



LBCoin & NEM

Cheng-Han (Hank) Tsai
hanktsai68@gmail.com

<http://www.free-powerpoint-templates-design.com>

Outlines

01 LBCoin

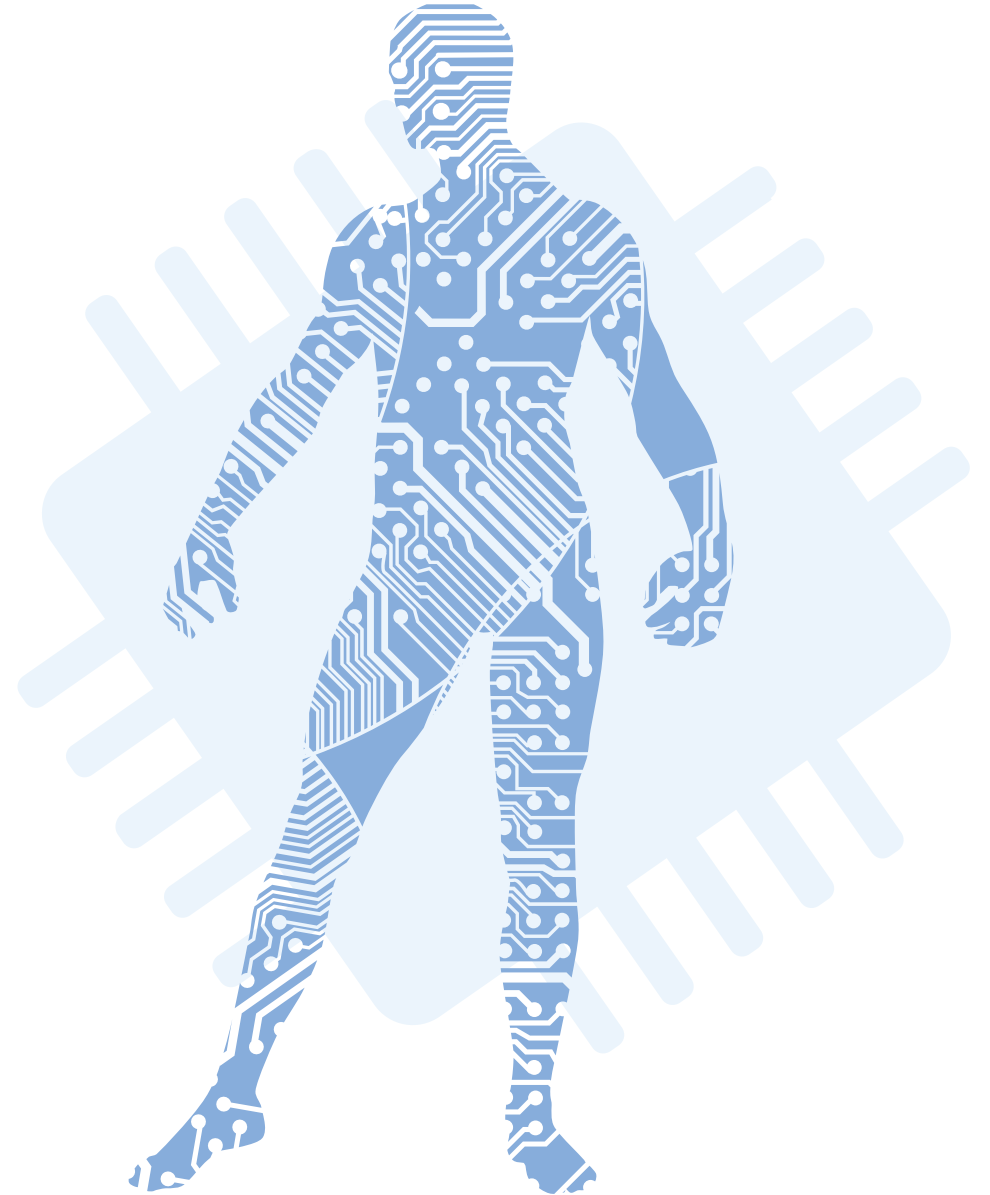
Digital token issued by Bank of Lithuania.

02 NEM Symbol

Blockchain implementation behind LBCoin

03 CBDC

Central Bank Digital Currency

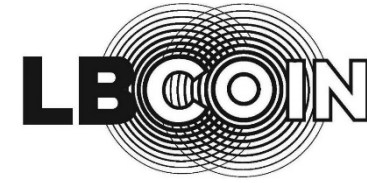


LBCoin

A digital collector coin issued by Bank of Lithuania, using blockchain technology.

