Vilnius University

„Blockchain“ – tai gerokai daugiau nei tik skaitmeninės valiutos

2021-05-25
Vilnius

Prof. dr. Remigijus Paulavičius

TURINYS

- **Trumpai apie įkurtą Blokų grandinių technologijų (*blockchain*) grupę**

1. **Blockchain istorija ir evoliucija**
   - **Pagrindiniai motyvai “blockchain" technologijos atsiradimui?**
   - **Kaip *Satoshiui Nakamoto* pavyko padaryta tai, ko nepavyko kitiems?**
   - **Kuo skiriasi „blockchain“ nuo *Bitcoin* ir nuo DLT?**
2. **Kitos skaitmeninės valiutos: *Ethereum*, *Dogecoin*, *Libra, LBCoin* ir pan.**
   - **Ar saugu yra naudoti skaitmenines valiutas: pagrindiniai atakų tipai ir ar realu jas įvykdyti?**
3. **Kokie yra kiti blockchain sprendimai ir taikymai?**
   - **Lietuvos Banko „LBChain“ projektas.**
   - **Ką mokslininkai veikia šioje srityje ir kokia galima šios technologijos artimiausia ateitis?**

Blokų grandinių technologijų grupė

Įkurta: 2018 m. vasario mėn., Vilniaus Universite, Duomenų Mokslo ir Skaitmeninių Technologijų Institute (DMSTI)

https://www.mii.lt/struktura/moksliniai-padaliniai/bloku-grandiniu-technologiju-grupe

Įkūrėjai: Prof. dr. **Remigijus Paulavičius** ir doc. dr. **Ernestas Filatovas**

Komanda: 1 vyriausias mokslo darbuotojas, 2 vyresnieji mokslo darbuotojai, 2 mokslo darbuotojai ir 5 doktorantai.

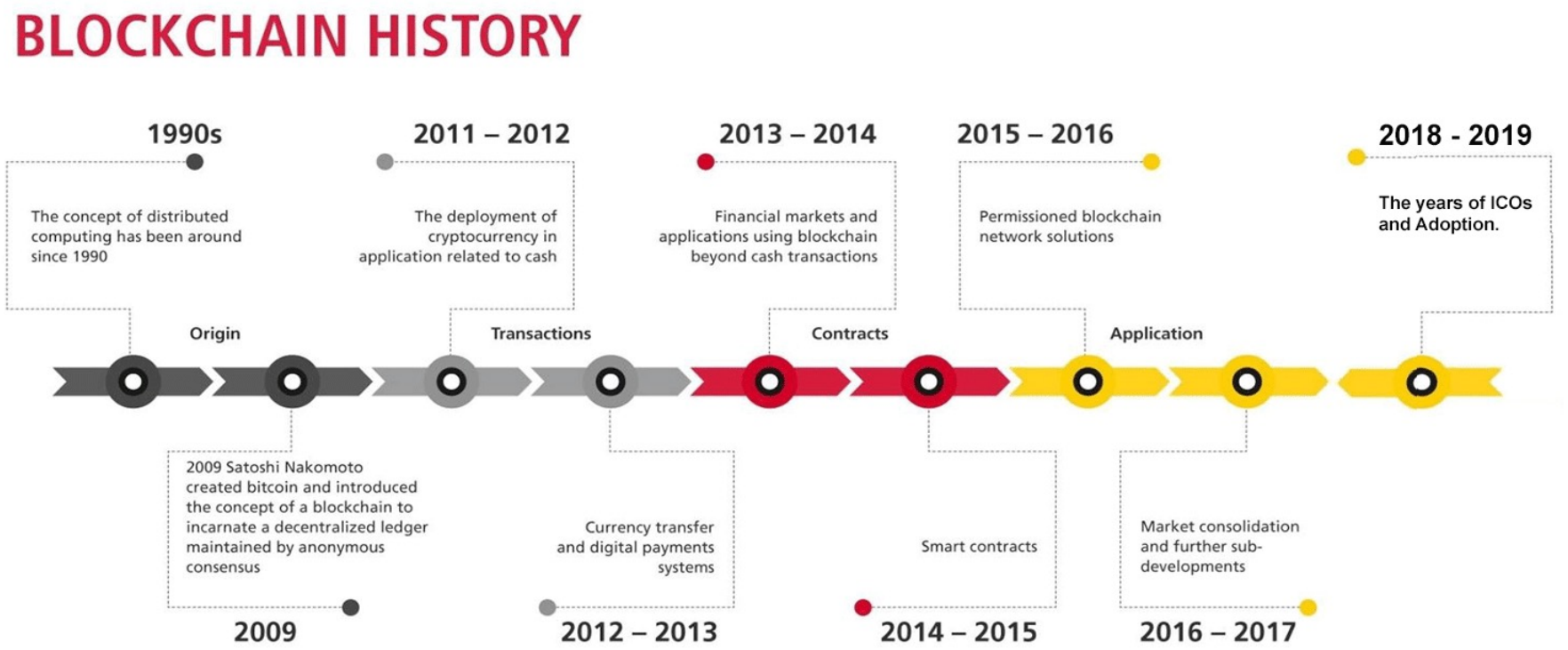
Misija: Dirbame ties efektyvesniais „blockchain“ sprendimais per švietimą, konsultavimą ir inovacijas.

Švietimas: „Blokų grandinių technologijos“ studijų moduliai bakalauro ir doktorantūros studijų pakopų studentams; organizuojame studentų praktikas; *blockchain* seminarai, *blockchain* technologijos populiarinimas.

Konsultavimas: Dirbame tiek su mokslinių tyrimų institucijomis tiek ir su verslo įmonėmis siekdami sukurti inovatyvių *blockchain* technologija paremtus sprendimus. Projektuojame koncepcijas bei prisidedame prie inovatyvių projektų įgyvendinimo.

Blockchain istorija ir evoliucija

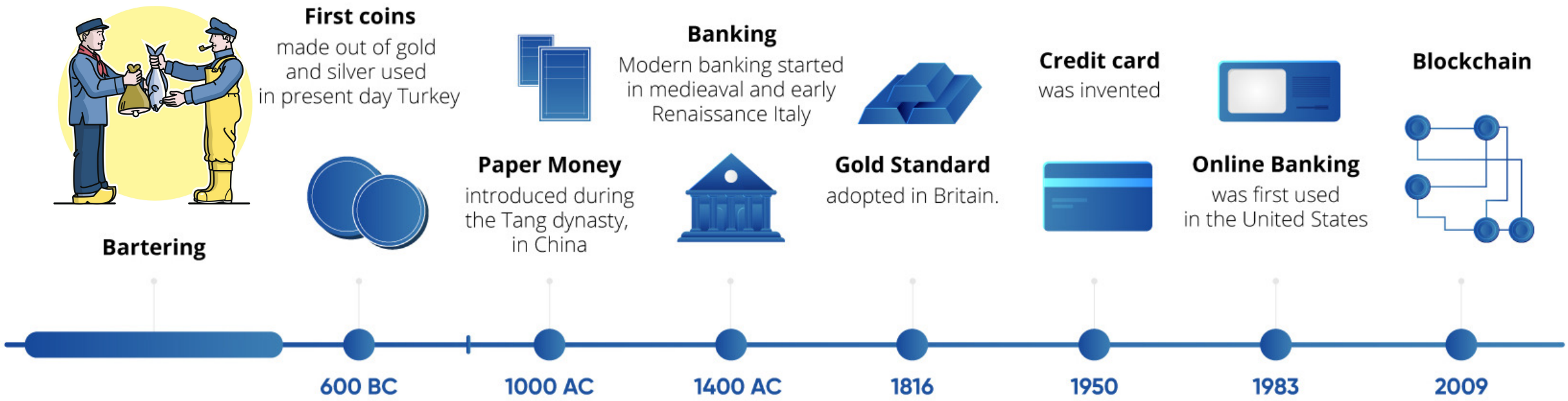
- **Pagrindiniai motyvai „blockchain“ technologijos atsiradimui?**
- **Kaip *Satoshiui Nakamoto* pavyko padaryta tai, ko nepavyko kitiems?**
- **Kuo skiriasi „blockchain“ nuo *Bitcoin* ir nuo DLT?**



Vilnius University

Blockchain atsiradimo prielaidos

Vertės (pinigų) istorija

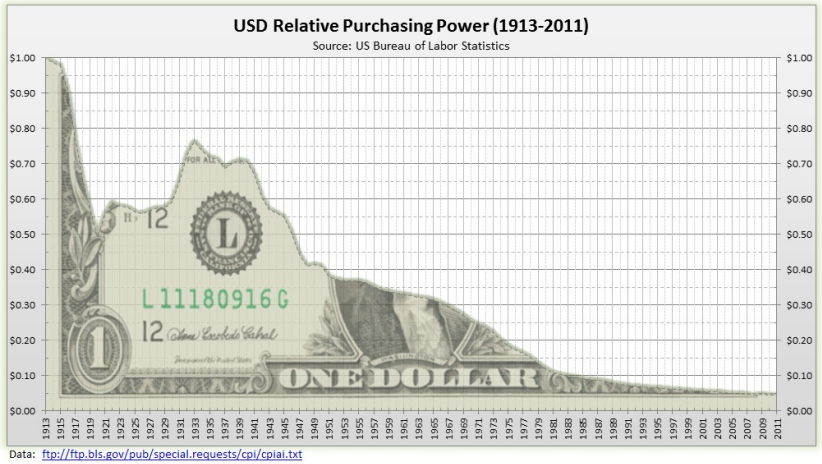


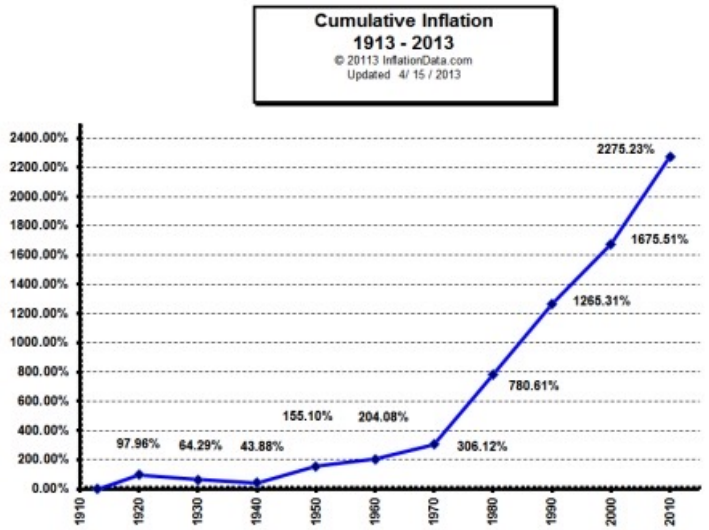
Šaltinis: https://lisk.io/academy/blockchain-basics/what-is-blockchain/history-of-value

- Pirmiausiai pinigų funkciją atliko mainai, kurių metu buvo keičiamasi bet kokiu turtu. Tačiau ne visi norėjo kumpio ar žuvies ☺
- Banknotai, kaip pinigai, buvo priimti skirtingu metu visame pasaulyje. Viena pirmųjų tai padarė Kinija.
- Pirmieji „bankai“ iš tikrųjų buvo religinės šventyklos.
- Tęsiant praktiškumo tendenciją XXI amžiuje, popieriniai pinigai pamažu nyksta, juos keičia praktiškesnės skaitmeninės laikmenos.
- Tačiau skaitmeninė bankininkystė, kuria dabar naudojamės kasdien, dar toli gražu nėra tobula. Pirmiausia, ją visiškai **kontroliuoja trečiosios šalys**.

