



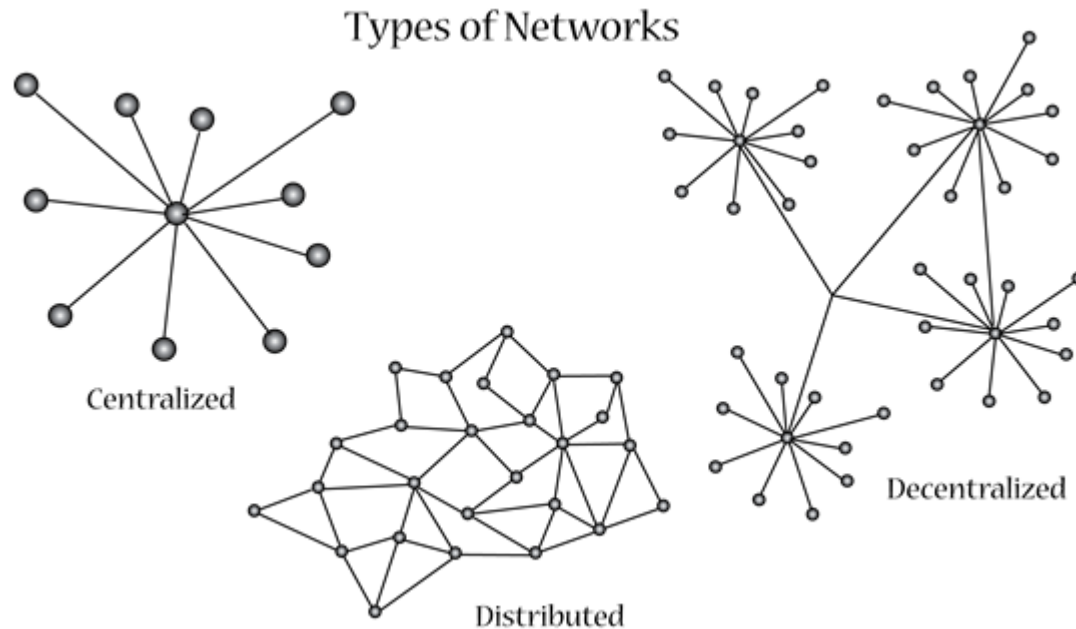
Blockchain, Bitcoin, Ethereum, Ripple és társai

