The Blockchain challenge for the electricity system

Fabrizio Armani
Alessio Pinzone

AIEE – 2nd Energy Symposium, November 4th 2017

Blockchains first application: cryptocurrencies

- Blockchains are open digital ledger representing the **backbone technology on which Cryptocurrencies are based**. Their main properties:

  - **Everyone is allowed to join by running a node of the network** (compiling the free open code / installing the software) which is connected to the internet.

  - **Transactions of digital value** are broadcasted through the network and collected into blocks forming the ledger which is completely inspectable by anyone.

  - **Decentralized P2P network** - the same copy of the ledger is distributed among all the nodes of the network. **No need of a trusted third part responsible for modifying and updating the ledger on behalf of the users**

  - **There is a consensus rule** according to which block are validated and stacked together guaranteeing that transactions included are not double spent. The validation activity (mining) is economically incentivized by the emission of new digital value.

- First applied example with Bitcoin protocol described in 2008 Satoshi Nakamoto white paper during the financial crisis.

Transactions as a digital signatures of some value

- The process of **constructing a transaction relies on asymmetric cryptography.** (example are with Bitcoin protocol - which exploit 256-bit Elliptic Curve Cryptography)

Public Key
the “IBAN equivalent”

1FUrh4B6bmiUCFP3ARqen1d6ConbZHLNFV

Private Key
the password

L22yhSzrwaRM5fv6KZJjquiYJrZGSPb94J7Nr5W2B4A2sbN7nTVA

Note: Both are Bitcoin encoded keys

- **The Public Key is generated from the private key according to the chosen cryptographic algorithm. Is not issued by any authority**. If you know the Private Key you can generate the Public Key but the inverse operation is computationally unfeasible.

- Basically, **a crypto transaction is a digital signature of some value** previously spent (i.e. signed with another private key) towards another Public Key.

Hashing functions and proof-of-work

- Hashing function are of fundamental importance in blockchains.
  They provide an (almost) **unique identifier -** the hash - of a greater size set of data

- Good Cryptographic Hashing functions are constructed in order to be non invertible and collision resistant (intended as computational infeasible). Here an example with SHA-256 (used in Bitcoin protocol):

I can easily verify these equalities but I cannot (easily) find the example phrase from the hash

SHA-256(“EnergySymposiumRome1”**)** =
“380ccfb8474f90609872f6aa4a1214b81e369c65c01b072b5c9c66968d576982”

SHA-256(“EnergySymposiumRome2”**)** =
“70962bde87a48fbe1e5eed1115e6641f6285a62725efcac045bfde407168ecdf”

.

.

.

I need more than 60k attempts to find an hash with 4 zeroes.
I gave a Prove-of- Work!