(Elektroninių) pinigų iššūkiai

- **Dvigubas išlaidavimas**
  - Siekiant išvengti dvigubo išlaidavimo reikalinga trečia šalis, kuria galima pasitikėti
  - Nustojus veikti trečiajai šaliai (dėl gedimo ar atakos) neįmano atlikti transakcijų
- **Infliacija**
  - Pinigų nuvertėjimas bėgant laikui dėl nuolat didėjančios pinigų emisijos
- **Naujų pinigų atsiradimo mechanizmas**
  - Kas atlieka pinigų emisiją?
  - Dažnai tai būna jokia verte nepadengti pinigai
- **Privatumas**
  - Daugumoje sistemų bankai „mato“ visas transakcijas





Skaitmeninės mokėjimo sistemos ir Bitcoin atsiradimo prielaidos

eCash[1] - *David Chaum* straipsnyje [Chaum, 1983][1] suformavo elektorinių pinigų koncepciją – aprašyta automatizuota mokėjimo sistema, kurioje trečioji šalis „nemato“ informacijos apie transakcijas.

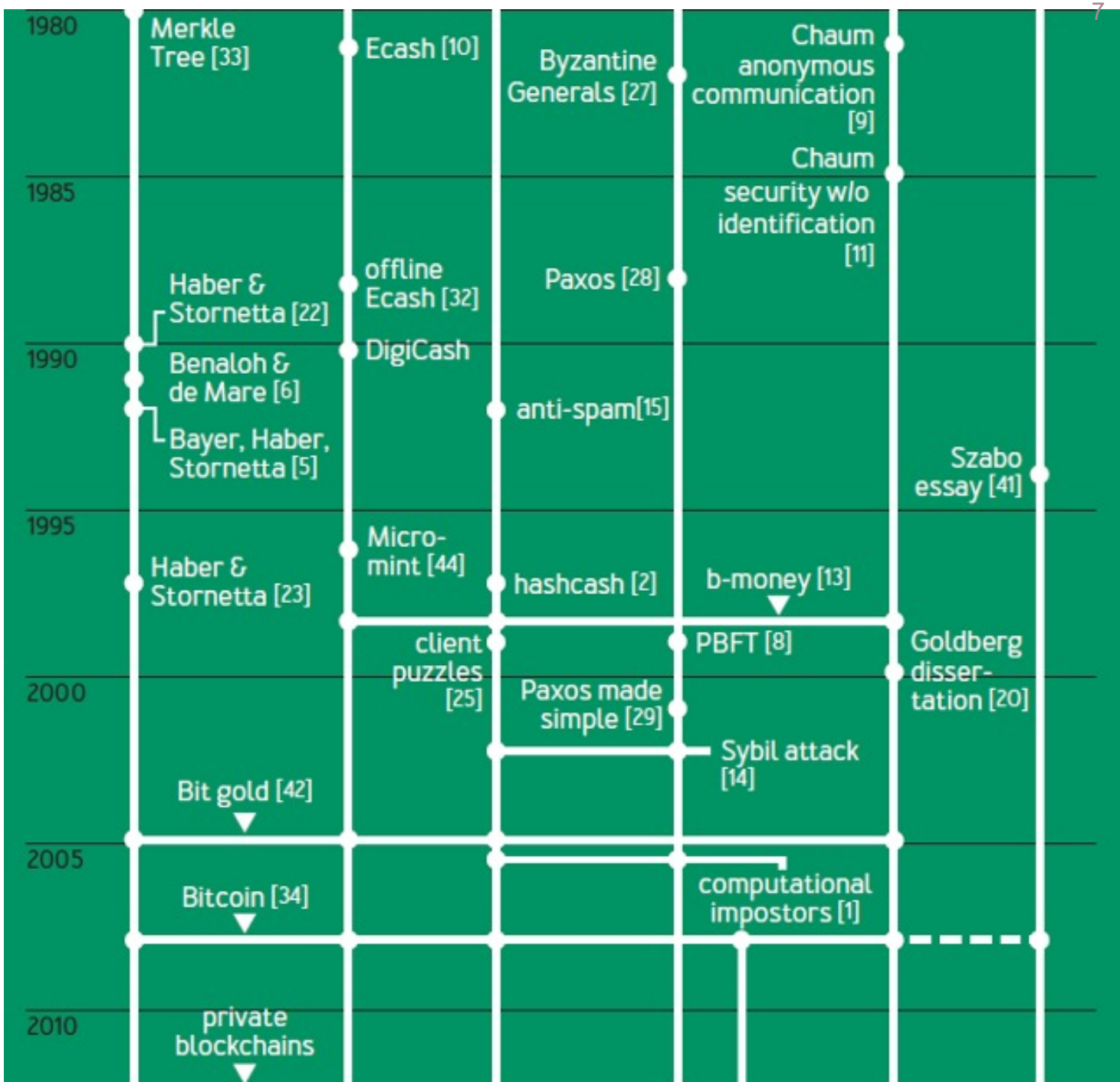
- Sistema sukurta 1990 m. *DigiCash* korporacijos
- Mokėjimu saugumas ir privatumas buvo užtikrinamas naudojant kriptografinius protokolus. Neįgijo pakankamai populiarumo

Hashcash[2] - 1997 m. *Adam Back* suprojektavo sistemą, kurioje naudojant pasiūlytas įrodymo darbu (angl. *Proof-of-Work*) algoritmas, siekiant kovoti su el. pašto brukalu ir DDOS atakomis.

b-money[3] - 1998 m. Wei Dai, pasiūlė decentralizuotos valiutos koncepciją. Niekada nubuvo įgyvendinta.

Bit gold[4] - 2005 m. *Nick Szabo* sukūrė mechanizmą decentralizuotai skaitmeninei valiutai. Niekada neįgyvendinta.

[1] *Chaum, D., 1983. Blind signatures for untraceable payments. Advances in Cryptology. In: Proceedings of Crypto, vol. 82. Springer, pp. 199–203.*
[2] A partial hash collision based postage scheme (Txt). Hashcash.org.
[3] http://unenumerated.blogspot.com/2005/12/bit-gold.html.
[4] http://www.weidai.com/bmoney.txt



Kas sukūrė Blockchain?

- **2008-10-31** anoniminis Bitcoin įkūrėjas **Satoshi Nakamoto** (pseudonimas) paskelbė ***white paper****, kuriame buvo pasiūlyta lygiarangė (angl. *peer-to-peer, P2P*) elektroninės valiutos (*Bitcoin)* koncepcija unikaliai apjungusi egzistavusias technologijas.
- **2009-01-03** Pradėjo veikti pirmasis ***blockchain*** - Bitcoin.

Google Scholar pacituota daugiau nei 15 000 kartų!

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving a trusted third parties to process electronic payments. While the system works well enough fo most transactions, it still suffers from the inherent weaknesses of the trust based model Completely non-reversible transactions are not really possible, since financial institutions canno