Distributed ledger

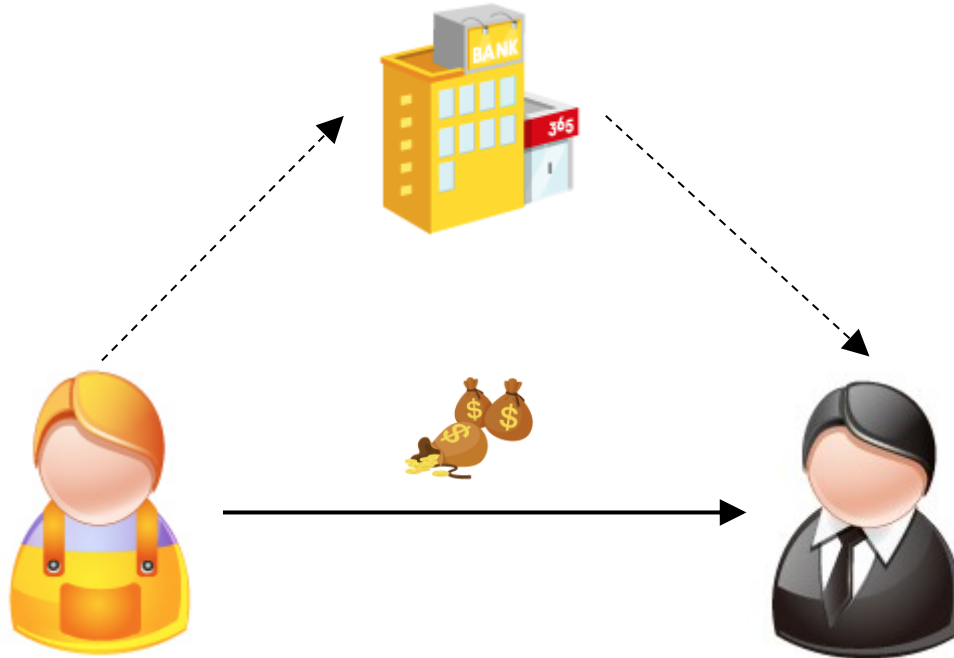
“Új típusú” fizetési módszerek

- Nincs központi autoritás
- Tranzakció validálása matematikai algoritmusokkal
- Nyilvános, követhető pénzmozgás
- “Fordított” információ
 - Hagyományos rendszerek:
Ismert számlatulajdonos, ismeretlen tranzakció
 - “Új típusú” rendszerek:
Ismeretlen számlatulajdonos, ismert tranzakció

