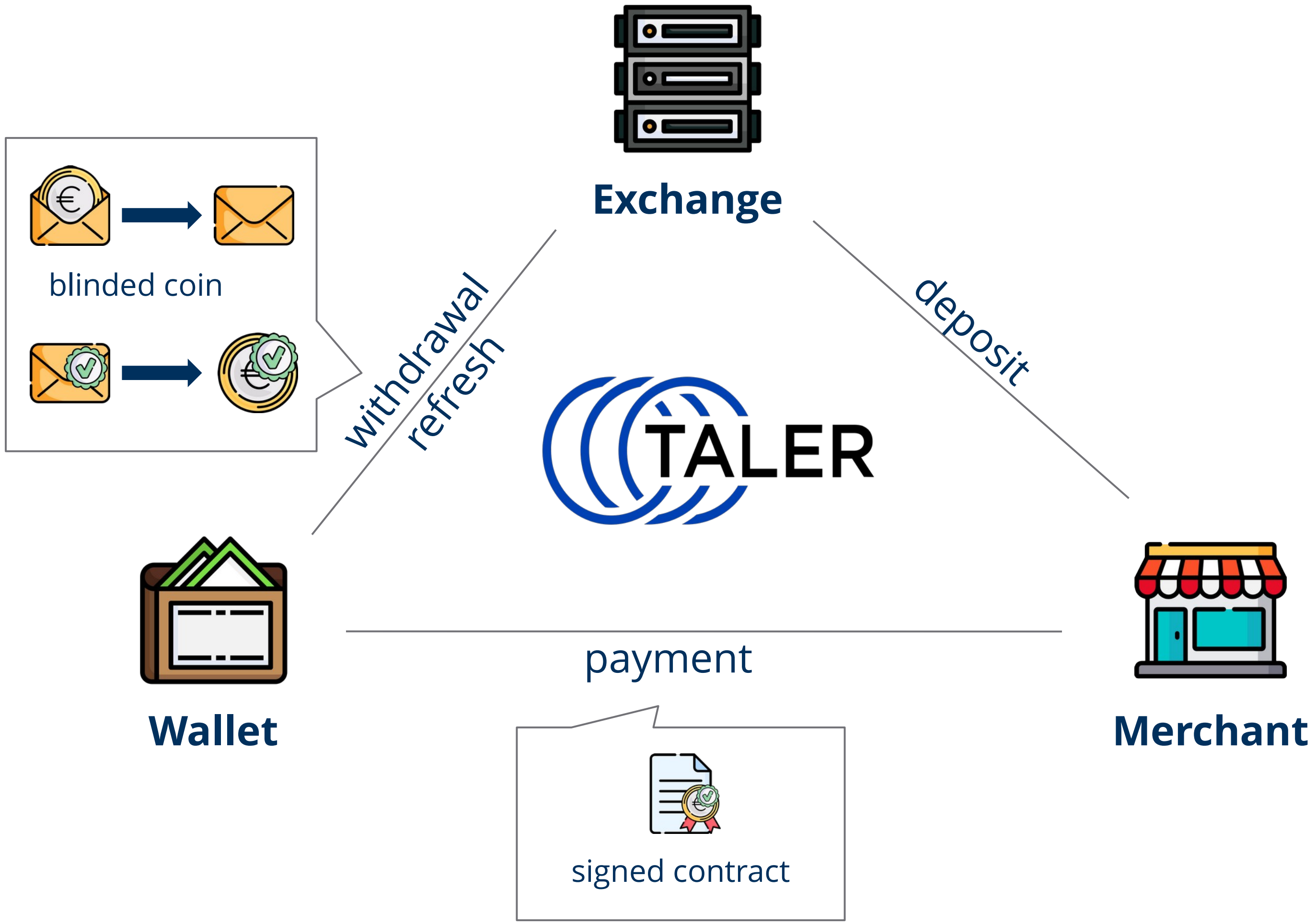
✉ = **RSA-FDH blinding*** scheme

✓ = RSA signature

*Clause Blind Schnorr Signature optionally supported, too

GNU Taler

distributed cryptographic protocol



€ = **Ed25519** keypair

ownership = private key

€✓ = coin signature

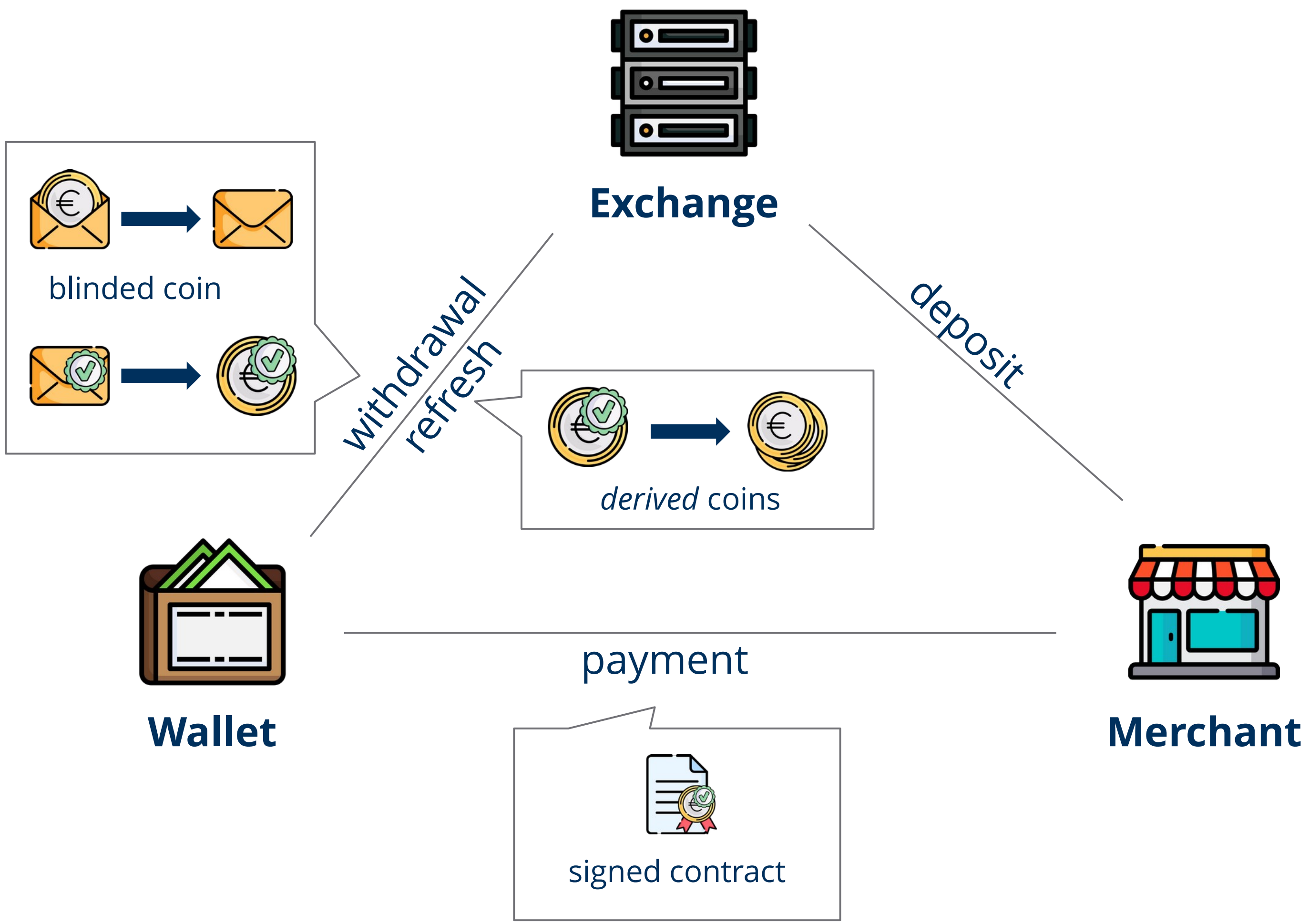
✉ = **RSA-FDH blinding*** scheme

✓ = RSA signature

*Clause Blind Schnorr Signature optionally supported, too

GNU Taler

distributed cryptographic protocol



€ = **Ed25519** keypair

ownership = private key

✓ = coin signature

✉ = **RSA-FDH blinding*** scheme

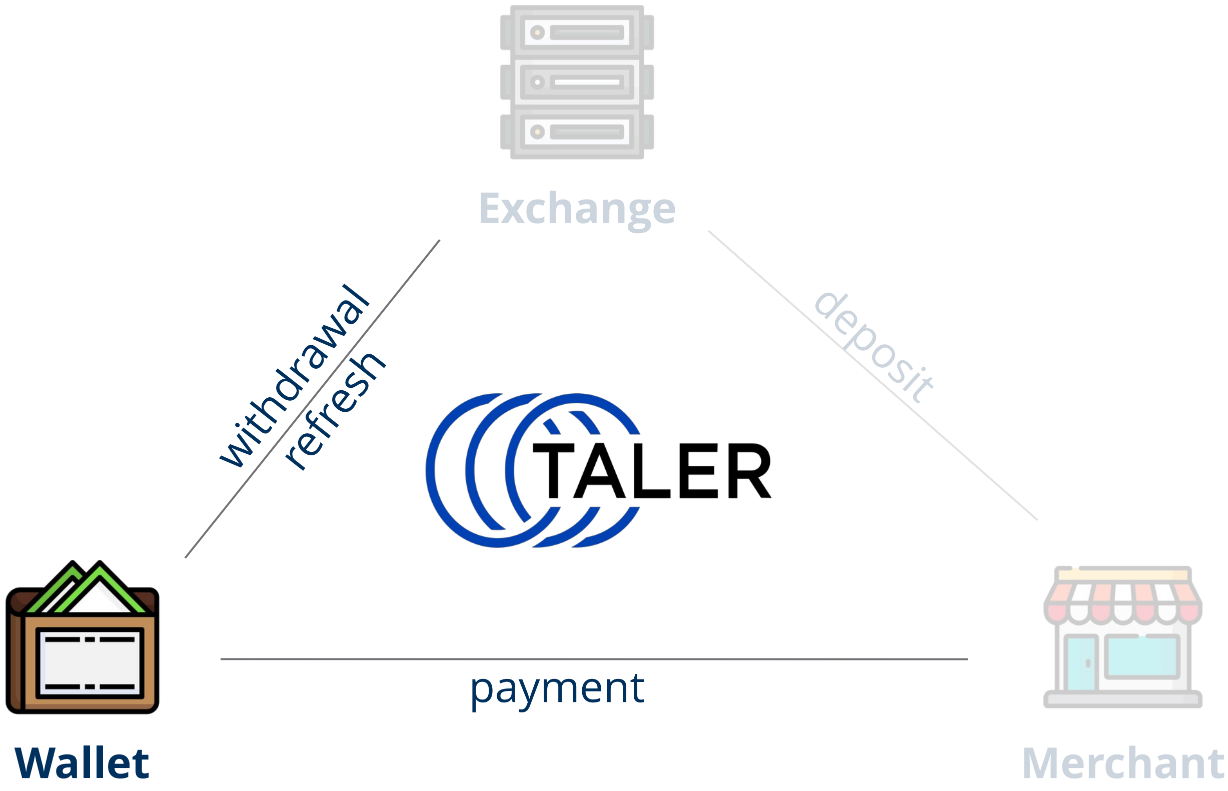
✓ = RSA signature

€ = **HKDF** for new private keys

*Clause Blind Schnorr Signature optionally supported, too

GNU Taler

typical e-cash wallet requirements



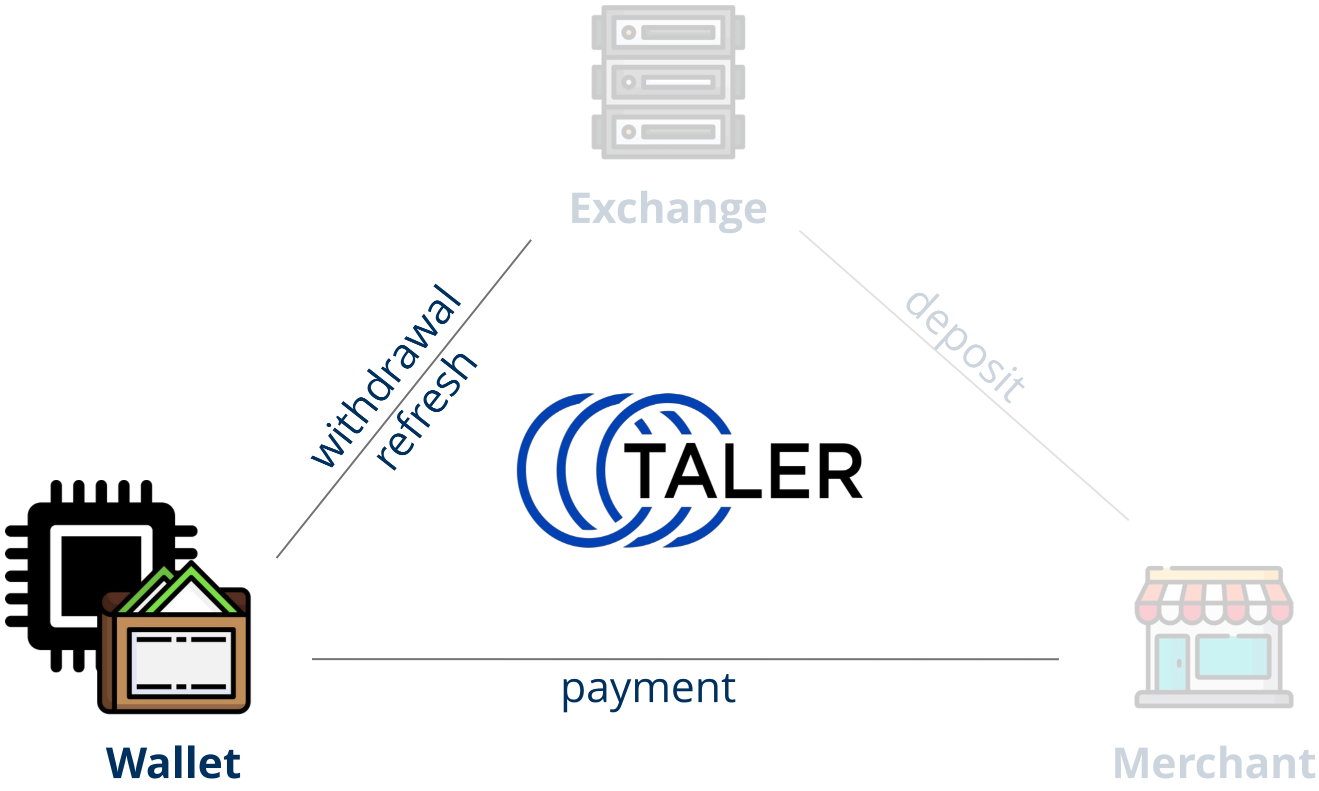
storage of coins

cryptographic operations

network access for communication with exchange and merchant