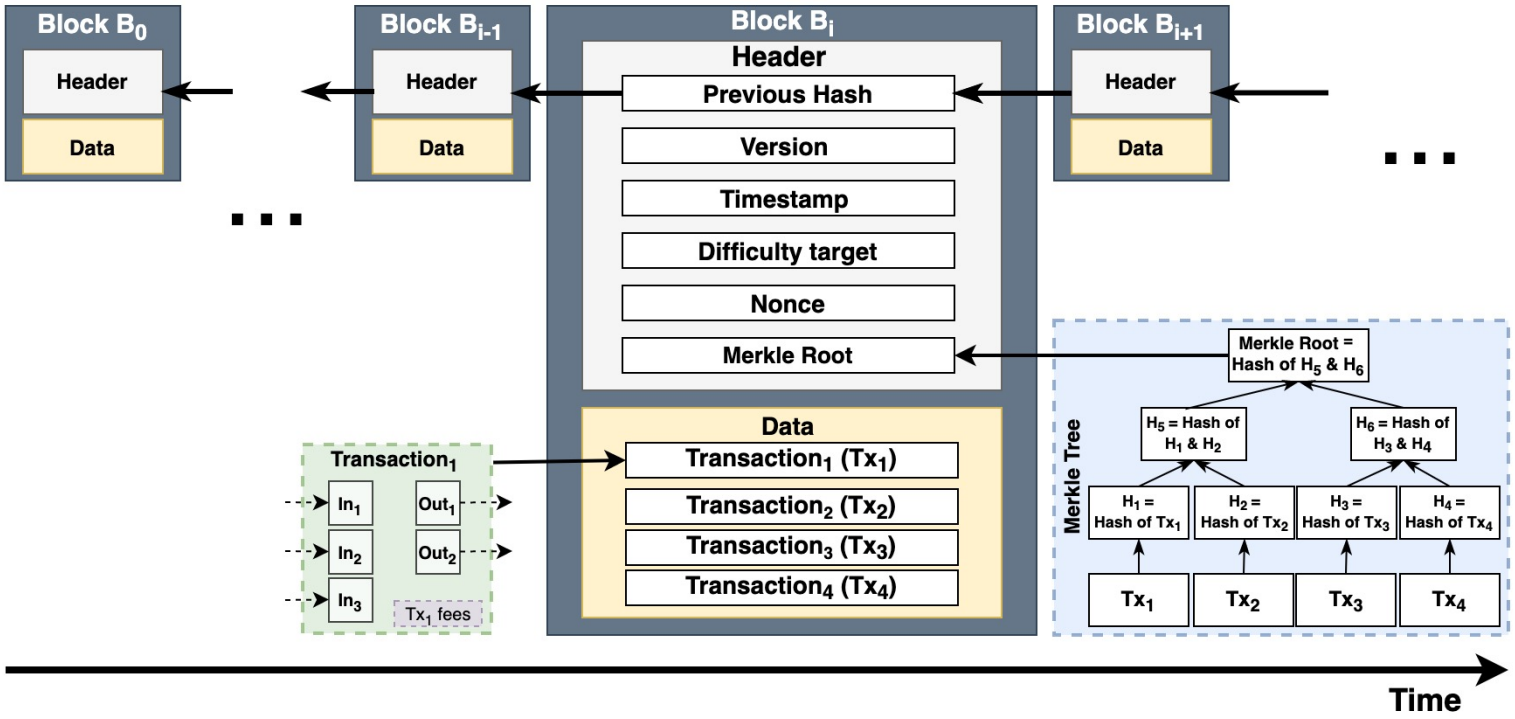
*https://bitcoin.org/bitcoin.pdf

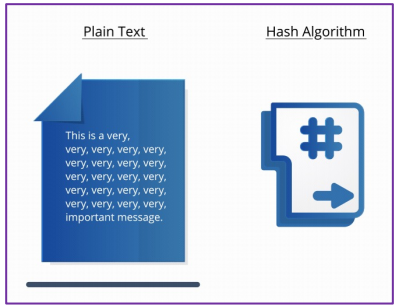
Pirmasis oficialus Bitcoin (BTC) panaudojimas komerciniame sandoryje

Kas yra blokų grandinė (angl. blockchain)?

Blokų grandinė (paprasčiausiai) apibrėžiama kaip decentralizuota paskirstytoji duomenų bazė/didžioji knyga (angl. *ledger*), kurioje registruojama skaitmeninio turto kilmė bendru konsensusu (sutarimu) nedalyvaujant 3-ai šaliai.

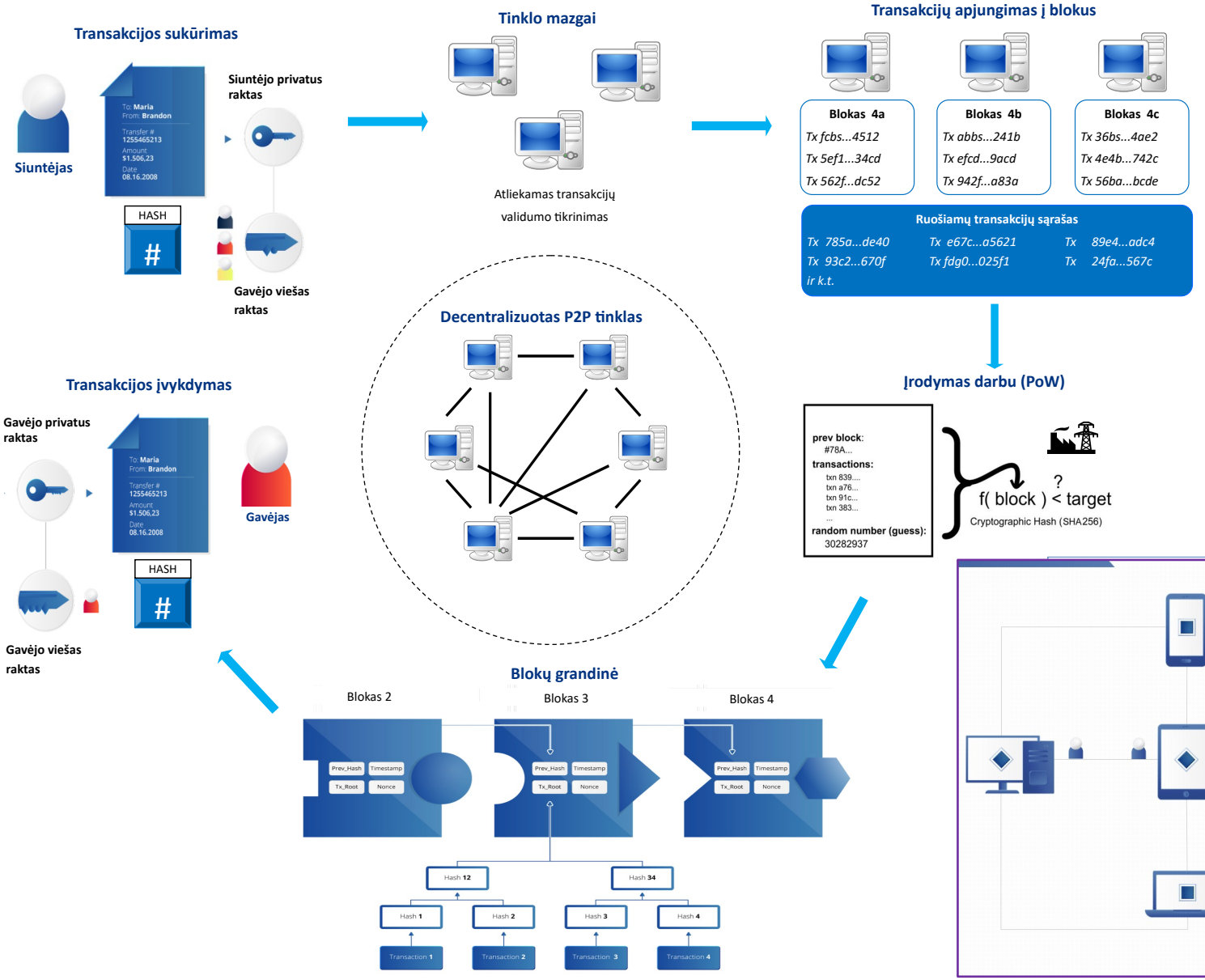
Blockchain tipo duomenų bazę yra sudaryta iš įrašų (transakcijų/sandorių), kurie sudaro vienas kitą susietus (panaudojant kriptografiją) **blokus**.

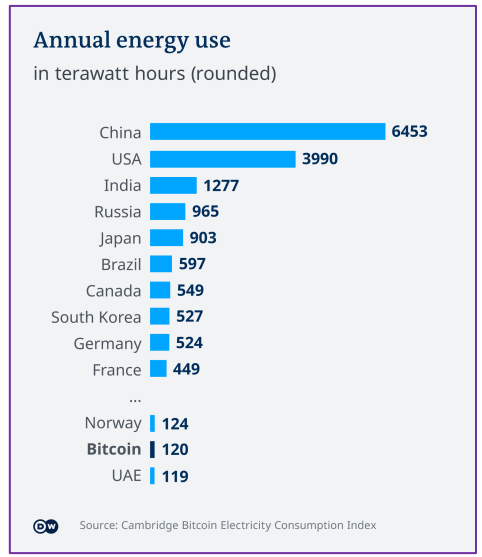




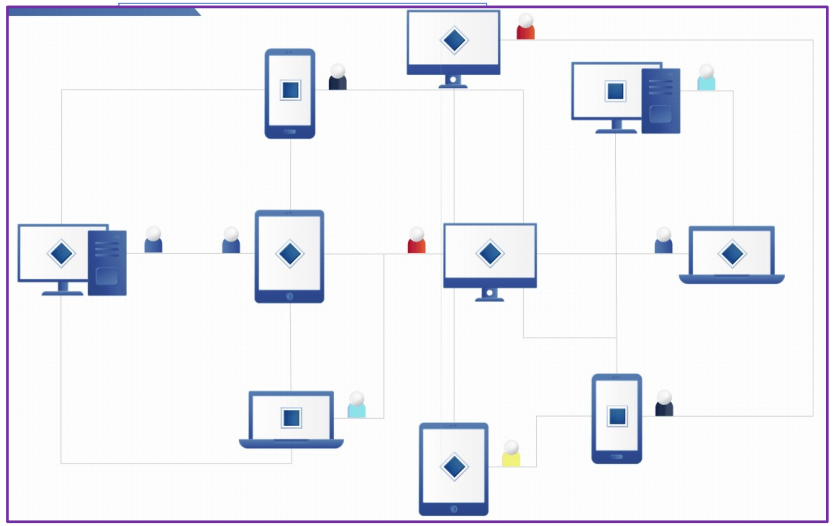
„Blockchain“ Lietuvoje: jau nuo ~1960 ☺

BLOCKCHAIN VEIKIMAS





https://cbeci.org/



Kaip patyrinėti blockchain'ą?

Dešinėje yra parodytas pats pirmasis Bitcoin blokas:
https://www.blockchain.com/btc/block/0

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks".


THE TIMES

Eat Out from £5
More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Israel prepares to send tanks and troops into Gaza

Michael Sheen Frost, Nixon and me

Working mums So that's how she does it

Detox in style The best spas on the planet

Salmon Rushdie I Won't Marry Again

Giant Killing? Guide to the FA Cup Third Round

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

https://en.bitcoin.it/wiki/Genesis_block

Blockchain.com Wallet Exchange Explorer Buy Bitcoin Trade

Explorer › Bitcoin Explorer › Block

Search your transaction, an address or a block

USD

Block 0

USD BTC

This block was mined on January 03, 2009 at 8:15 PM GMT+2 by Unknown. It currently has 684,810 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 50.00000000 BTC ($1,911,850.50). The reward consisted of a base reward of 50.00000000 BTC ($1,911,850.50) with an additional 0.00000000 BTC ($0.00) reward paid as fees of the 1 transactions which were included in the block. The Block rewards, also known as the Coinbase reward, were sent to this address.

A total of 0.00000000 BTC ($0.00) were sent in the block with the average transaction being 0.00000000 BTC ($0.00). Learn more about how blocks work.

Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Confirmations	684,810
Timestamp	2009-01-03 20:15
Height	0
Miner	Unknown
Number of Transactions	1
Difficulty	1.00
Merkle root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Version	0x1
Bits	486,604,799
Weight	1,140 WU
Size	285 bytes
Nonce	2,083,236,893
Transaction Volume	0.00000000 BTC
Block Reward	50.00000000 BTC
Fee Reward	0.00000000 BTC

Block Transactions

Hash	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7a...		2009-01-03 20:15
	COINBASE (Newly Generated Coins)	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa	50.00000000 BTC
Fee	0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 204 bytes)		50.00000000 BTC

Bitcoin dydis ir tinklo dalyvių skaičius

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Mon May 24 2021 23:29:52 GMT+0300 (Eastern European Summer Time).