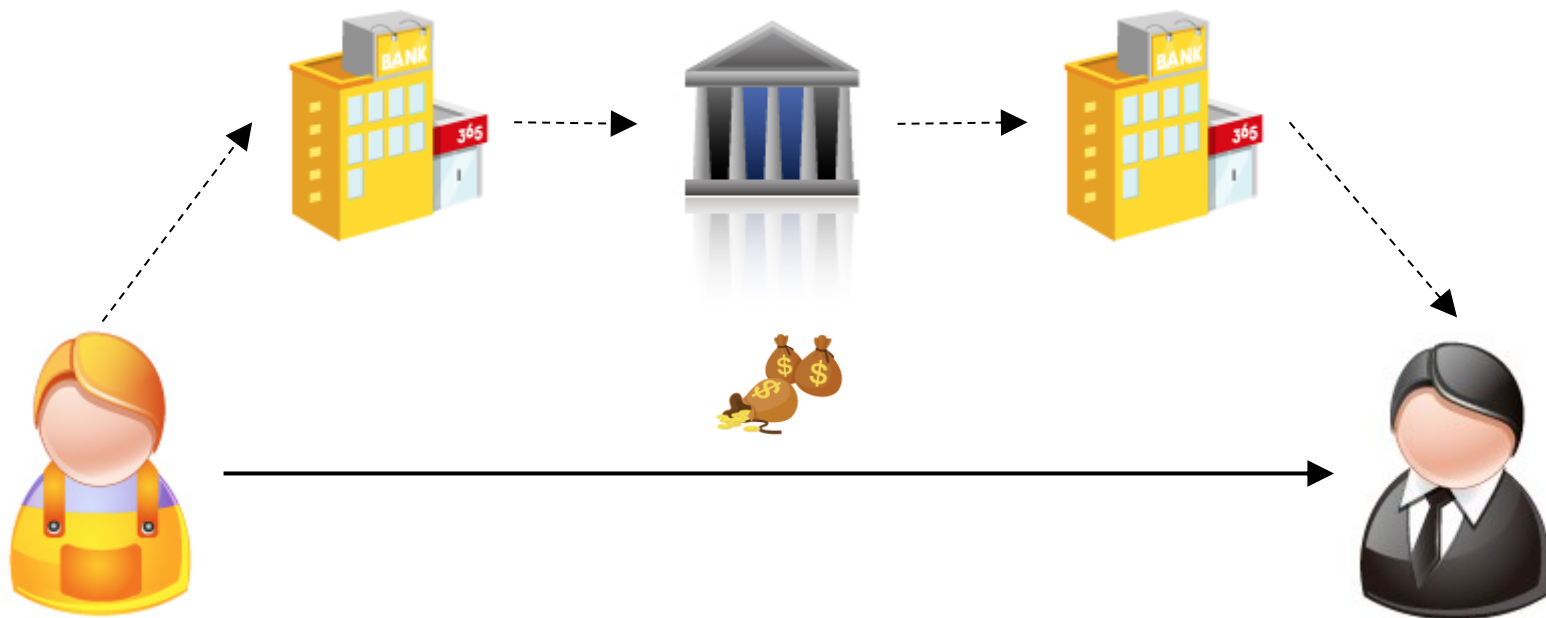
Elosztott -distributed



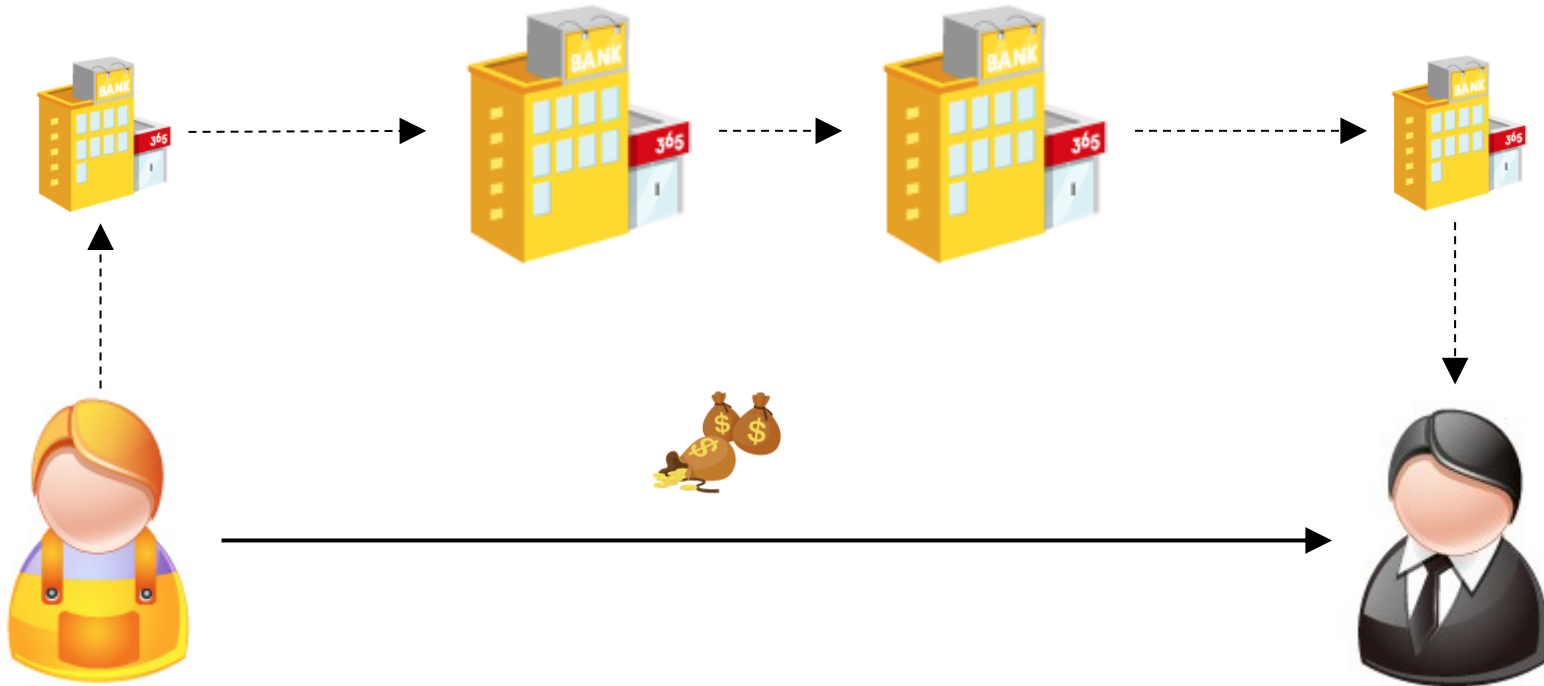
Bankon belüli átvzetés



Belföldi átutalás

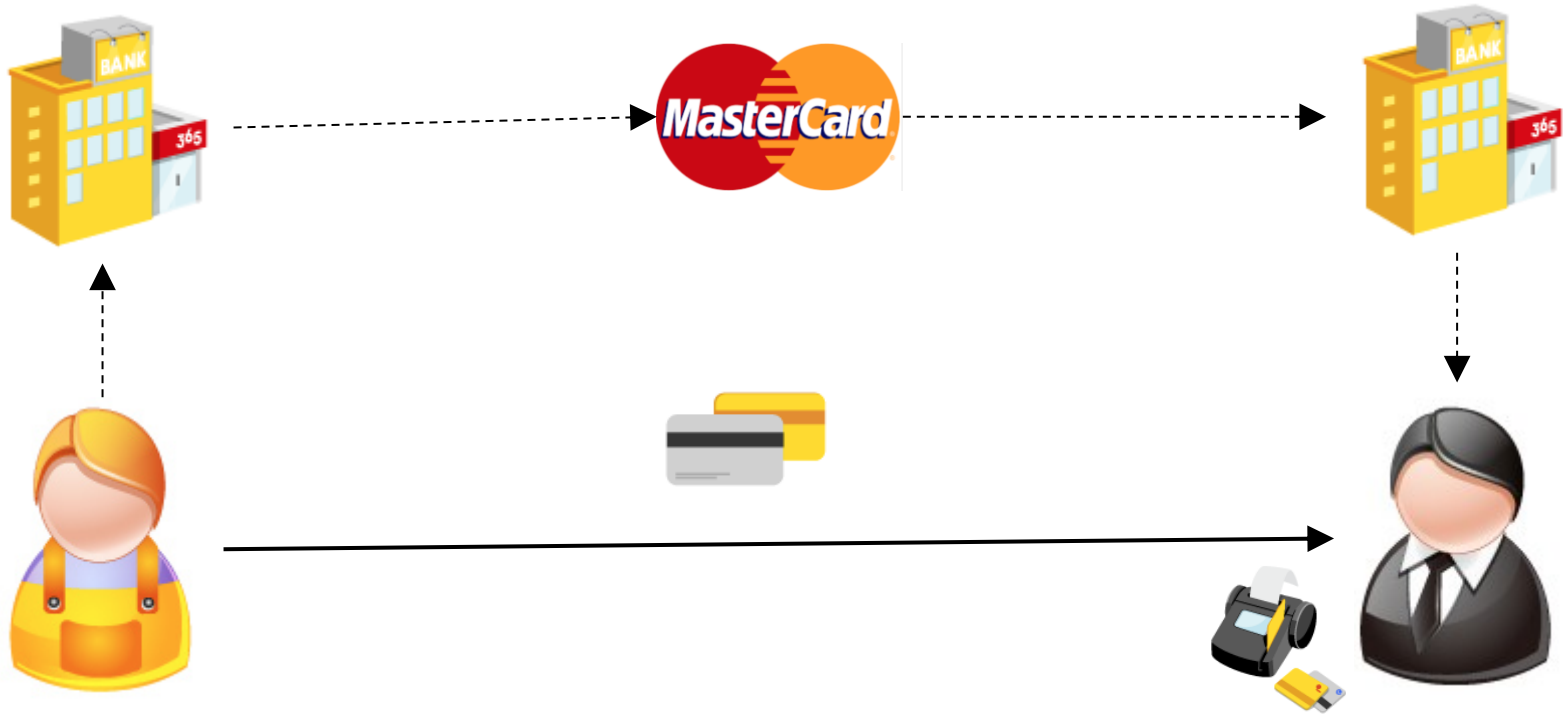