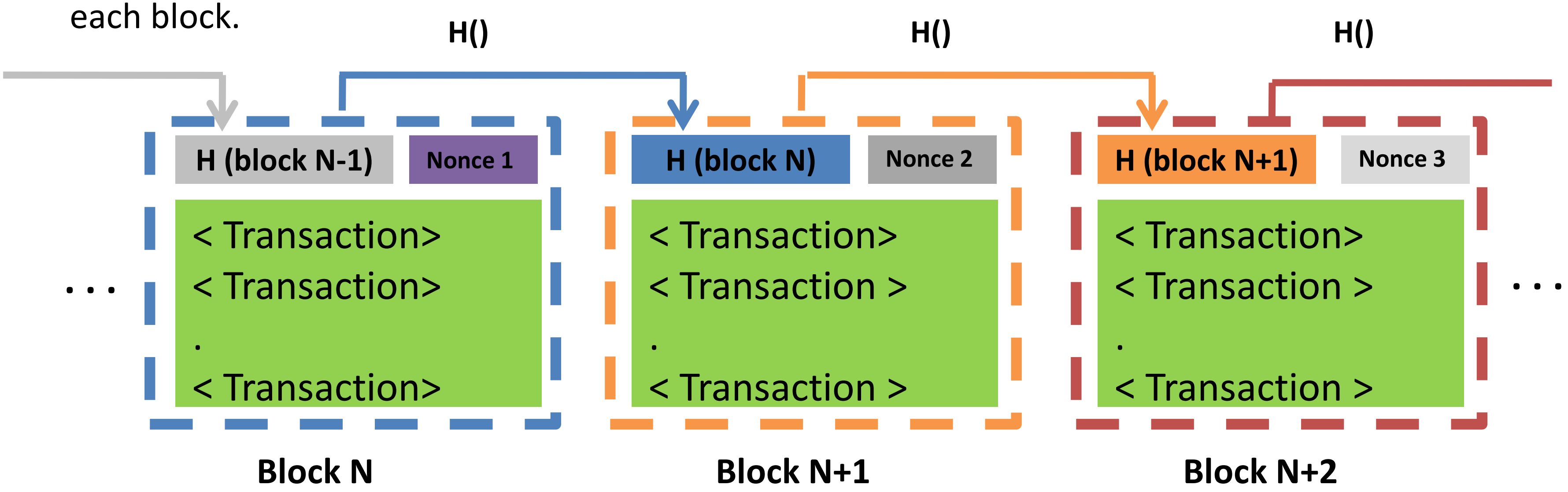
Nonce = number of attempts

SHA-256(“EnergySymposiumRome69884”) =
“0000ba59fa638cd47cf26e945da26ab9a31ab0c4db6fd58ff9becdcd022e7d01”

Number of leading zeroes = difficulty Established by the network

The proof-of-work blockchain mechanism

- Block stacking is realized thanks to the use of **Hashing function H()** as it is possible to get a **footprint of the information stored in the block** and a footprint of the block itself. The difficulty of the proof of work is increased in order to maintain a fixed average time between the creation of each block.



- Mining consist in try to find an **Hash with a certain leading value of zeroes using transaction, nonce and the hash of a previous block**. Finding such an hash is a matter of probability which is proportional to the computational power of miners**. The consensus is achieved by following the chain with greatest computational work (the longest chain).**

- **Transaction included in a block are secured from double spending** as more blocks are appended to the chain. **Miners finding blocks are paid by issuing fresh new coins** (decreasing over time) and by transaction fees

Different Blockchains

- **Hash based proof – of –work** is not the only method to achieve distributed consensus even if is the most common in public blockchain. **Proof-of-stake algorithms** represent an alternative way to achieve consensus relying upon value possession rather than computational power.

- The blockchain ecosystem itself relies on **rapidly changing definition, features and best practices**. **Consensus issue is one among the most debated together with scalability** within the IT community.

- A further element of differentiation among blockchains :

Public Blockchain

- **Permissionless access** - both transaction and mining (consensus)
- Underlying code is open and can be exploited for other initiative.
- Blockchain is published in its entirety
- Registered transaction are irreversible
- Consensus is incentivized

Private Blockchain/Distributed Ledger Technology (DLT)

- **Permissioned access**
- Underlying code is closed
- Participation is generally subjected to invitation also for blockchain querying
- Transaction can be modified ex-post as consensus can be centralized
- Consensus may be not incentivized

- **Private blockchains can be more considered as data structures** rather than distributed consensus blockchains.
  However, it is worthwhile to point out **that public blockchains pays in term of computational efficient**

Cryptocurrencies vs. electricity system

Cryptocurrency Blockchain

- Digital Value
- Total supply is algorithmically limited
- Bilateral transaction and **smart contracts**
- No time constraint (sender chose when to transact)
- P2P – flat topology. Each node has the same importance and distance from each other
- Nodes and address are free to open (free software/private key)