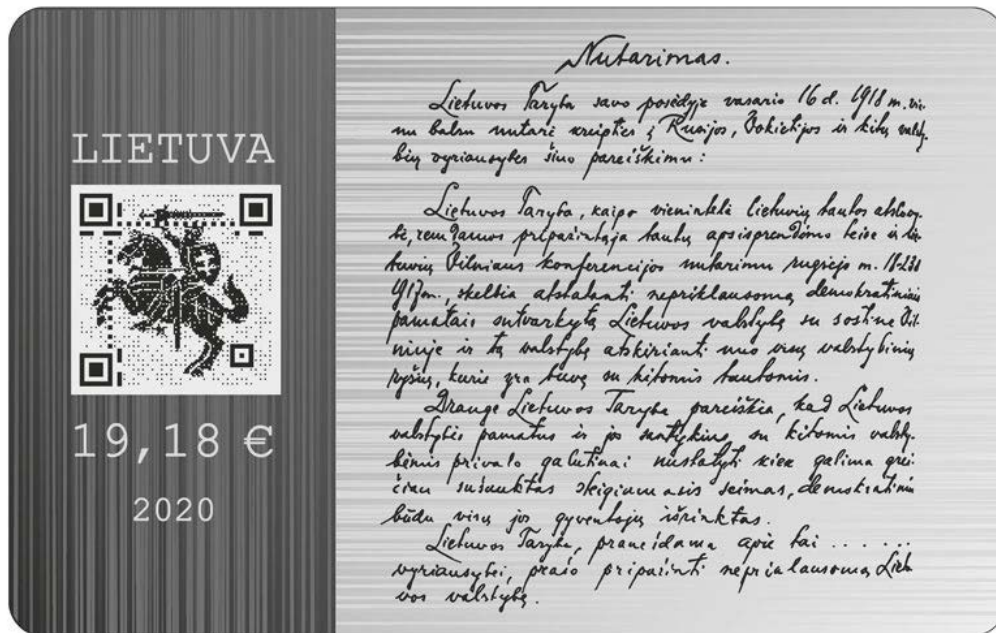


Facts about LBCoin



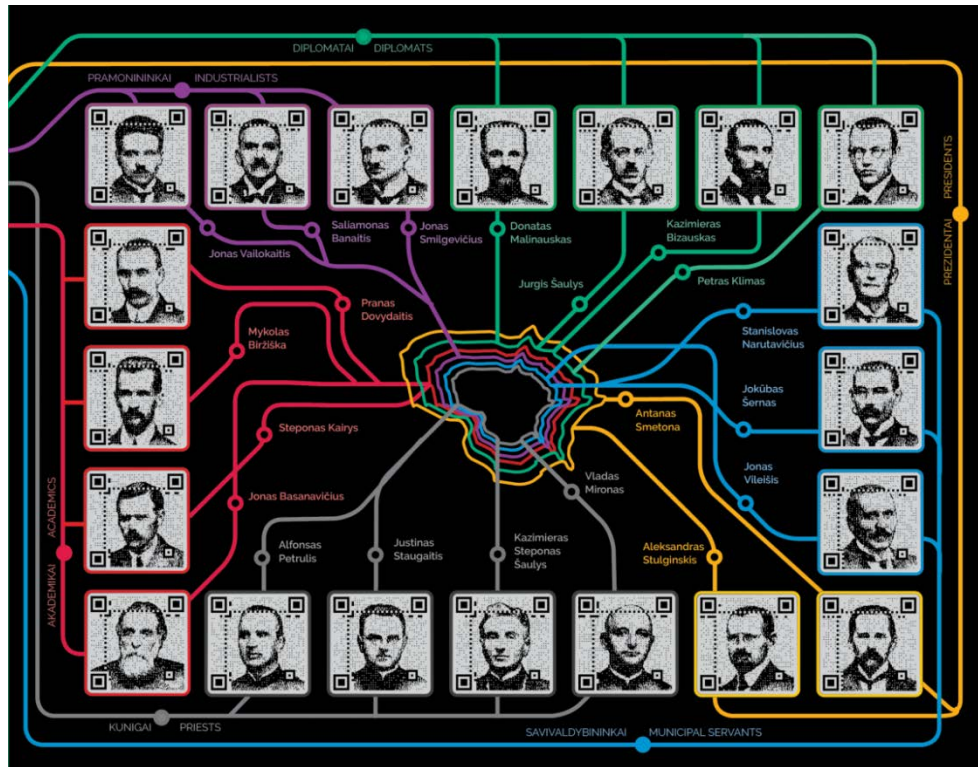
- A digital collector coin issued by Bank of Lithuania
 - Consists of digital tokens and physical collector coin
 - First issued at 23rd, Jul, 2020
 - Open to be traded for 30 months
 - Available all over the world
- Blockchain technology
 - Using NEM technology (NEM NIS1 and NEM Symbol)
 - The digital tokens can be transferred to public NEM blockchain
- An experiment for CBDC