GNU Taler meets low-end IoT

with challenging device constraints



storage of coins

cryptographic operations

network access for communication with exchange and merchant

resource constraints: limited processing power, storage, energy, networking bandwidth

Outline

Motivation: payments for a distributed IoT economy

The many faces of IoT

Suitable payment systems for the IoT

A typical e-cash scheme: GNU Taler

IoT e-cash wallet challenges and proposed solutions

IoT e-cash wallet

challenges

storage for coins **is limited**

cryptographic operations are often **computationally-intensive**

network access via **low-power** network protocols with **limited payload sizes and bandwidth**

IoT e-cash wallet

challenges and proposed solutions

storage for coins **is limited**

minimize amount of coins with intelligent **coin selection strategy**

cryptographic operations are often **computationally-intensive**

use **hardware acceleration** if available

offer lightweight cryptography and support **cipher agility**

network access via **low-power** network protocols with **limited payload sizes and bandwidth**

minimize **communication overhead** and **data redundancy**: e.g., CBOR/CoAP instead of JSON/HTTP

IoT gateway for internet access

IoT e-cash wallet
challenges and proposed solutions

storage for coins **is limited**

minimize amount of coins with intelligent **coin selection strategy**

cryptographic operations are often **computationally-intensive**

use **hardware acceleration** if available

offer lightweight cryptography and support **cipher agility**

network access via **low-power** network protocols with **limited payload sizes and bandwidth**

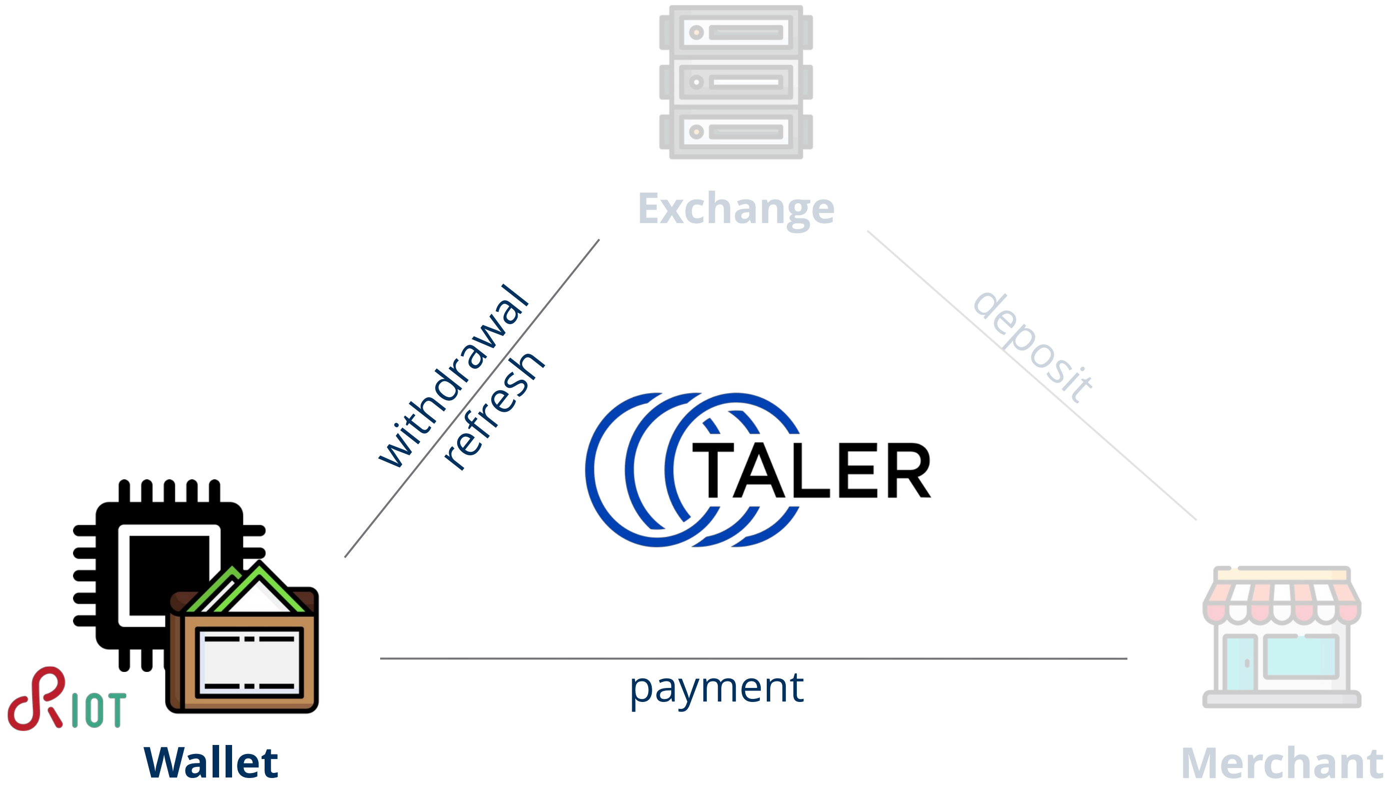
minimize **communication overhead** and **data redundancy**: e.g., CBOR/CoAP instead of JSON/HTTP