Electricity system

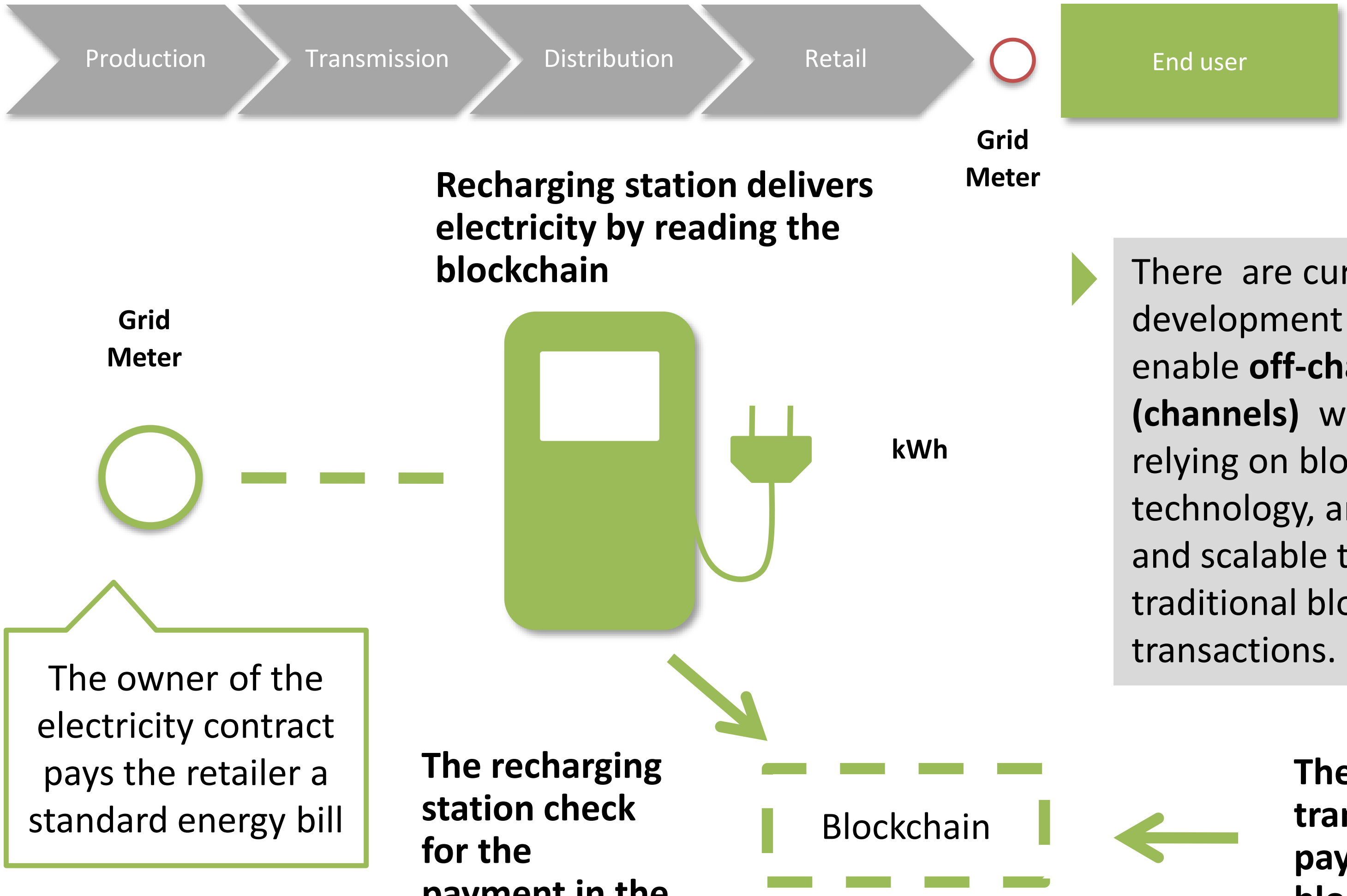
- Electricity – physical good
- Electricity depends on generators and interconnections
- Market and Bilateral transaction
- Forwardness feature of the electricity market. Production must equal consumption in real time and kWh are not all equal.
- Grid topology and hierarchy of delivery and consumption nodes
- Nodes are usually identified by meter device and their installation need to be authorized

On-going Blockchain application for the electricity system

Among the considerable number of project we have identified 3 main model for **which blockchain is being tested** in the electricity ecosystem:

- Behind the meter applications
- Retailer model
- Wholesale electricity market trading

Behind the meter application – Recharging station



Recharging station delivers electricity by reading the blockchain

The owner of the electricity contract pays the retailer a standard energy bill

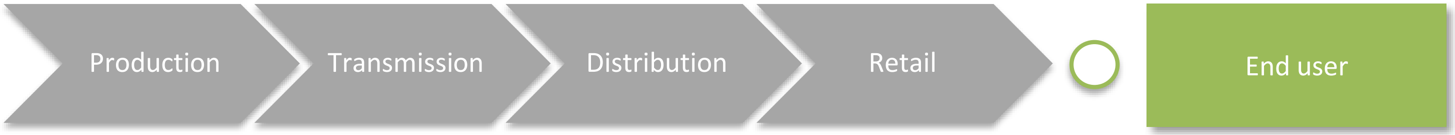
The recharging station check for the payment in the blockchain

The user make a transaction payment on the blockchain with a cryptocurrency or using a token

There are currently under development system that enable **off-chain payments (channels)** which, while relying on blockchain technology, are much faster and scalable than traditional blockchain transactions.