Physical Collector Coin



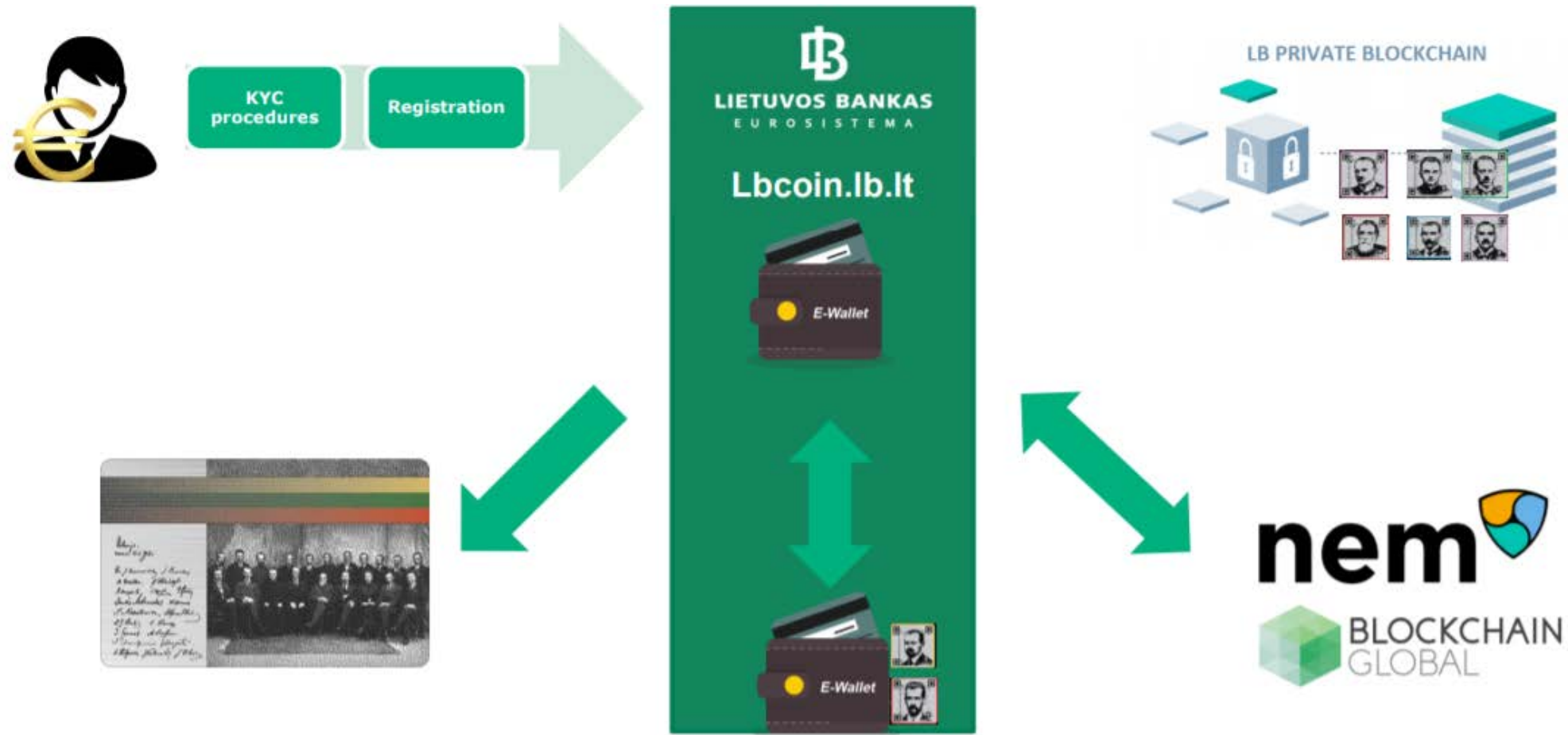
- Denomination €19.18
 - In memorial of the independence of Lithuania in 1918
- QR code link to LBCoin e-shop
- Act of Independence
- Silver-made, minted by Bank of Lithuania

Digital Tokens



- 24,000 tokens
 - 6 categories
 - 20 signatories of Act of Independence
- Issued on private blockchain
- Exchange through e-wallet
- Can be transferred to public NEM blockchain

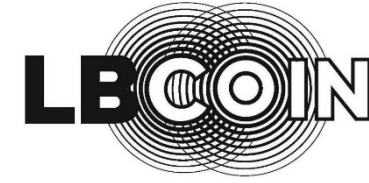
How does it work?