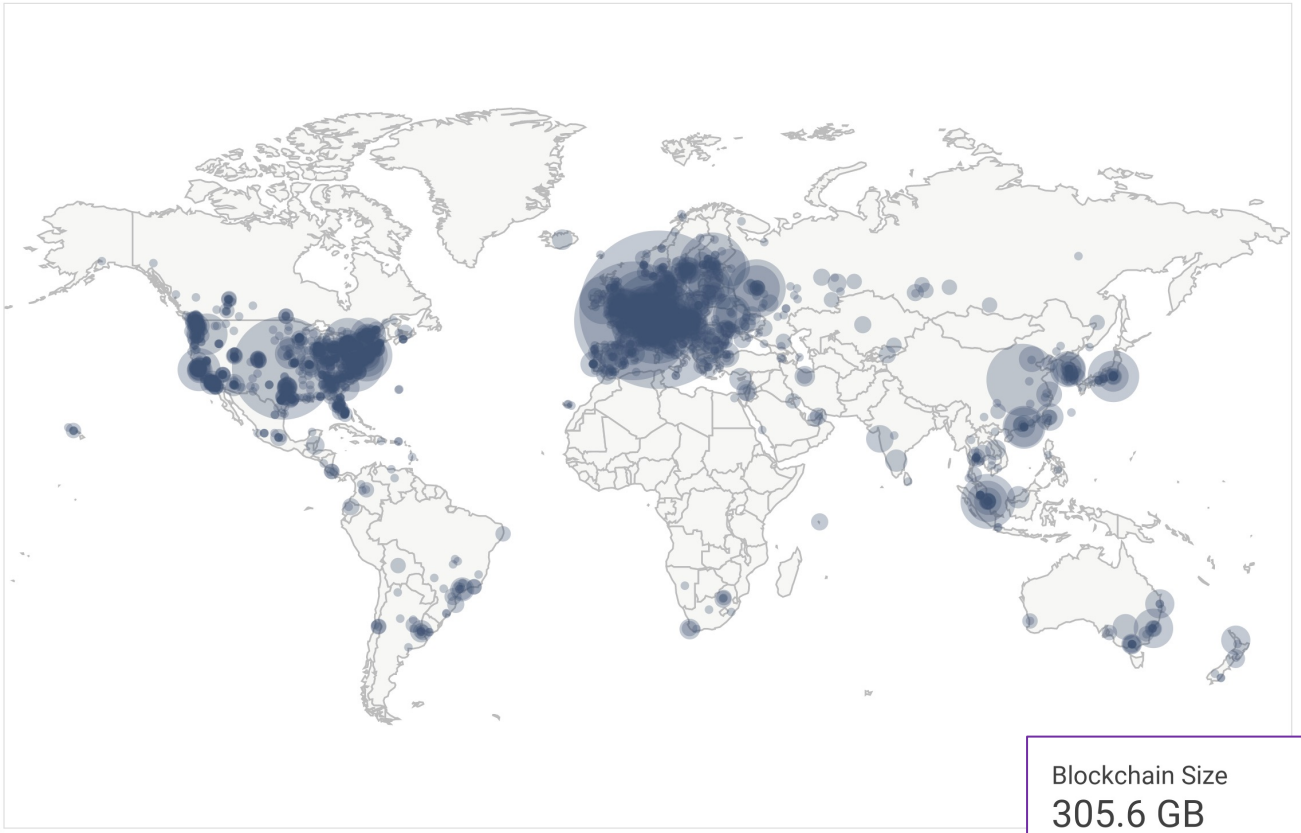
9863 NODES

24-hour charts »

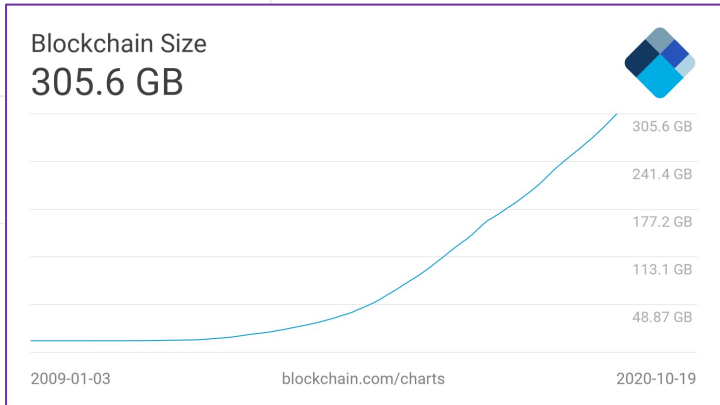
Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	1931 (19.58%)
2	n/a	1927 (19.54%)
3	Germany	1792 (18.17%)
4	France	591 (5.99%)
5	Netherlands	418 (4.24%)
6	Canada	319 (3.23%)
7	United Kingdom	265 (2.69%)
8	Russian Federation	247 (2.50%)
9	China	195 (1.98%)
10	Finland	155 (1.57%)

More (93) »



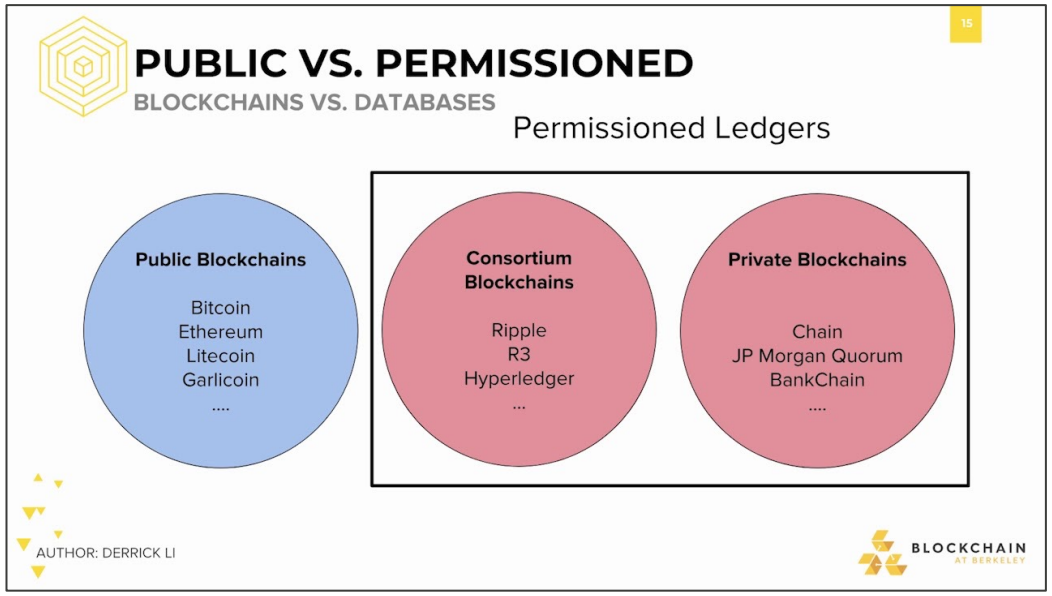
Map shows concentration of reachable Bitcoin nodes found in countries around the world.

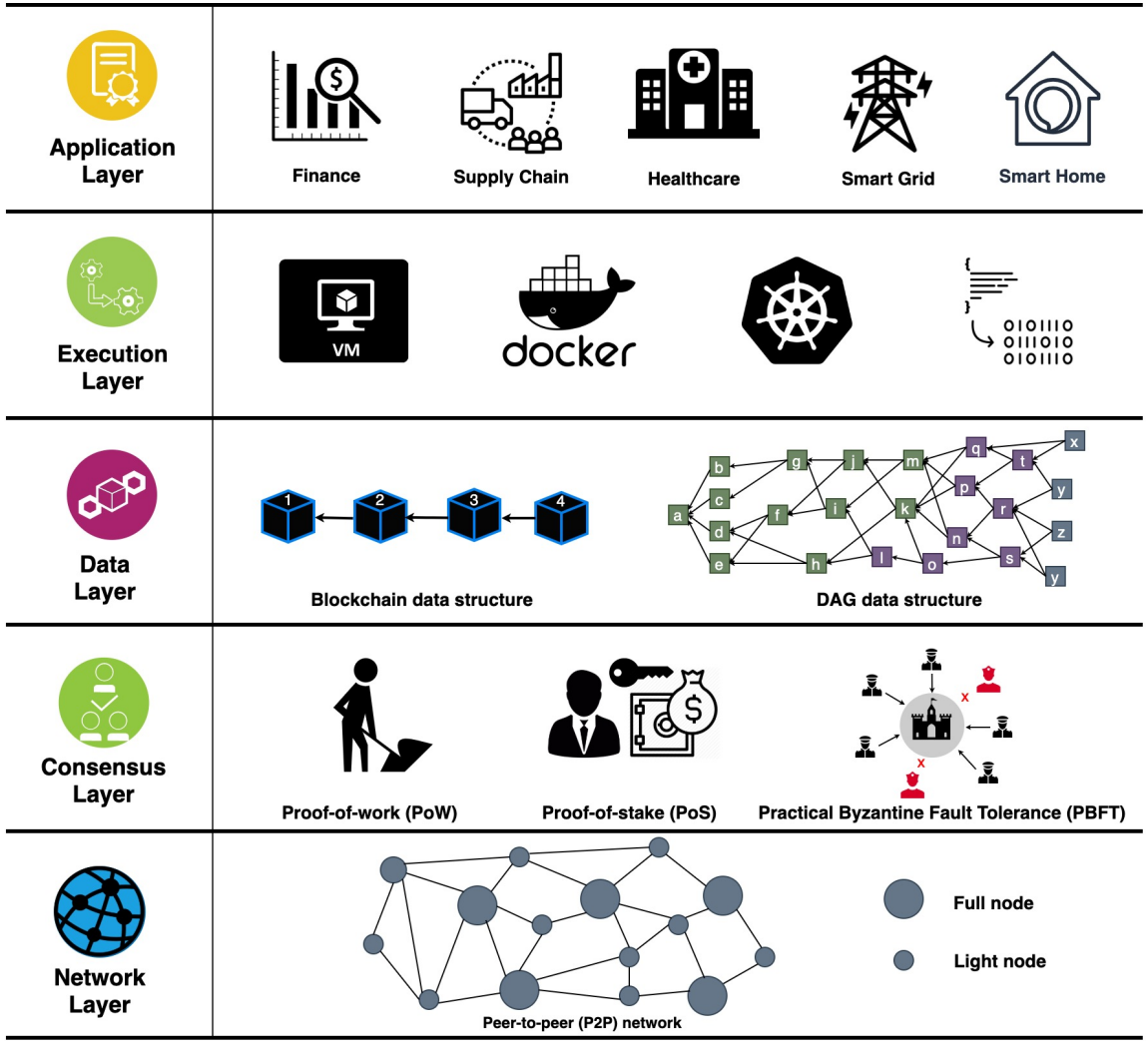


Blockchain - paskirstytųjų duomenų technologijų (angl. *distributed ledger technologies*, DLT) poaibis