IoT gateway for internet access

hardware heterogeneity accommodated via general-purpose IoT OS: RIOT

GNU Taler meets low-end IoT

a change in system design

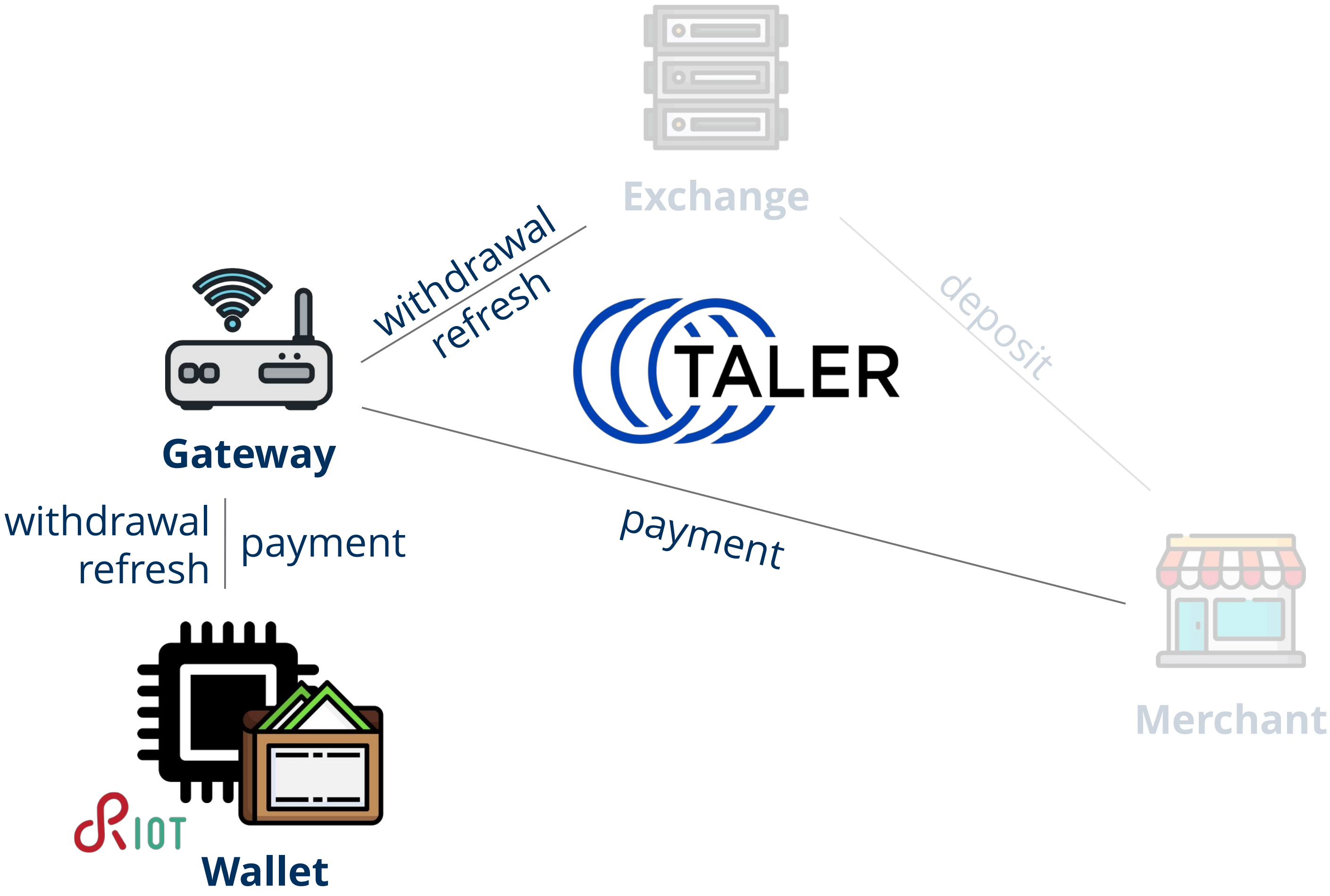


network access via

IoT gateway

GNU Taler meets low-end IoT

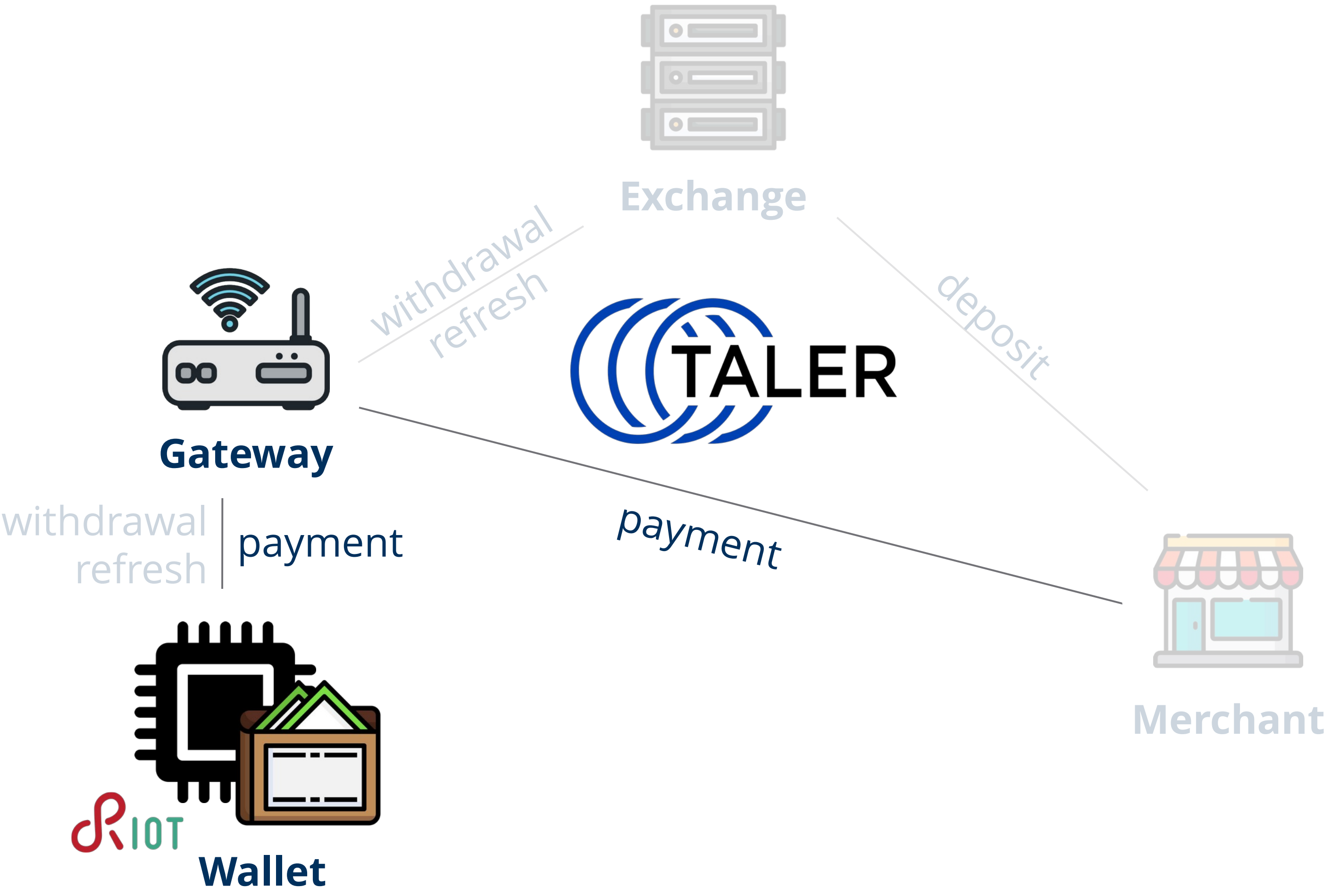
a change in system design