https://www.lb.lt/uploads/documents/files/LBCOIN%20pristatymas_EN.pdf

LBCoin & NEM

Features Required

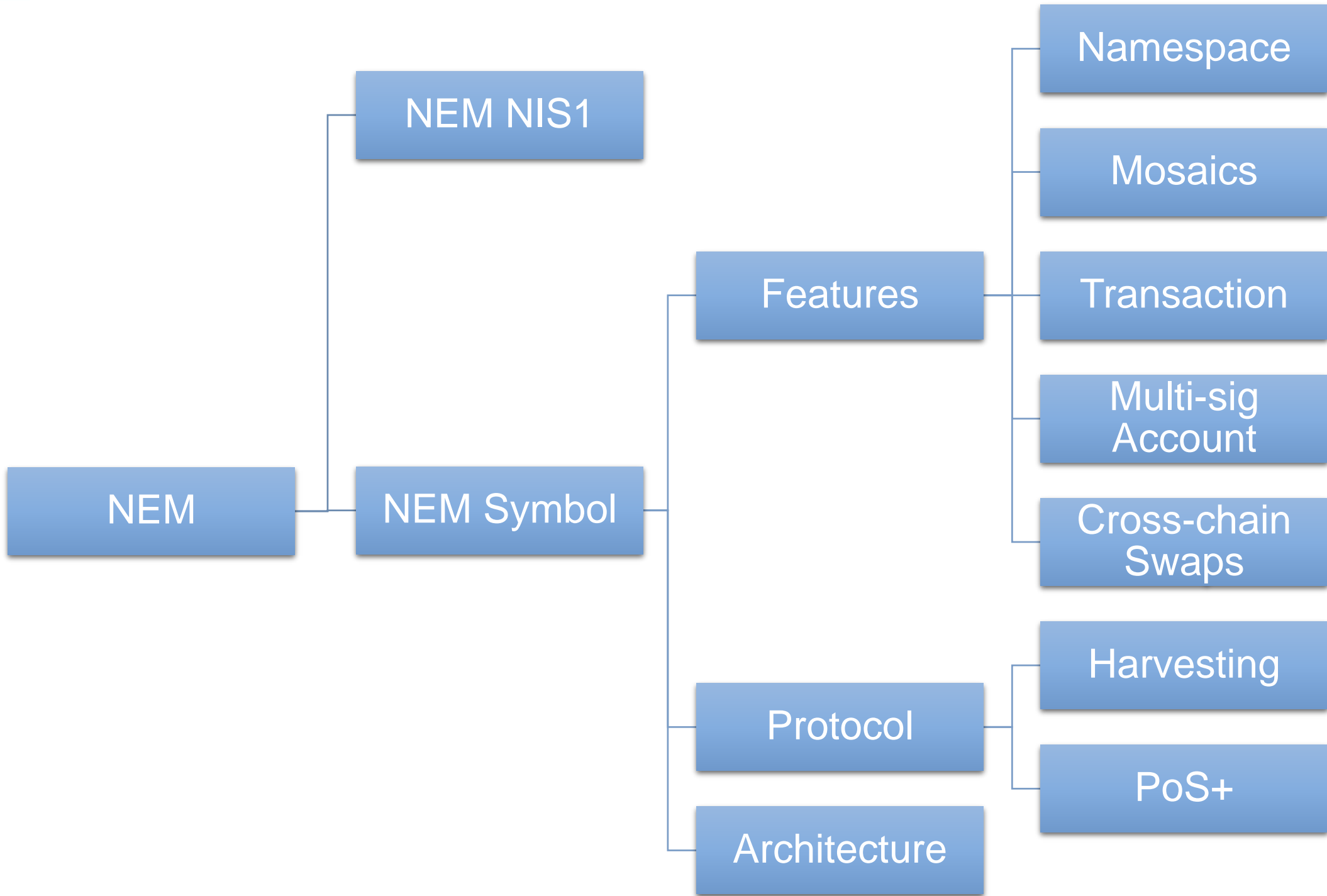


- Remote KYC procedures
- Blockchain
 - Transaction
 - Token swaps
 - Cross-chain swaps
 - A consensus algorithm with no transaction fee

NEM Symbol

Blockchain implementation





NEM (New Economy Movement)

- Blockchain developed from scratch
 - Implementation in most of the popular programming languages
 - Smart contracts can be written in those languages
 - Dedicates to making blockchain easy to used in assets trading
- Built-in features are “off-chain”
 - Unlike Ethereum (Quorum), NEM is not truly decentralized
 - Ease of future debug and update
- NIS1 (XEM) & Symbol (XYM)
 - Public NEM blockchain now using NIS1 and will be transit into Symbol in 2020
 - Symbol supports cross-chain swaps

Features

Smart Assets

Namespace & Mosaics
make assets recognizable

Transaction

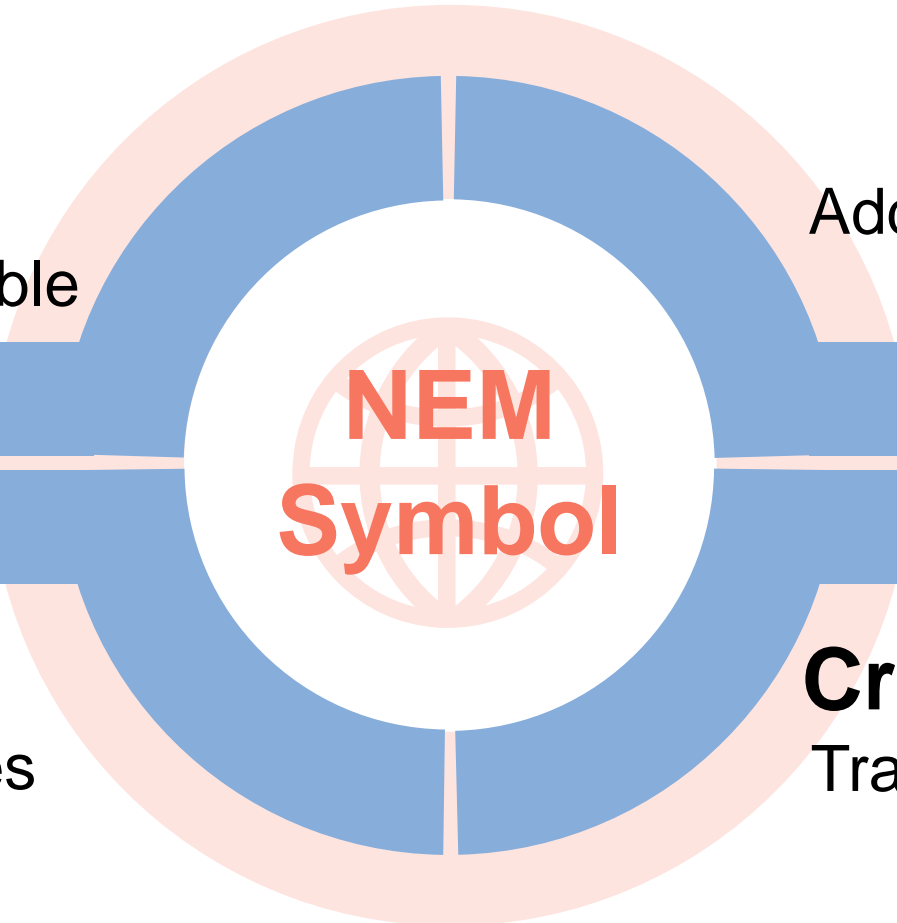
Additional secret message
is able to be attached

Account

Multi-sig account makes
account management
more convenient

Cross-chain Swaps

Transaction is not limited to
a single blockchain

The logo features a central white circle containing a red globe icon with latitude and longitude lines. Overlaid on the globe is the text "NEM" in red, with "Symbol" in red below it. This central element is surrounded by a thick blue ring, which is further enclosed by a thin light red ring. Two horizontal blue bars with a slight 3D effect extend from the left and right sides of the blue ring. A solid blue horizontal bar runs across the bottom of the entire image.