MODEL: VOLTACHAIN

Behind the meter application – Extended model

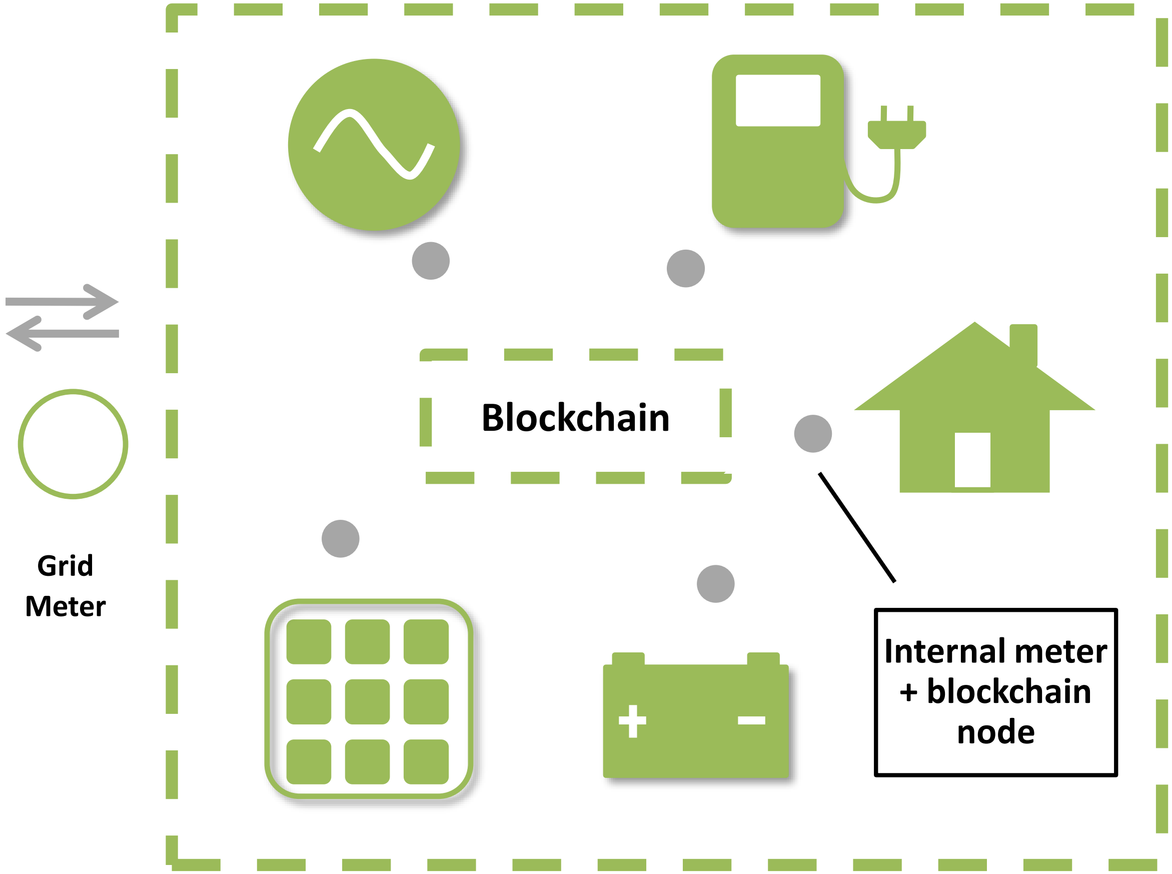

Production

Transmission

Distribution

Retail

End user


Blockchain

Internal meter + blockchain node

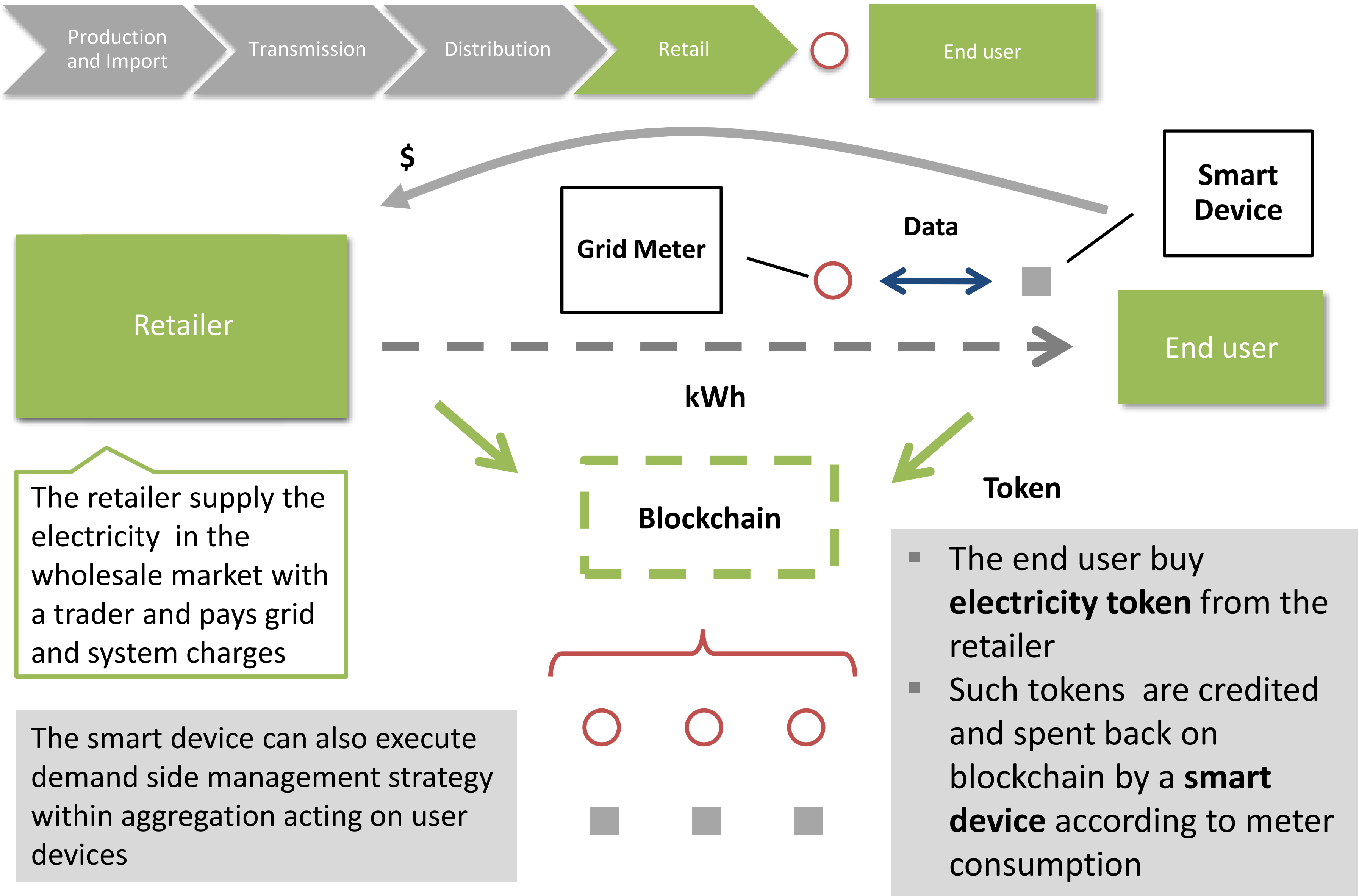
Grid Meter

- The same model applied to an **energy community** behind a grid meter
- **A common blockchain** either private or public must be chosen and single participants’ meters can write on the blockchain
- In case of tokens, an issuance provider is needed maybe connected to community governance
- Cryptocurrency or token can be used to pay other services