network access via **IoT gateway**

GNU Taler meets low-end IoT

first prototype



RIOT-based **wallet** on **nRF52840 SoC**

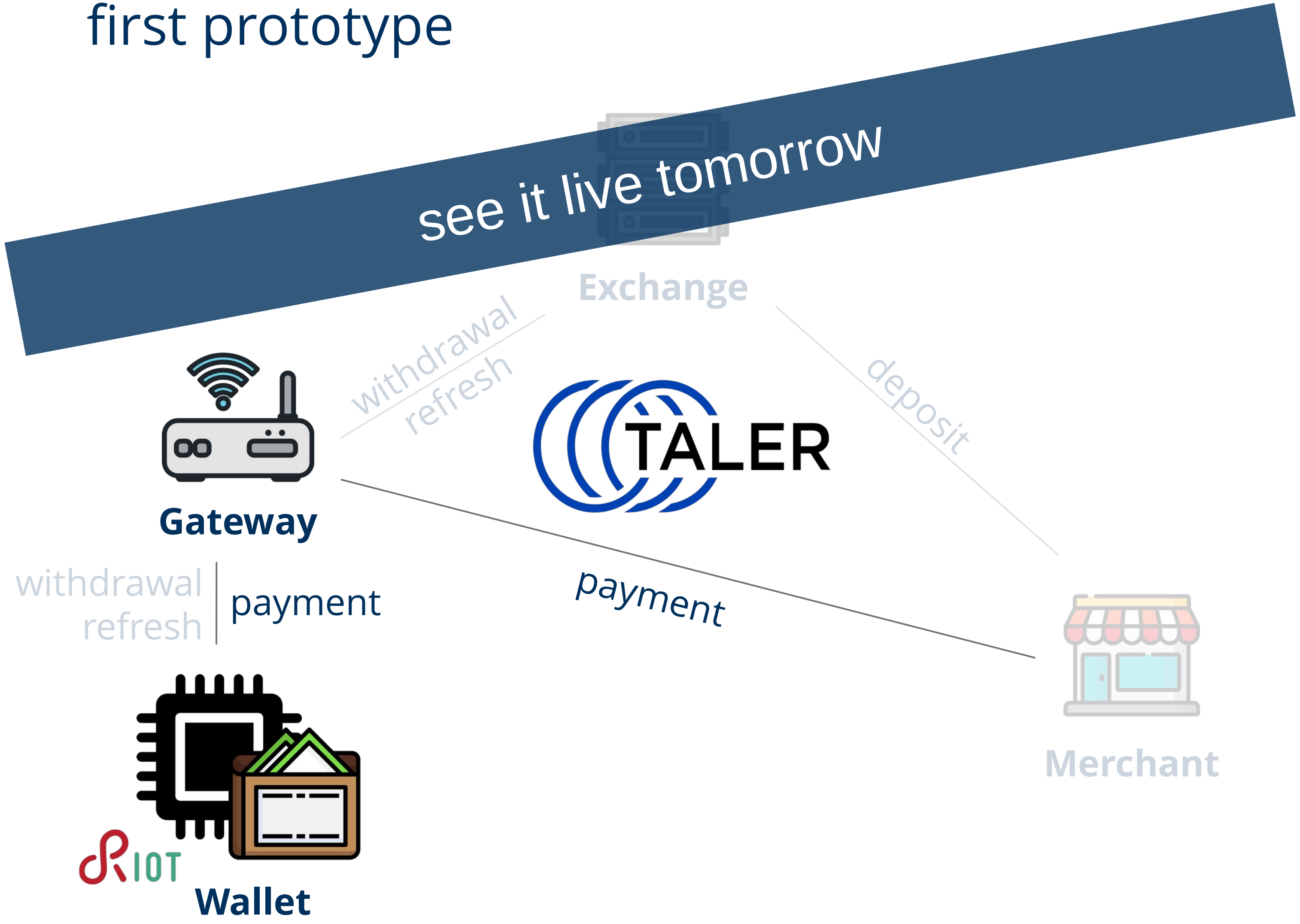
- storage: 256 kB RAM, 1024 kB flash
- connectivity: **802.15.4**, BLE
- HW-accelerated Ed25519, RSA, SHA2
- price tag: **~4$**
- UI (display/NFC) for demo purposes