**NEM
Symbol**

Smart Assets: Mosaics

- Digital tokens
 - Can be anything that can be transferred
- Configurable properties
 - Divisibility
 - Duration
 - Transferable
- Restriction
 - The creator can decide which accounts can access the mosaics

Namespace

- Can be linked to an account or a mosaics
 - The “name” replacing an id
 - Two mosaics cannot have a same name
 - Subnamespaces can be built under a namespace
- The duration time can up to 365 days (15 sec. a block)
 - After that, the original account registering the name have priority to continue the registration in 30 days
- Rental fee is required

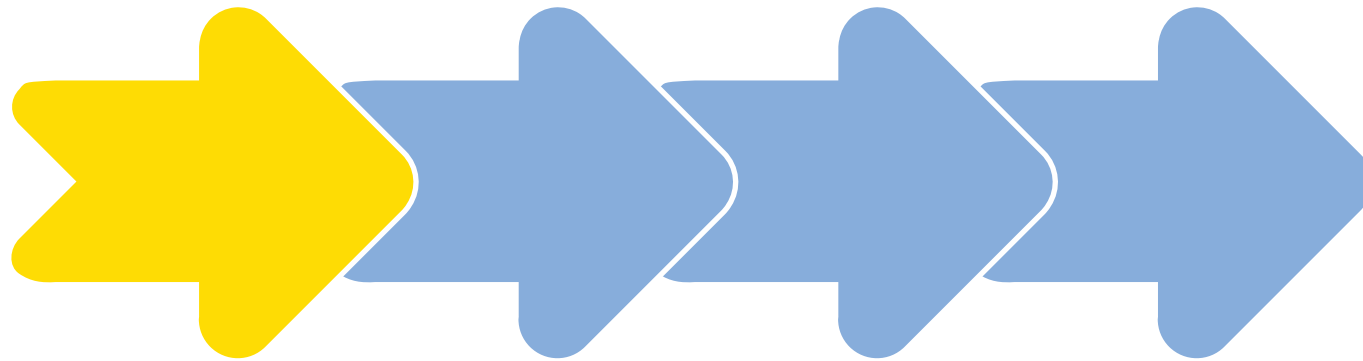
Transaction

- Transfer transaction
 - Transfers mosaics from an account to another account
 - An encrypted message can be attached
- Aggregate transaction
 - Multi-participants transaction
 - Before the transaction is verified by the harvester, all participants' signatures should be attached
 - All transfers inside is processed at the same time
 - Can be used in token swaps scene

Atomic Cross-chain Swaps

- Transaction between two blockchain
 - In LBCoin's case, transfer LBCoin to NEM public blockchain
- Hashed Timelock Contract (HTCL)
 - Two accounts in each network
 - Lock the payloads in transactions
 - To unlock the payloads, a “proof” is required
 - Once all transaction are done, the payload will be unlock simultaneously in both blockchains
- Limitations
 - The same hash algorithm is required
 - Certain formats of transaction should be compatible

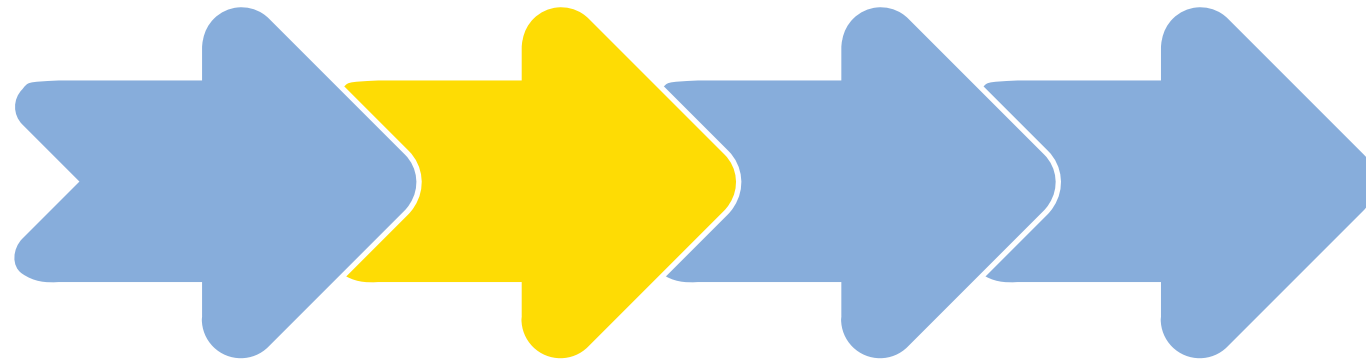
Supposed that Alice pays 10 token1 (private blockchain) in exchange of 10 token2 (public blockchain) from Bob...



01 Transaction 1 (private)

Alice generates a random number called proof (10~1000 bytes), stating payload (10 token1) with the hash value of proof in Tx1. Only by knowing the proof can Bob unlock the payload.