Kuo skiriasi „blockchain“

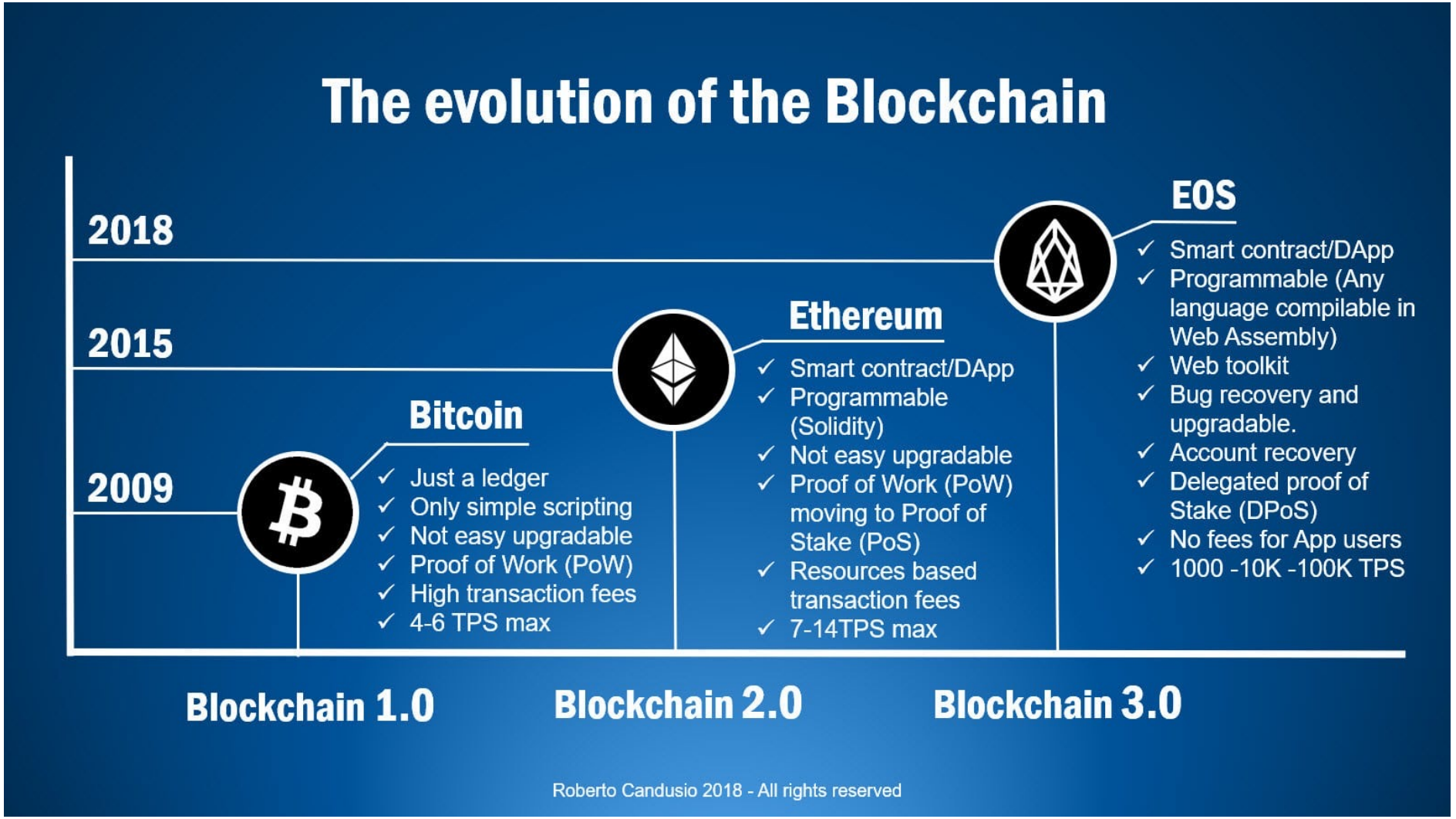
nuo *Bitcoin* ir nuo DLT?





DLT kaip daugiasluoksnės sistemos abstrakcija

Blockchain evoliucija



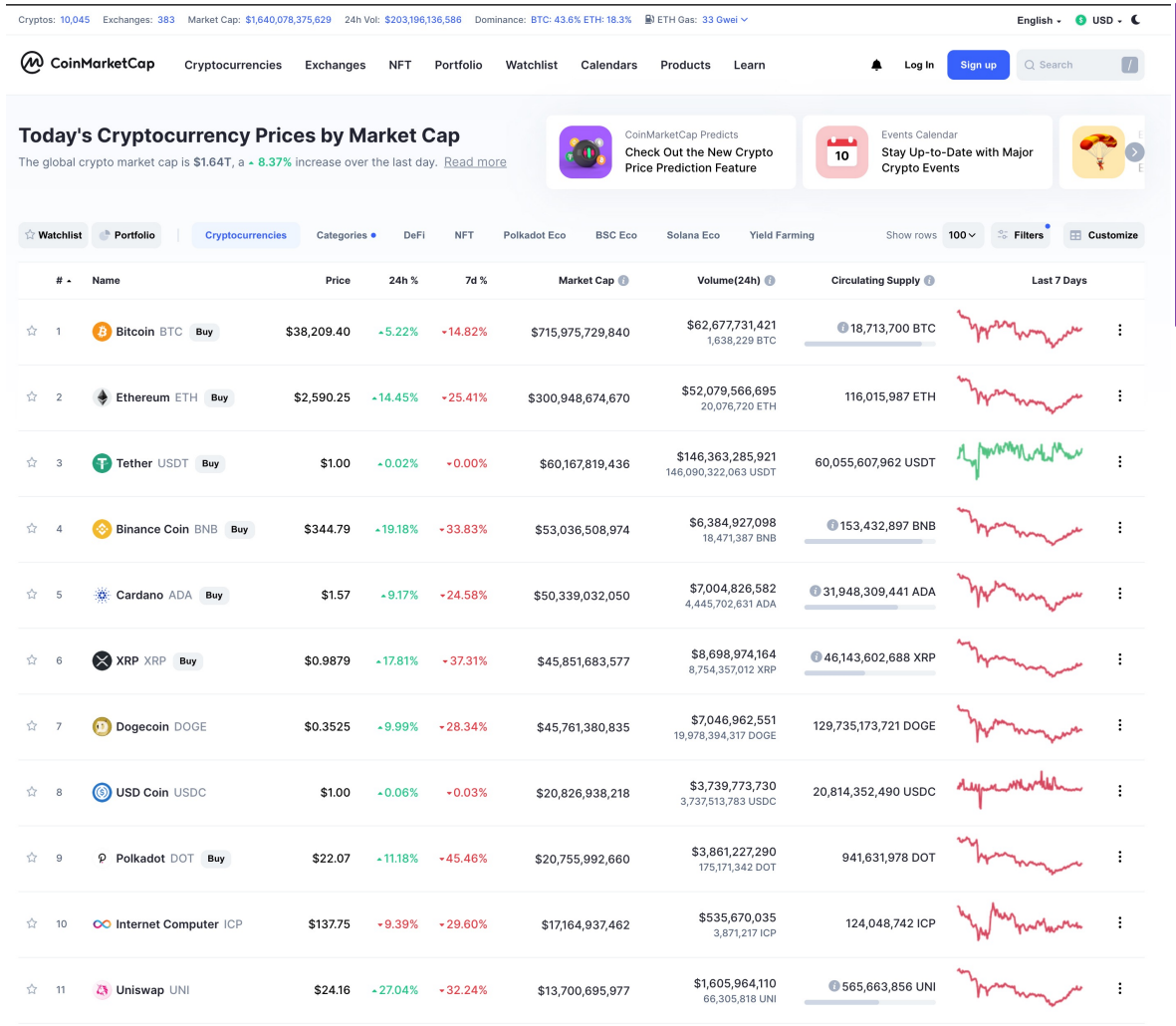
Šaltinis: https://trybe.one/the-blockchain-is-slowly-becoming-mature/

Kitos skaitmeninės valiutos: *Ethereum*, *Dogecoin*, *Libra, LBCoin* ir pan.

- **Ar saugu yra naudoti skaitmenines valiutas: pagrindiniai atakų tipai ir ar realu jas įvykdyti?**

Vilnius University

Daugiau nei 10 000 skirtingų skaitmeninių valiutų



https://coinmarketcap.com/

What Is Ethereum (ETH)?

Ethereum is a decentralized open-source blockchain system that features its own cryptocurrency, Ether. ETH works as a platform for numerous other cryptocurrencies, as well as for the execution of decentralized smart contracts.

Ethereum was first described in a 2013 whitepaper by Vitalik Buterin. Buterin, along with other co-founders, secured funding for the project in an online public crowd sale in the summer of 2014 and officially launched the blockchain on July 30, 2015.

Ethereum's own purported goal is to become a global platform for decentralized applications, allowing users from all over the world to write and run software that is resistant to censorship, downtime and fraud.

Libra

Facebook is shifting its Libra cryptocurrency plans after intense regulatory pressure

The Libra project will now support existing currencies in addition to the proposed Libra token

By Nick Statt | @nickstatt | Mar 3, 2020, 5:54pm EST

SHARE

White paper: https://www.diem.com/en-us/white-paper/

Dogecoin

Buterin atsakas: https://vitalik.ca/general/2021/05/23/scaling.html

LBCoin –

pirmoji pasaulyje skaitmeninė kolekcinė moneta

LBCOIN moneta yra pirmoji pasaulyje skaitmeninė kolekcinė moneta, sukurta taikant blokų grandinės technologiją.