Raspberry Pi / laptop as IoT gateway and CoAP-HTTP / CBOR-JSON proxy

payment support only *for now*

GNU Taler meets low-end IoT

first prototype



RIOT-based **wallet** on **nRF52840 SoC**

- storage: 256 kB RAM, 1024 kB flash
- connectivity: **802.15.4**, BLE
- HW-accelerated Ed25519, RSA, SHA2
- price tag: **~4$**
- UI (display/NFC) for demo purposes

Raspberry Pi / laptop as IoT gateway and CoAP-HTTP / CBOR-JSON proxy

payment support only *for now*

Conclusions and Outlook

necessity for **digital payments** in a distributed **IoT economy**

requirements on autonomy, privacy, micropayments, settlement

- **e-cash** as a fitting solution

additional constraints for IoT e-cash wallet

- storage, cryptographic operations, network access

promising results with first prototype

- next: withdrawal with blind signature scheme

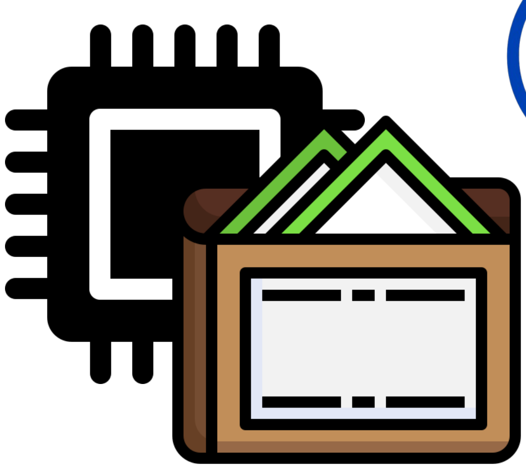


Image Credits

Icons created by Futuer and Freepik on Flaticon

https://unsplash.com/photos/silver-and-gold-round-coins-yJpjLD3c9bU

https://taler.net/images/logo-2021.svg

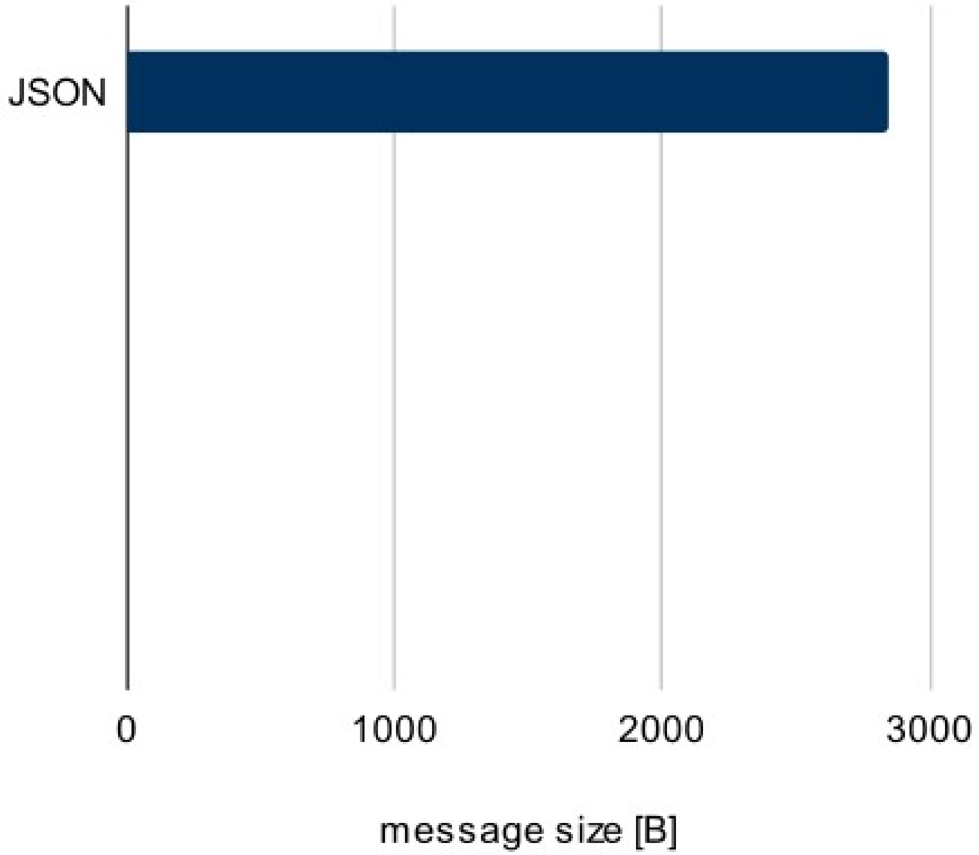
https://www.riot-os.org/branding.html

Backup Slides

Network access
Encoding matters

Example: Withdrawal of four coins

```
{"planchets": [
 {"denom_pub_hash":"50581Q8P6Y2…",
  "reserve_sig":"DNMCWA19F8191Z…",
  "coin_ev": {
   "cipher":"RSA",
   "rsa_blinded_planchet":"B9GNS…"
  }
 },
 {"denom_pub_hash":…}, {…}, {…}
]}
```