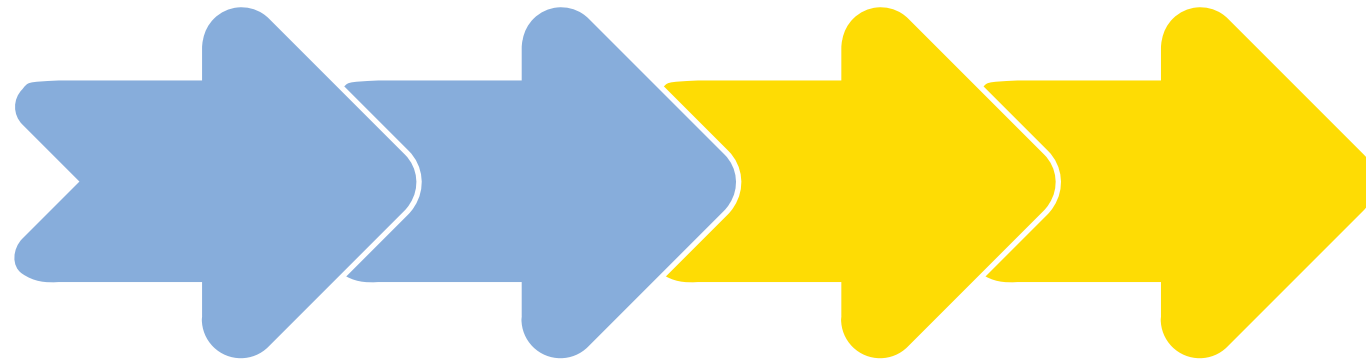
Supposed that Alice pays 10 token1 (private blockchain) in exchange of 10 token2 (public blockchain) from Bob...



02 Transaction 2 (public)

After receiving Tx1, Bob sends Tx2 to public blockchain, stating the payload (10 token2) and the hash value of proof from Tx1. Only by knowing the proof can Alice unlock the payload.

Supposed that Alice pays 10 token1 (private blockchain) in exchange of 10 token2 (public blockchain) from Bob...



03 Transaction 3 (public)

After receiving Tx2, Alice announces the proof to unlock her token2.

04 Transaction 4 (private)

After knowing the proof, Bob is able to unlock his token1.

PoS+

- Developed from Proof of Stake
 - PoS makes the rich richer, causing a huge wealth gap among the network though PoS is indeed efficient
 - Instead of stake, PoS+ calculates important scores to determine the harvester (validator)
- Important score
 - The node having more contribution to the network has higher possibility to be chosen as the harvester
 - Calculated from stake score (S'), transaction score (T') and node score (N')
 - Changeable parameter: a, p, t, n

Important Score

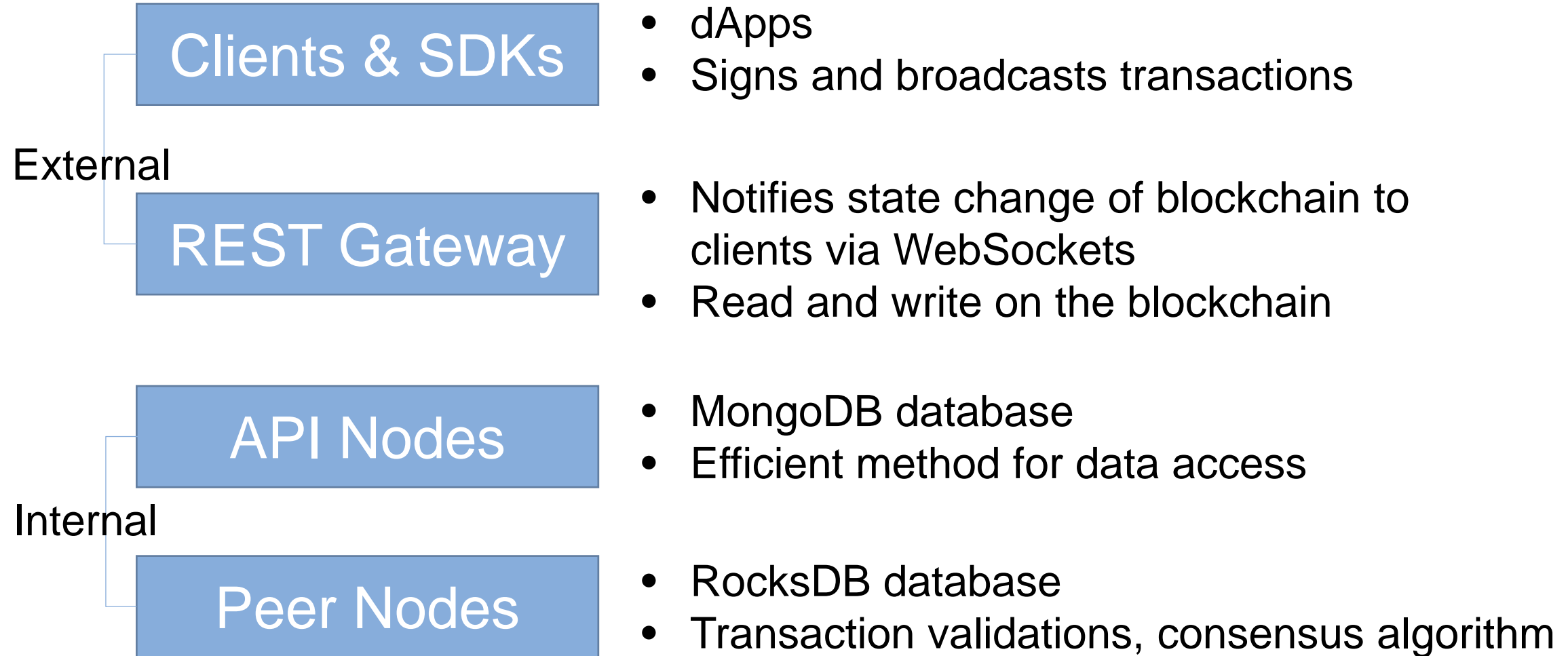
$$(1 - a) * S' + a * \left| \frac{p}{S'} * (t * T' + n * N') \right|$$

- Stake Score (S'): percentage of effective balance of all high-value account.
- Transaction Score (T'): percentage of total transaction fees in a period.
- Node Score (N'): percentage of total beneficiaries in a period.