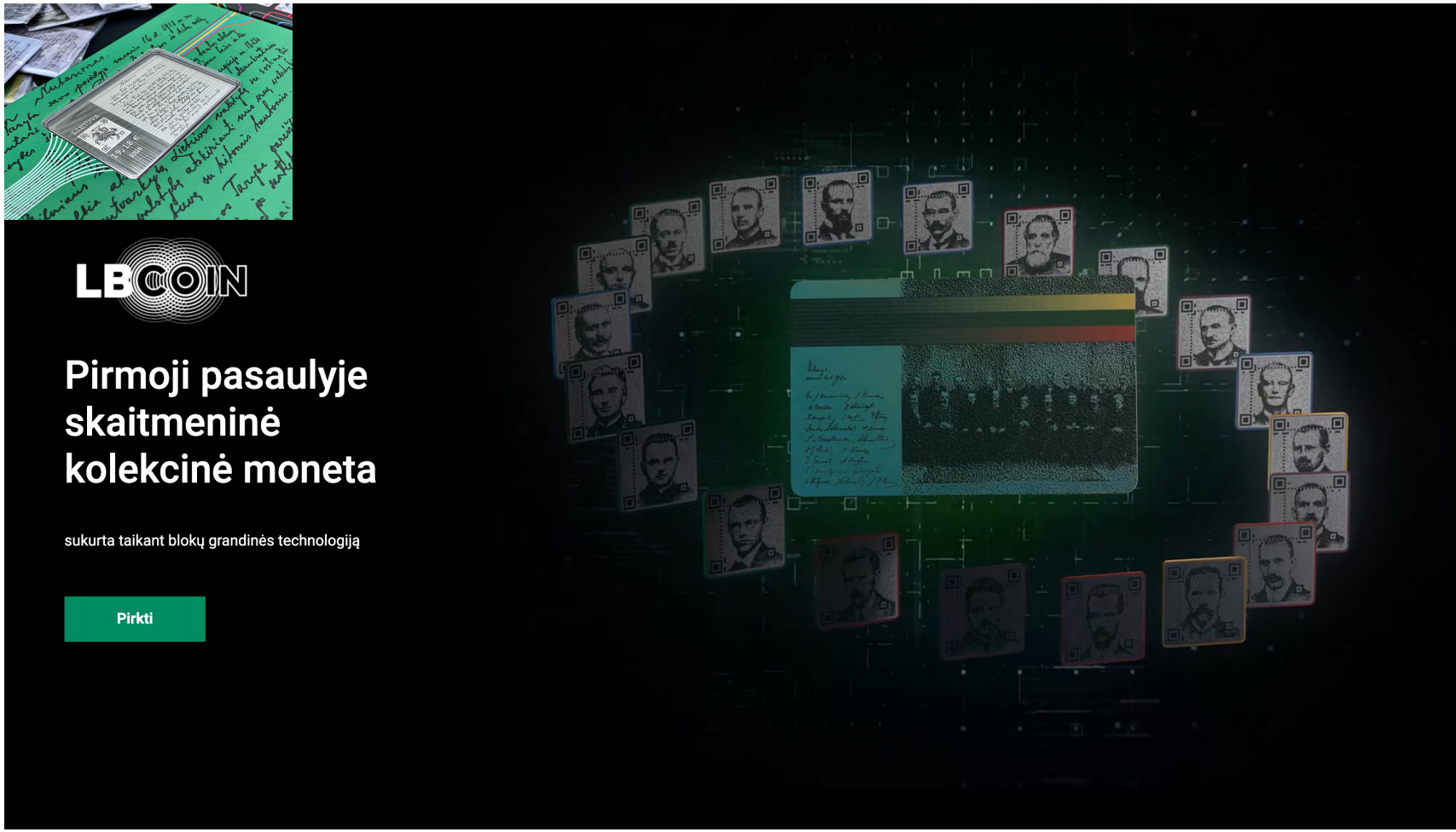
LBCOIN moneta yra Lietuvos banko išleistas šešių skaitmeninių žetonų komplektas ir fizinė kolekcinė moneta, kurią pirkėjas gaus mainais už šešis skaitmeninius žetonus.

Lietuvos bankas išleis 24 tūkst. blokų grandinės technologija sukurtų skaitmeninių žetonų ir 4 tūkst. fizinių kolekcinių monetų.

Kiekvienas skaitmeninis žetonas vaizduoja vieną iš dvidešimties signatarų. Skaitmeniniai žetonai suskirstyti į šešias kategorijas, atsižvelgiant į signatarų veiklos sritis – po 4 tūkst. kiekvienos kategorijos vienetų.

Pirkdami LBCOIN monetą, gaunate šešis atsitiktine tvarka parinktus skaitmeninius žetonus, tačiau tik surinkę šešis **skirtingų kategorijų** žetonus, juos galėsite išsikeisti į fizinę **kolekcinę sidabro monetą**.

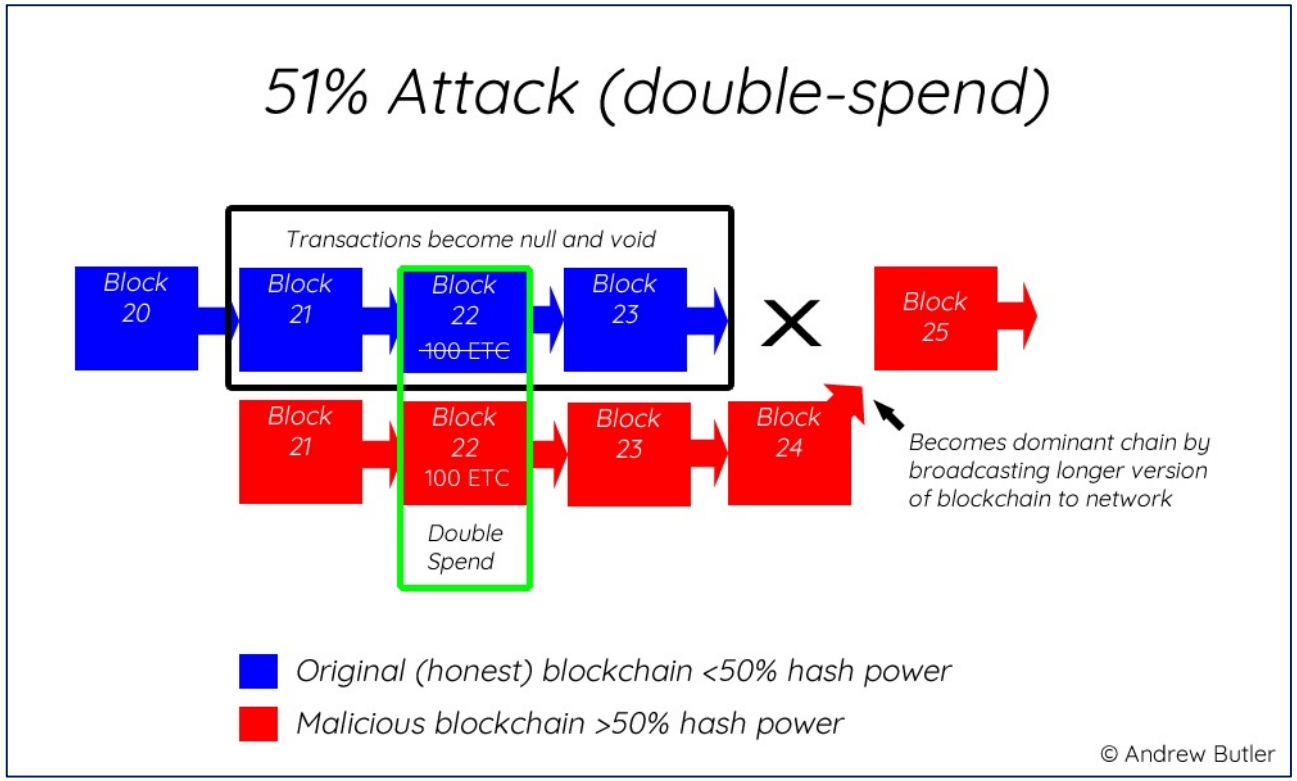
Fizinės kolekcinės monetos nominalas neįprastas – 19,18 Eur, jis skirtas 1918 m., Lietuvai svarbiai datai, įamžinti. Sidabro moneta – banko kortelės dydžio ir formos, joje vaizduojamas Nepriklausomybės aktas ir signatarai.



Daugiau informacijos: https://lbcoin.lb.lt/

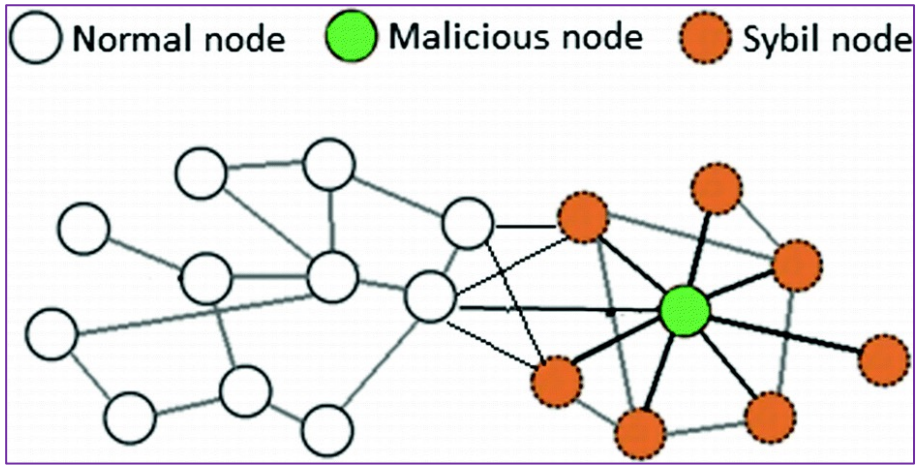
Ar saugu yra naudoti skaitmenines valiutas?