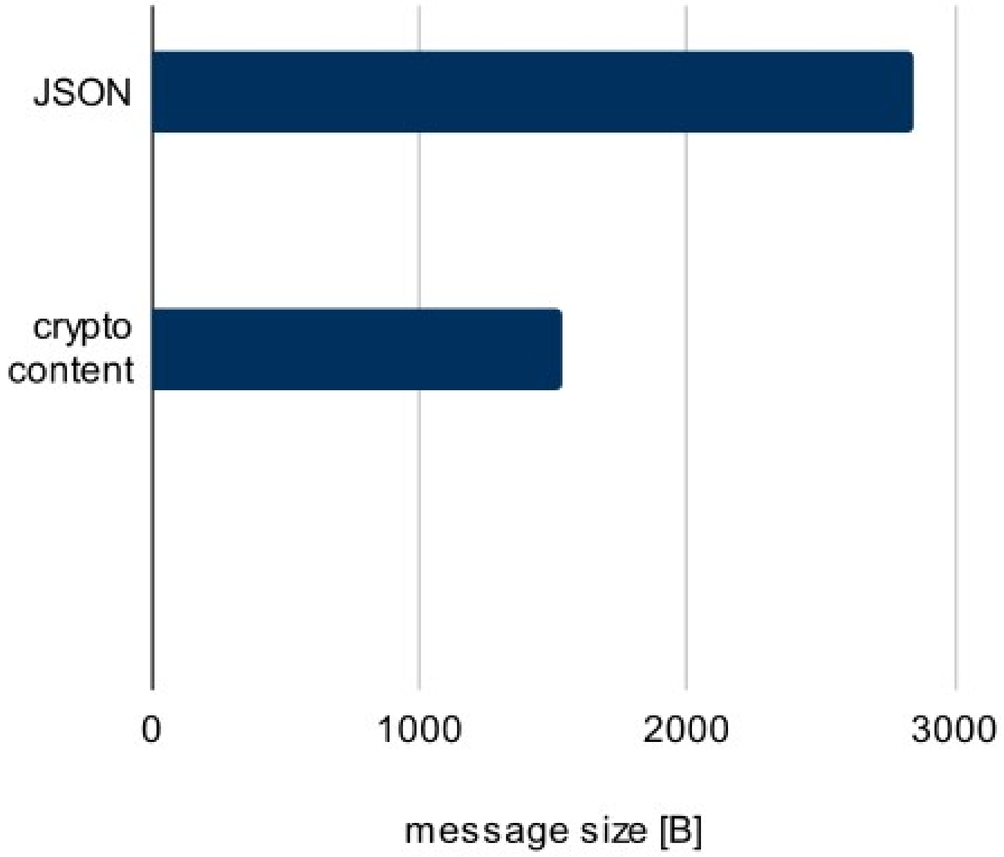


Network access

Encoding matters

Example: Withdrawal of four coins

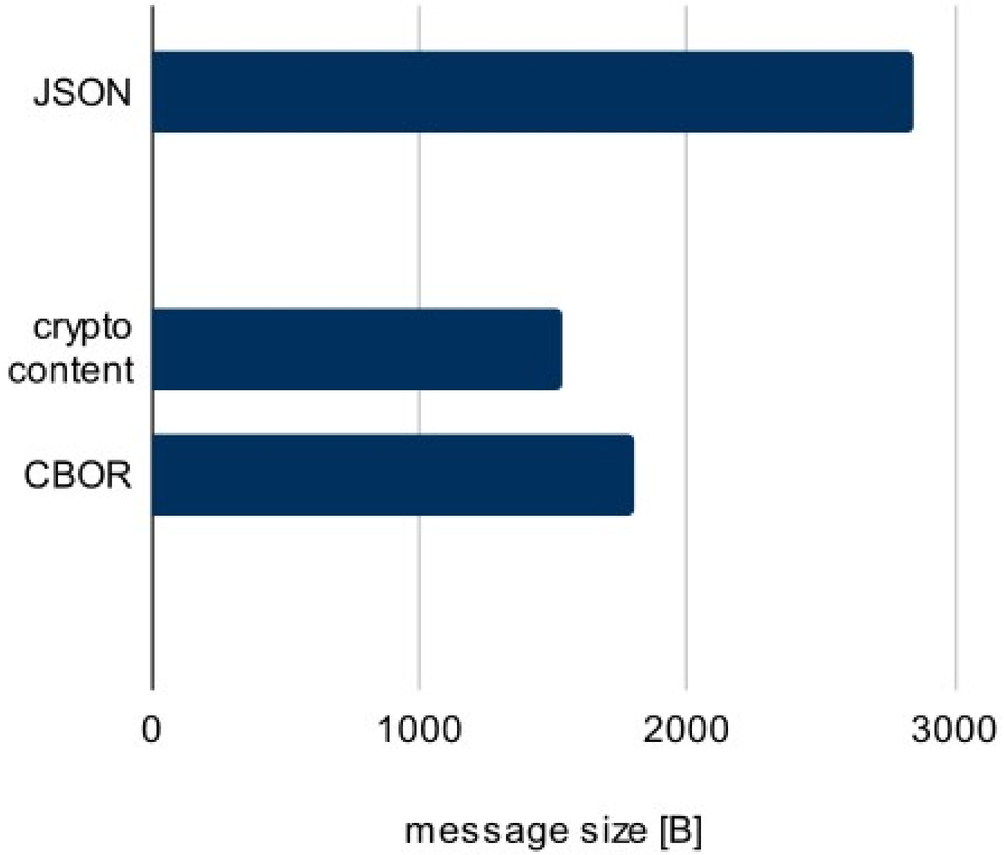
```
{"planchets": [
 {"denom_pub_hash":"50581Q8P6Y2…",
  "reserve_sig":"DNMCWA19F8191Z…",
  "coin_ev": {
   "cipher":"RSA",
   "rsa_blinded_planchet":"B9GNS…"
  }
 },
 {"denom_pub_hash":…}, {…}, {…}
]}
```



Network access
Encoding matters

Example: Withdrawal of four coins

```
{"planchets": [
 {"denom_pub_hash":"50581Q8P6Y2…",
  "reserve_sig":"DNMCWA19F8191Z…",
  "coin_ev": {
   "cipher":"RSA",
   "rsa_blinded_planchet":"B9GNS…"
  }
 },
 {"denom_pub_hash":…}, {…}, {…}
]}
```