Cryptography

- Digital Signature Algorithm
 - EdDSA with Ed25519
- Message Digest (inconsistency in official document)
 - SHA-512 in EdDSA (SHA3-512 in NIS1)
 - SHA3-512 in Merkle Tree
- AES with CBC mode

4-Tiered Architecture



CBDC

Development of Central Bank
Digital Currency and its possible
impact on current financial
system



29 million of mobile accounts in Taiwan

1.23 mobile phones per person on average

85.9 % of citizens have access to the internet

Much more higher than global average

**It is such an attractive proposal to
make transactions “digital”...**

Central Bank

- Lender of last resort (The bank of commercial banks)
- Fiat money (banknotes) minter
- Goals
 - Single vs. Dual
 - High employment, Price stability, Economic growth
 - Financial stability (after financial crisis in 2008)
 - FED: “Maximum sustainable employment, stable prices and moderate long-term interest rate”
 - 央行：「促進金融穩定，健全銀行業務，維護對內對外幣值穩定，於上述目標範圍內，協助經濟之發展」

Central Bank Digital Currency (CBDC)

- Fiat digital currencies
 - The values are backed by CBs
- Features (according to The Bank of England)
 - Can be accessed more broadly than reserves
 - Greater functionality for retail transactions than cash
 - Separate structure to other forms of CB money, allowing it to serve a different core purpose
 - Interest bearing (will be discussed later)
- Implementation
 - Blockchain? Decentralized networks?

CBDC: Advantages

- RTGS (Real Time Gross Settlement)
- Efficiency
 - Payment systems and Cross-broader payments
 - More perfect financial market
 - Lower default risk
- No counterfeit
- Competition from private e-payment services
 - E-payment services are de facto financial institution
- CBs can directly affect markets
 - Helicopter money

Currency

- Functions

- Unit of account, medium of exchange and standard for deferred payment

- Money supply

- Reserve money: $H = C + R$
 - $M_{1A} = C + DD$
 - $M_{1B} = C + DD + SD = m \times H$
 - $M_2 = M_{1B} + Q$
 - CB's goal is to affect M_2 implicitly through its direct control over H

Possible Impact on Monetary Policy

- Money multiplier

- $m = \frac{M_{1B}}{H} = \frac{1+d+s}{d+\rho_d+\rho_s s+e}$

- How much “money” can CB create by changing reserve money

- CBDC's impact

- CBDC is a payment method, which meets the definition of \mathcal{C}
 - Households will shift their bank deposits to payment instrument
 - $d \uparrow$ (Institutional side), $s \downarrow$ (costumer's side) $\rightarrow m \downarrow$
 - CB may find harder to conduct an expansionary policy

Possible Impact on Interest Rate

- Structure of interest rate
 - Risk structure: $i = r + \pi^e + d + l + m + t$
 - Fisher's equation: $i = r + \pi^e$
- Shall CBDC pay interest?
 - CBDC has high liquidity, with no default risk
 - Compare to bank deposits: $d \downarrow, l \downarrow$
 - Compare to cash: $l \uparrow$
 - CBDC interest rate will be the floor of money market rate → monetary policy instrument