Pagrindiniai atakų tipai: 51% ataka



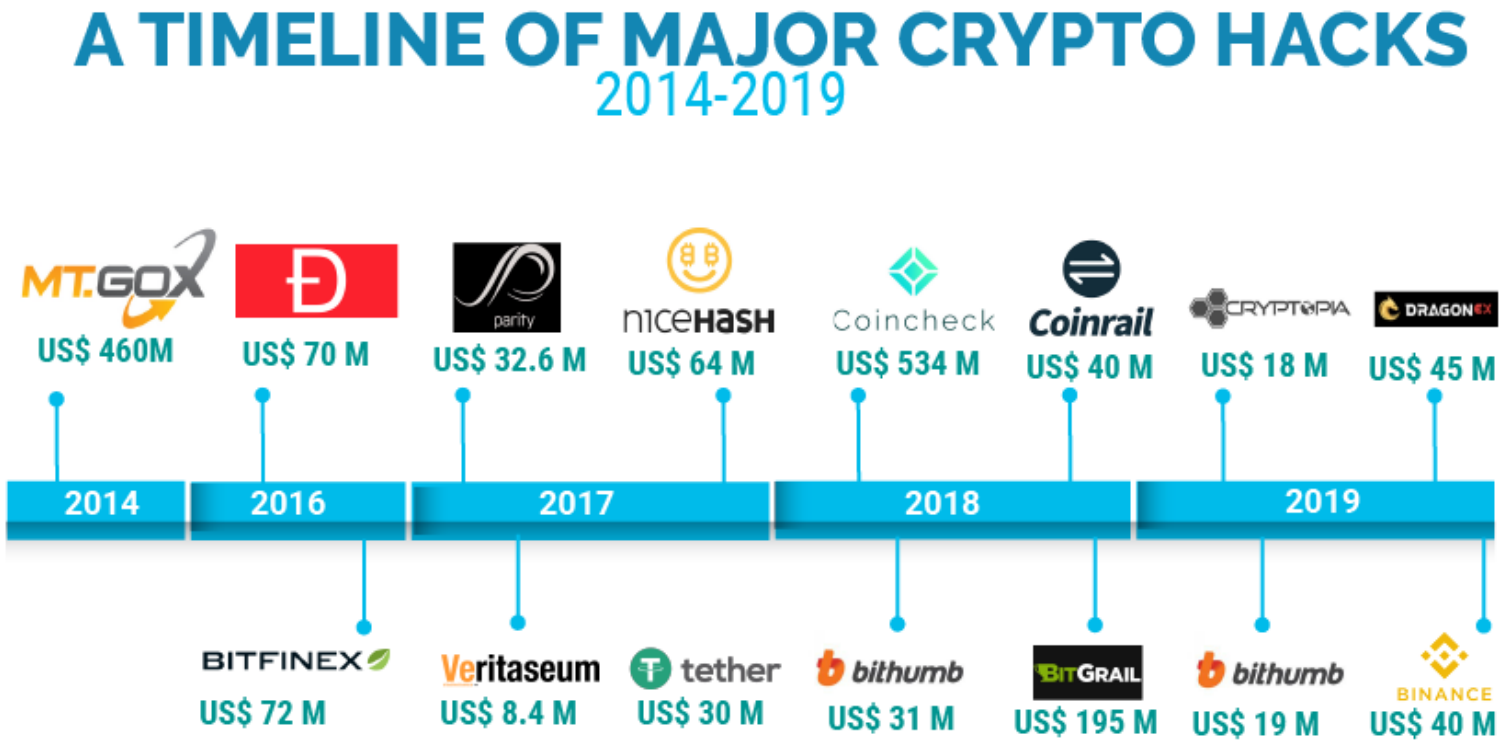
Plačiau: https://academy.binance.com/en/articles/what-is-a-51-percent-attack

Sybil ataka



Plačiau: https://academy.binance.com/en/articles/sybil-attacks-explained

Ar realu įvykdyti ataką?



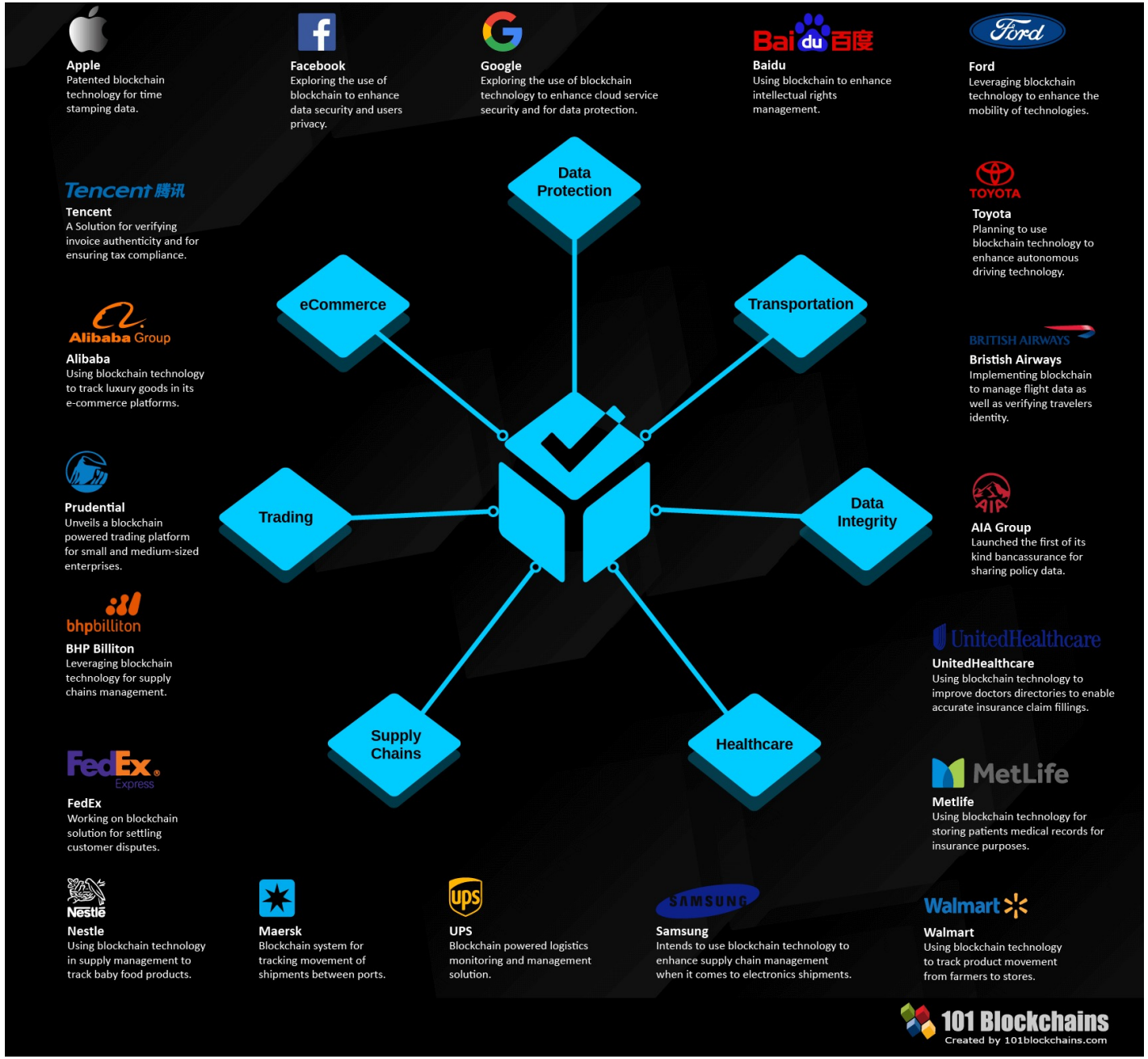
FINTECH SINGAPORE
fintechnews.sg

Šaltinis: https://fintechnews.sg/23594/blockchain/cryptocurrency-hack-binance/

Kiti blockchain sprendimai ir taikymai?

Lietuvos Banko „LBChain“ projektas

Ką mokslininkai veikia šioje srityje ir kokia galima šios technologijos artimiausia ateitis?



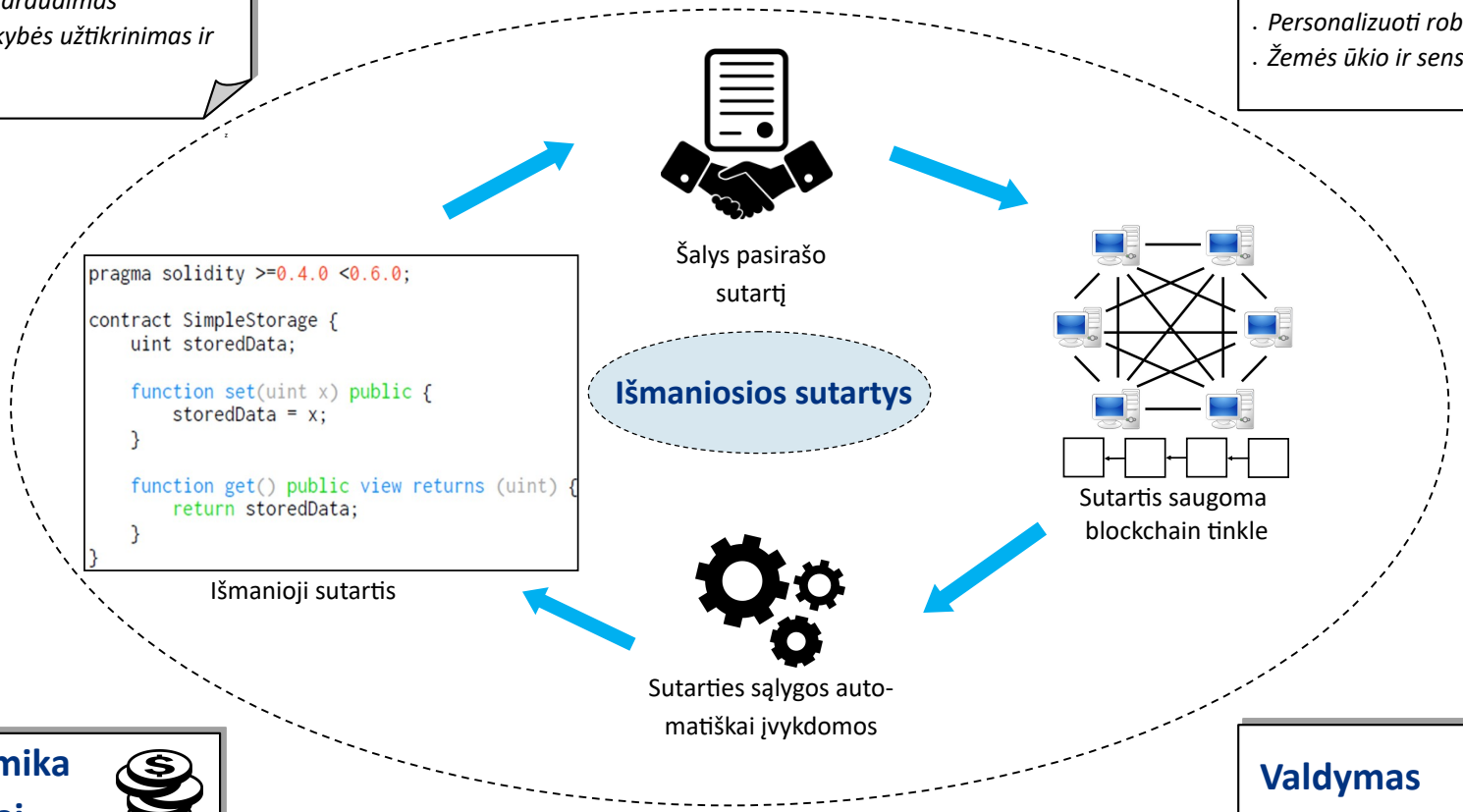
BLOCKCHAIN TAIKYMAI

Sveikatos apsauga

. *Elektroniniai sveikatos įrašai*
. *Klinikinių tyrimų duomenų bazės*
. *Sveikatos draudimas*
. *Vaistų kokybės užtikrinimas ir tiekimas*