MODEL: BROOKLIN

Retail blockchain application

MODEL: GRID+



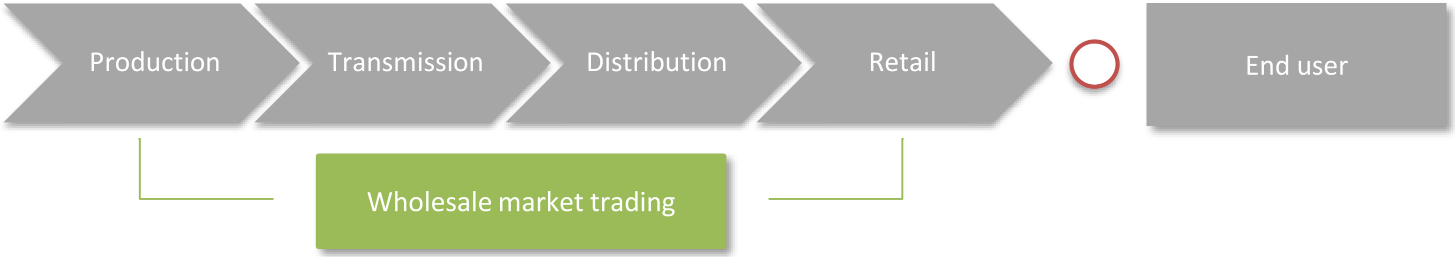
The retailer supply the electricity in the wholesale market with a trader and pays grid and system charges

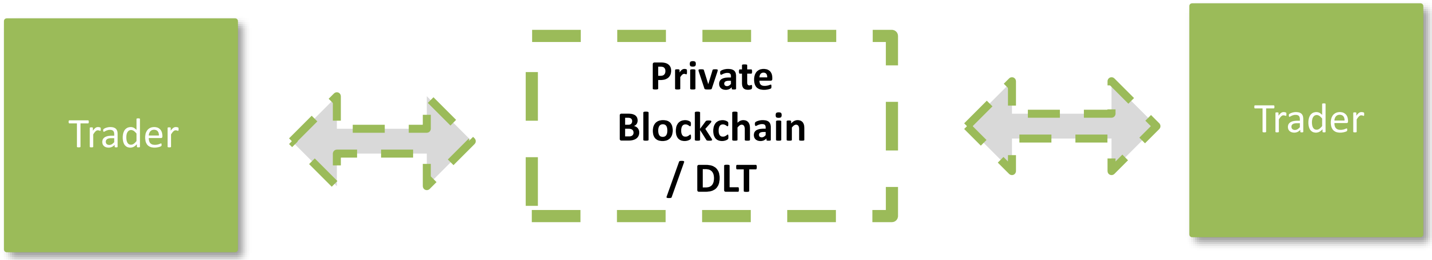
The smart device can also execute demand side management strategy within aggregation acting on user devices

- The end user buy **electricity token** from the retailer
- Such tokens are credited and spent back on blockchain by a **smart device** according to meter consumption

Energy market application

MODEL: ENERCHAIN





- Trades take place in a **P2P permissioned OTC platform**
- Settlement and post-trading activity is made simpler
- Main project structure are not generally disclosed and in particular:
  - Consensus rules
  - How trade net position registration is performed into the physical market/other OTC linked platform?
  - How financial position is settled? Use of a Clearing House?

Conclusions

- Blockchain in the electric energy sector **should be used as a mean of value transfer** rather than a new energy technology. **The challenge consists in creating suitable interfaces** between the two ecosystem exploiting existing IOT technology.

- **The (smart) meter** represents the connection point amid the electricity value chain and the blockchain. Trust and security issues thus rely on this device and its communication system without affecting existing energy regulation.

- **Energy communities** application are really promising as the adoption of a common blockchain can more easily implemented. Within the **retailer model** the blockchain system **empower prosumers as well** but we are more strongly dependent on service provider accounting.

- Only few project are based on cryptocurrency use to pay for electricity. Public Blockchain benefit already by community testing and improving and could represent an interesting choice.

- A broader application of the blockchain involving electricity system in its entirety including TSO/DSO **need to be based on regulation** defining its common technical characteristics exploitable for **grid services**. Some project are undergoing but such model is not likely to be applied in the short term.

AREA RIDEF

www.arearidef.it

For any doubts or request of clarification please feel free to contact us:

innovation@arearidef.it