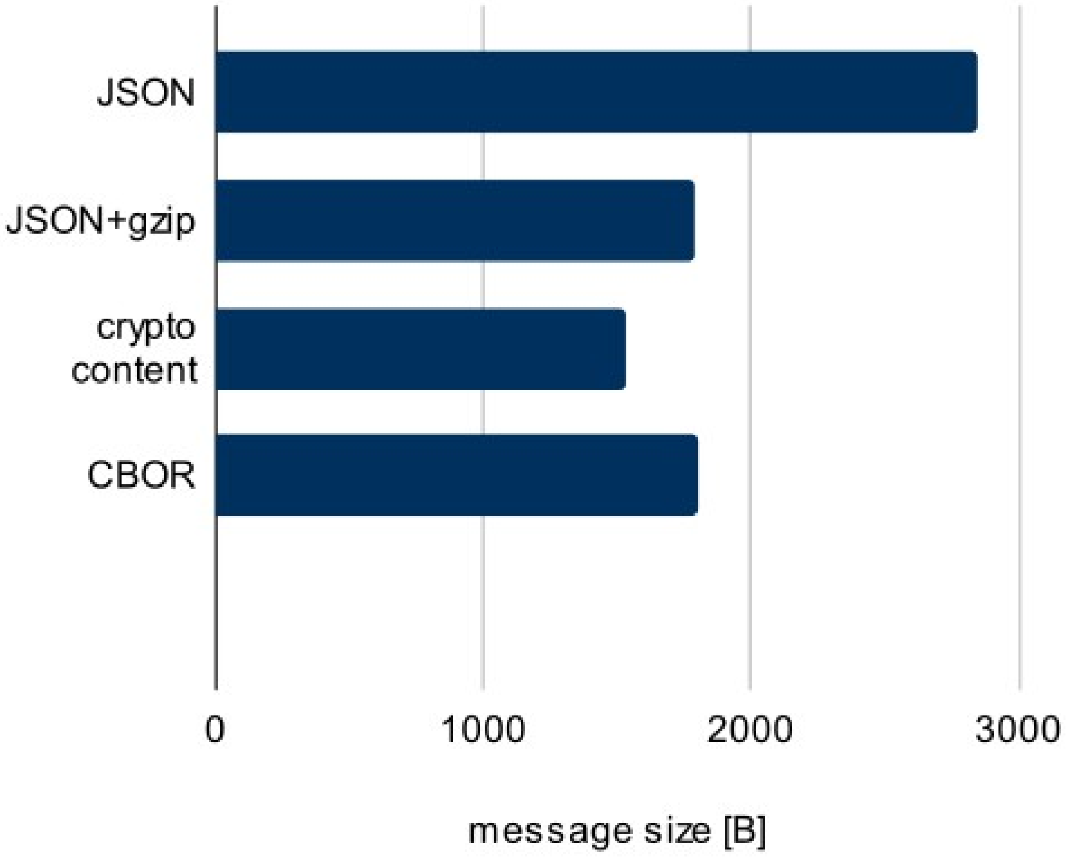


Network access

Encoding matters

Example: Withdrawal of four coins

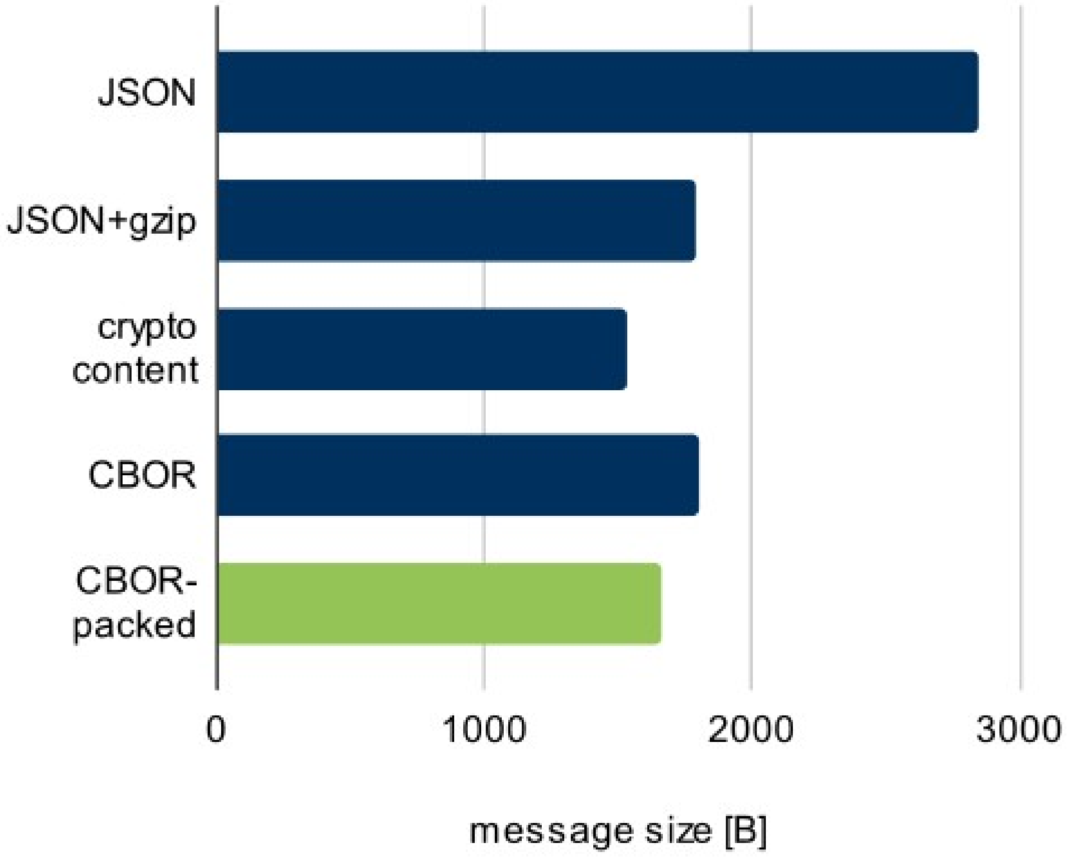
```
{"planchets": [
 {"denom_pub_hash":"50581Q8P6Y2…",
  "reserve_sig":"DNMCWA19F8191Z…",
  "coin_ev": {
   "cipher":"RSA",
   "rsa_blinded_planchet":"B9GNS…"
  }
 },
 {"denom_pub_hash":…}, {…}, {…}
]}
```



Network access
Encoding matters

Example: Withdrawal of four coins

```
{"planchets": [
 {"denom_pub_hash":"50581Q8P6Y2…",
  "reserve_sig":"DNMCWA19F8191Z…",
  "coin_ev": {
   "cipher":"RSA",
   "rsa_blinded_planchet":"B9GNS…"
  }
 },
 {"denom_pub_hash":…}, {…}, {…}
]}
```


JSON
JSON+gzip
crypto content
CBOR
CBOR-packed
message size [B]