Daiktų internetas

. *Išmanieji namai ir miestai*
. *Automobilių pramonė*
. *Tiekimo grandinės*
. *Personalizuoti robotai*
. *Žemės ūkio ir sensorių tinklai*




```
pragma solidity >=0.4.0 <0.6.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

Ekonomika Finansai

. *Kriptovaliutos*
. *Tarptautinės transakcijos*
. *P2P prekybos platformos*
. *Paskolos*
. *Bankinės paslaugos*

Iššūkiai

Auditavimas poreikis: išmaniųjų sutarčių atitikimas teisiniams dokumentams

„Orakulų“ problema: vykdymui reikalingų duomenų teisingumo užtikrinimas

Integracijos problema: integracija su kitomis susijusiomis duomenų saugyklomis

Valdymas

. *Skaidrūs rinkimai*
. *Tapatybių valdymas*
. *Registrų įrašų saugojimas*
. *Mokesčių administravimas*
. *Notarinės paslaugos*

LBChain

Benefits and value

- State-of-the-art technological testing platform based on Hyperledger Fabric / Corda
- Regulatory support from the Bank of Lithuania
- Technological support from leading blockchain integrators
- Cost-efficient and low-risk path to innovation

Examples of tested solutions

- KYC solution for AML compliance
- Cross-border payments
- Smart contract for factoring
- Mobile POS and payment card solution
- Unlisted share trading platform
- Crowdfunding platform
- Payment token

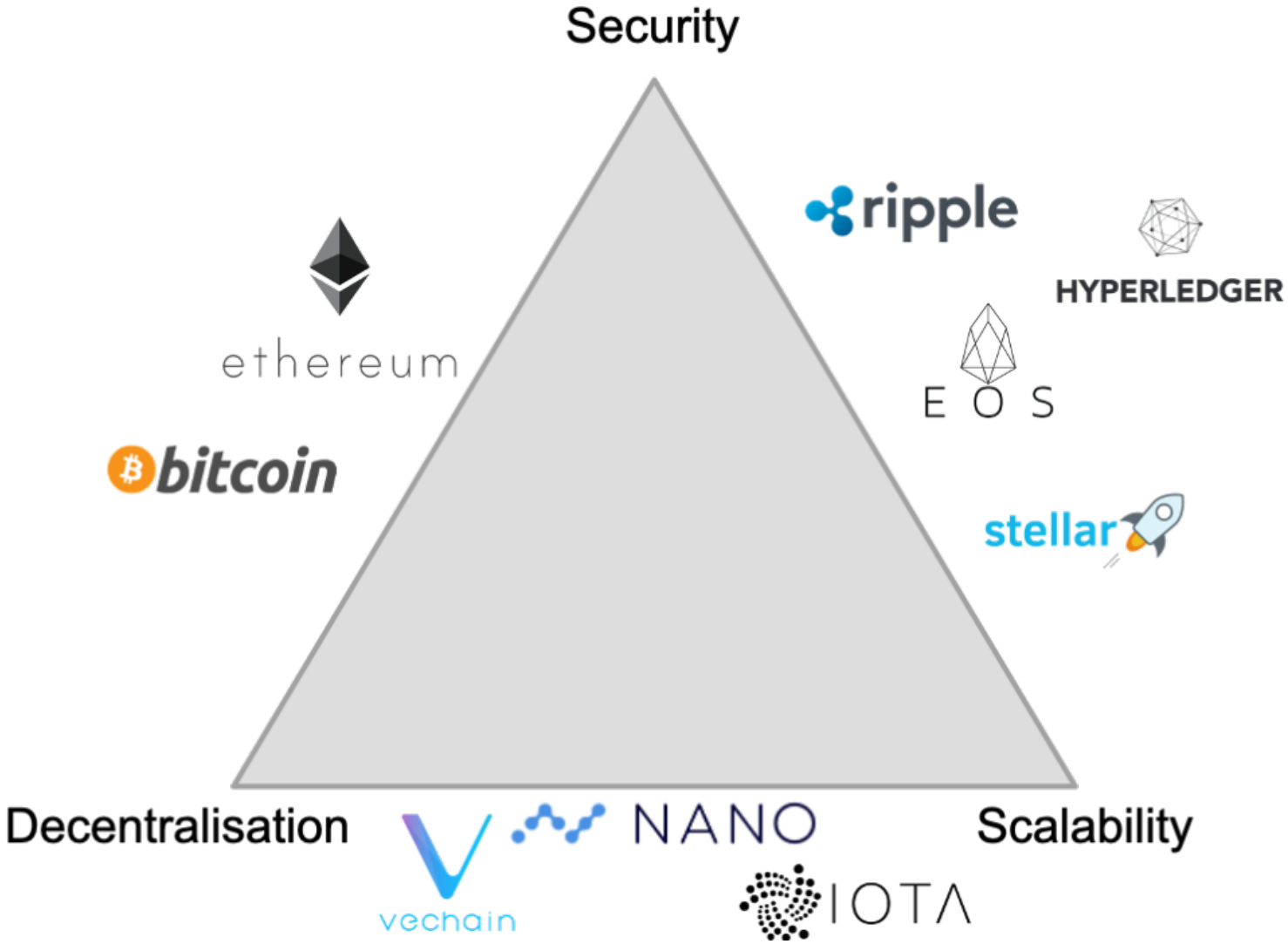
Award. LBChain has won the national round of „World Summit Awards" (WSA) in the category Government and citizen engagement.

WSA Lithuania Winner 2020

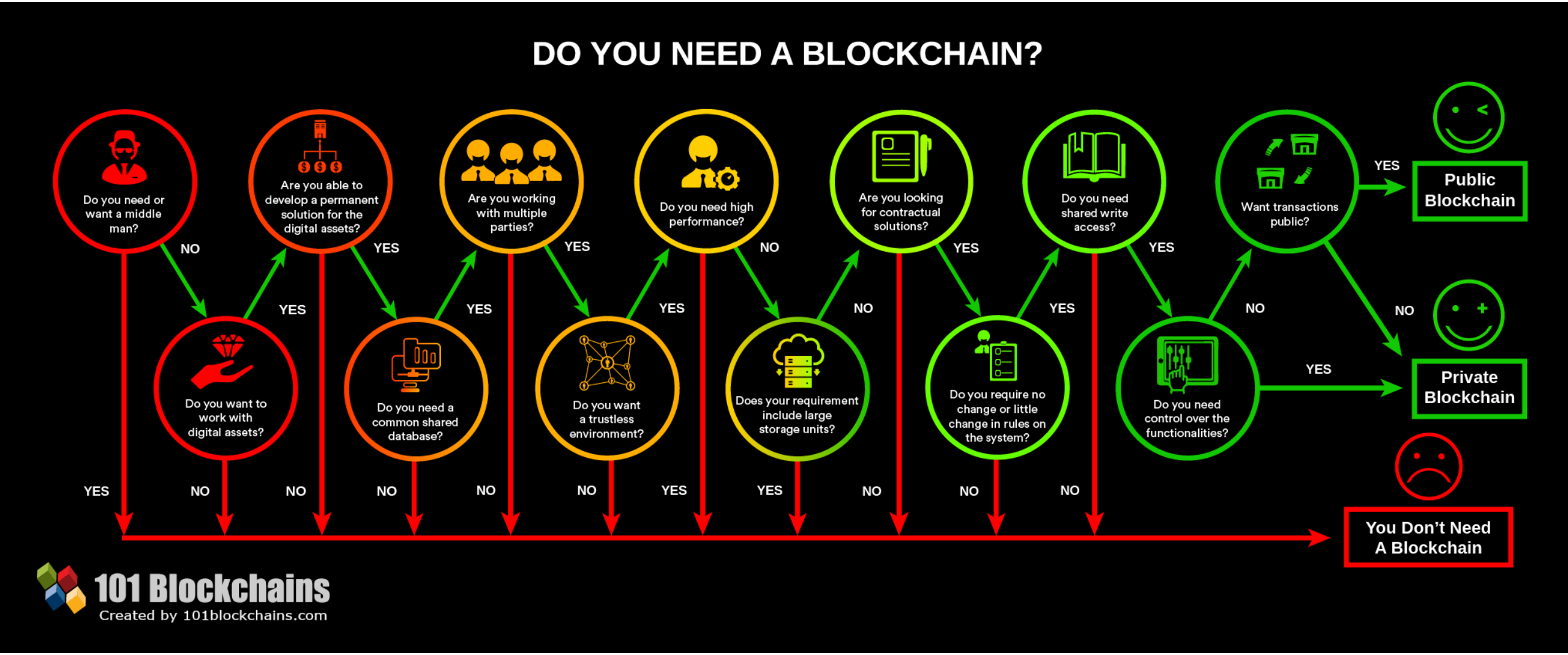
Plačiau: https://www.lb.lt/en/lbchain

Ką mokslininkai veikia šioje srityje?

Blockchain trilema:



Blockchain nėra „panacėja“



Klausimai?

Mano el. paštas:

remigijus.paulavicius@mif.vu.lt