Possible Impact on Interest Rate

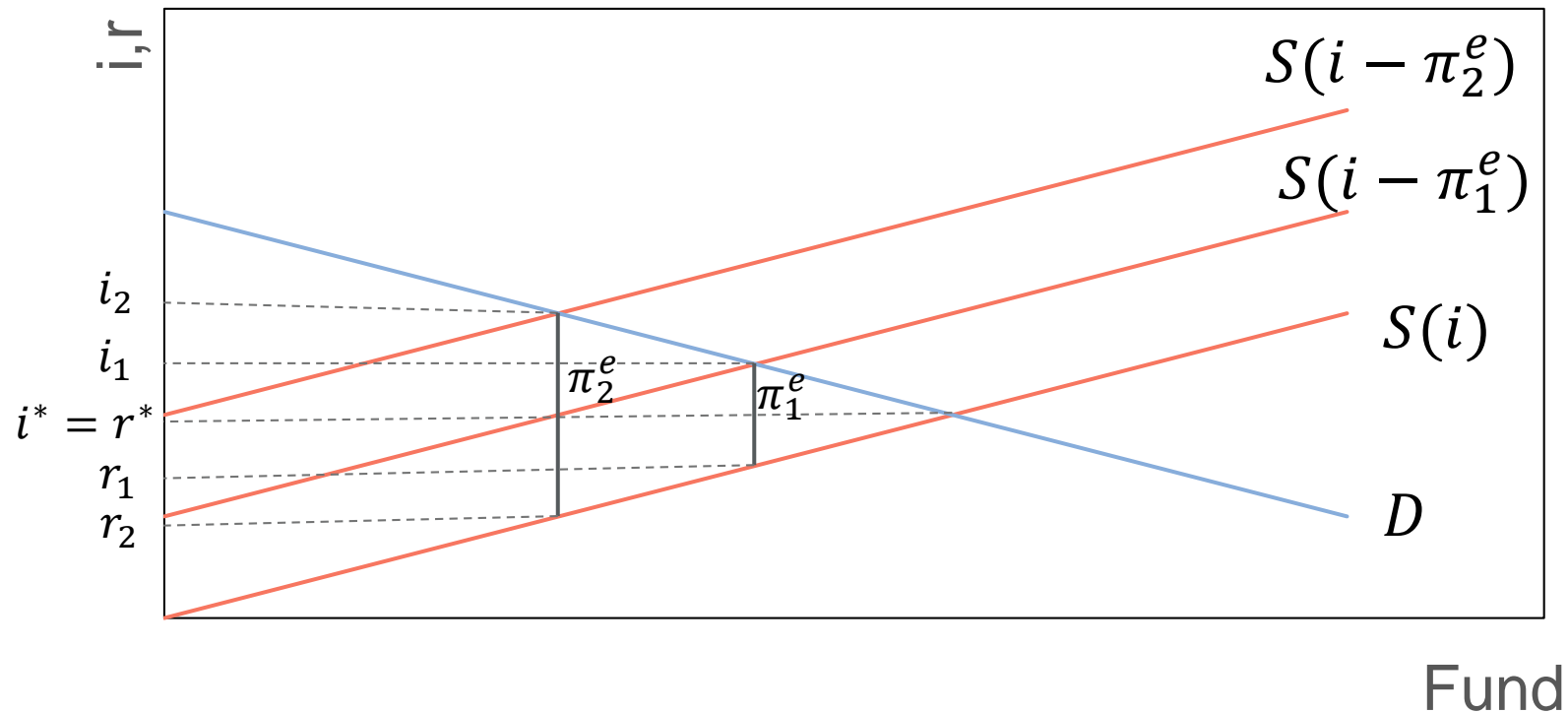
- Short-term impact
 - Money market assets and bank deposits may have higher return rates due to losing demand
 - Fisher effect ($\Delta\pi^e = 0$): $i \uparrow, r \uparrow$
 - An austerity policy in disguise, causing lower output of an economy
- Long-term impact
 - If CB doesn't conduct expansionary policies with the issuance of CBDC, through income effect the economy will be likely to undergo deflation
 - If CBDC replaces cash to some extent, it will be easy to set the nominal interest rate lower than zero

Possible Impact on Interest Rate

- It is difficult to say which future will happen
 - There are no historical data
 - CBDC is something between cash and money market assets
 - It depends on investors' expectation
 - There are models showing different result
- Impact on monetary economics
 - CBDC may give rise to a new field to study in for monetary economists
 - Regarding this, economists can have a deeper insight to the behavior of investors and consumers

Possible Impact on Interest Rate

- A reverse way to see this (Mundell-Tobin effect)
 - Suppose in long-term, i, r, π^e are not sticky, then $i \uparrow, r \downarrow, \pi^e \uparrow$
 - Now it is a expansionary policy, causing the rise of output



Other impacts

- Helicopter money
 - Ultimate measure to boost economy in theory
 - QE means that CB buys financial assets (such as bonds), which means the currency it uses to buy assets will come back eventually
 - Helicopter money will not go back to CB's pocket
- Stability
 - Unlike deposits, CBDCs are fully backed. There are no default risk
 - Though in long-term this improves financial stability, it may result in bank runs in short term

Other impacts

- Disintermediation of banks
 - Commercial banks are financial intermediaries in current financial system
 - Blockchain technology can make P2P loans possible and with minimum default risk
 - Competition between banks and CBDC
 - More reliance on other services
- Privacy
 - Trade-off between security and privacy
 - How should we design CBDC?

Other impacts

- A huge change in financial systems
 - Not in foreseeable future, but can be an ultimate goal
 - Stock exchange can be continuous, non-stop, and matched through smart contracts
 - In fact, it is possible for all transferable assets to achieve this
 - An economy with low (or even no) transaction cost and friction
 - Intermediaries are not necessary anymore
- Transition to a more perfect market
 - Adding an assets to an economy with incomplete market may make everyone worse off (Newbery and Stiglitz 1984)

CBDC: Design

- Will it replace banknotes?
 - Is saying goodbye to physical currencies the ultimate goal?
- Cross-broader integration
 - There should be a technical standard in order to perform efficiency in cross-broader transactions
- Regulations
 - Is there any restriction to use CBDCs?
 - Which measures can CB use to affect the market, and under which circumstances can CB intervene the market?

Blockchain Design

- **Permissioned or permissionless network**
 - Shall users undergo KYC process?
- **Consensus**
 - Trade-off between speed and the extent of decentralization
 - Nodes have no trust to each other, but CB node must be trusted
- **Wholesale or retail**
 - Shall CBDC directly face the public, or facing financial institutions only?
- **Public or private transaction**
 - Trade-off between privacy and financial stability
 - To what extent shall the government monitor the market?

CBDC in Taiwan

- Challenges

- Taiwan is an opened economy, where exchange rate is of significant important in regard of international trade
- Technical details must be integrated with our trade partner in order to enjoy lower cost of cross-broader payments
- Consensus with domestic banks as well as foreign banks on the development of CBDC

CBDC in Taiwan

- Design
 - Wholesale CBDC
 - For financial institutions only
 - Banks may develop their own digital currencies for their customers
- Project status
 - The CBDC will undergo concept proof in Q3, 2020



Q & A



Thank You