Nemzetközi átutalás

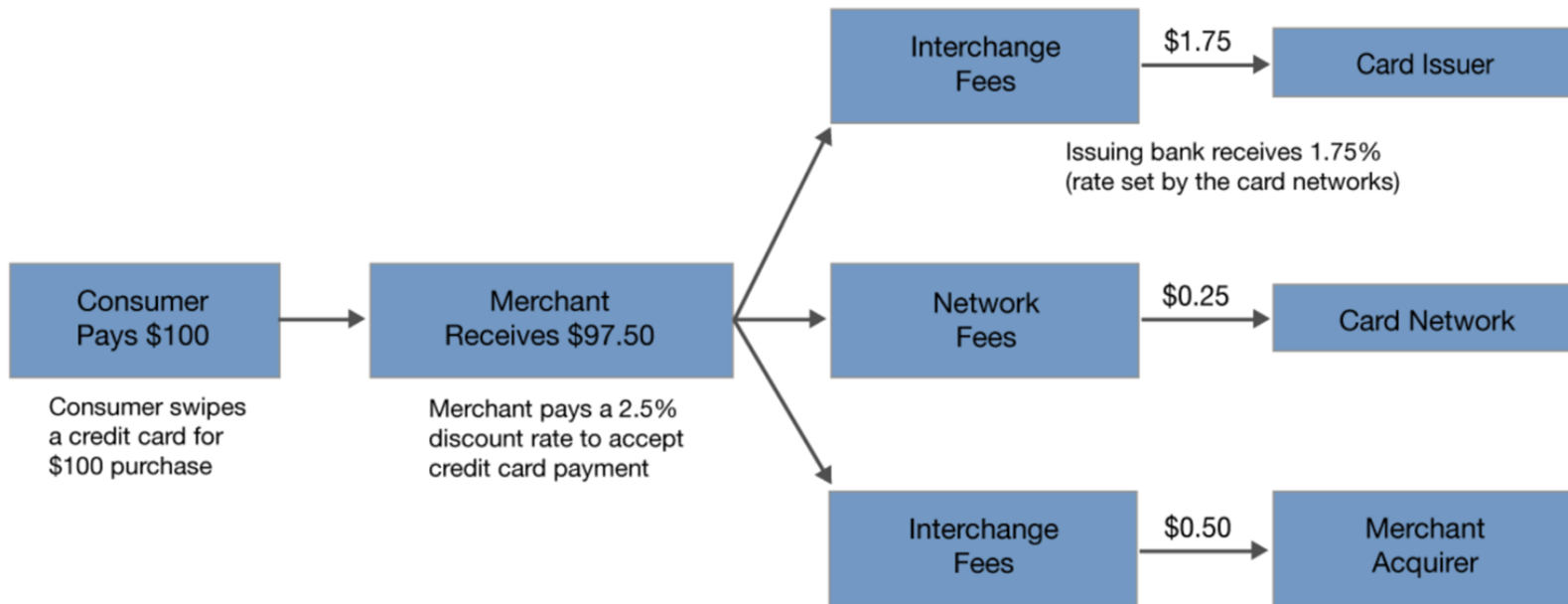


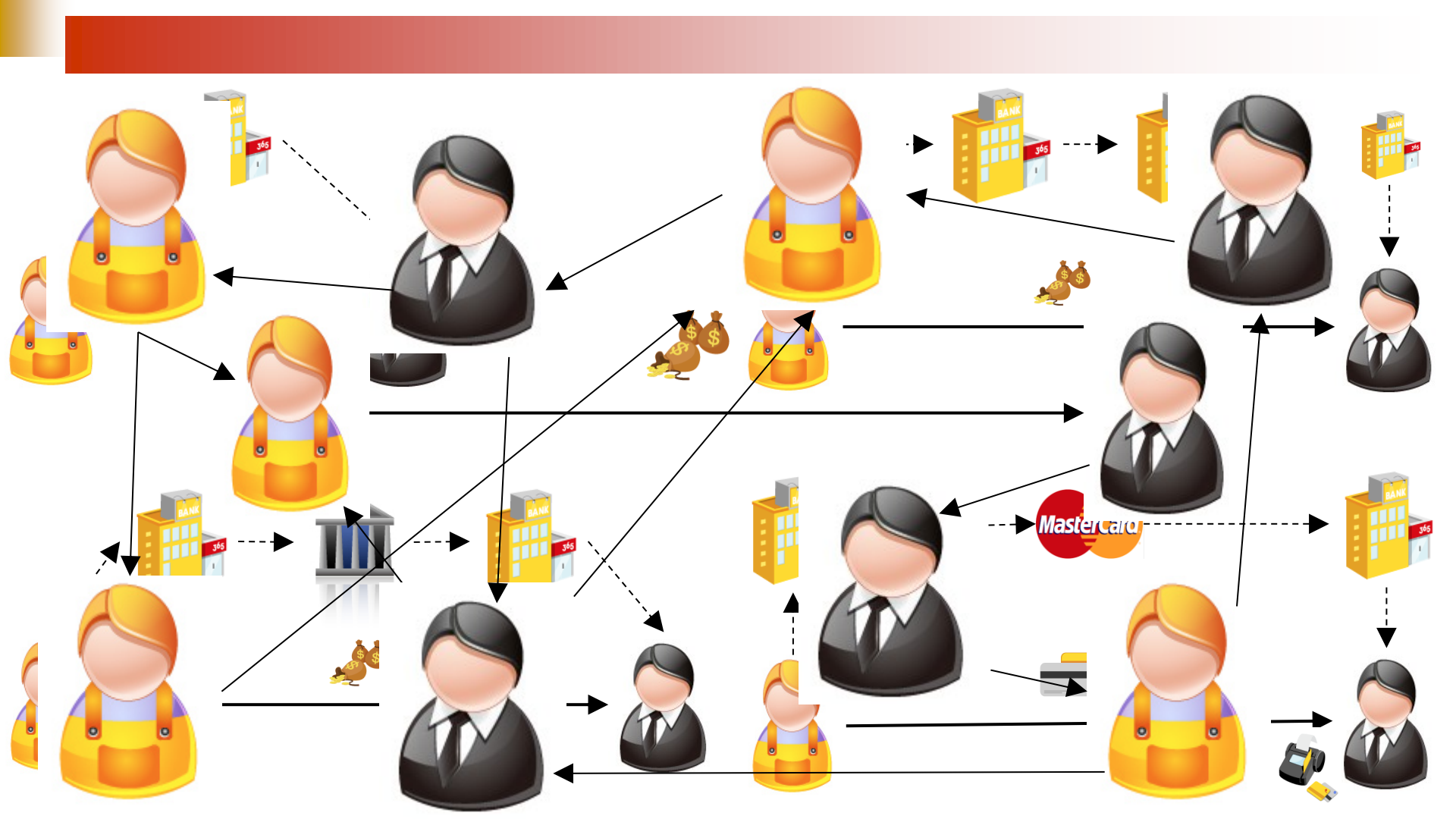


Kártyás fizetés



Kártyás fizetés költségei





Megoldandó problémák

Double spending

Centralizált hálózatoknál triviális

Bizalom a partnerben

Bizalom a pénzben (nem hamis)

Bitcoin



- 2009 Satoshi Nakamoto (?)
- Peer to peer hálózat
- Nyilvános elosztott könyvelés (public distributed ledger)
- Natív pénznem: BTC - decentralized virtual currency (U.S.Treasury)
- Digitális érték (digital asset)
- Visszavonhatatlan tranzakciók
- <https://bitcoin.org/bitcoin.pdf>

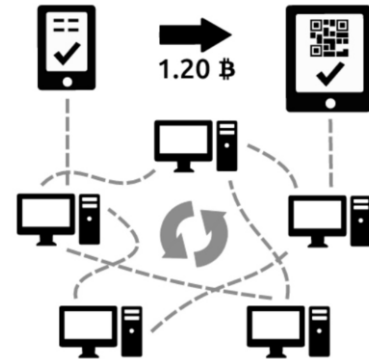
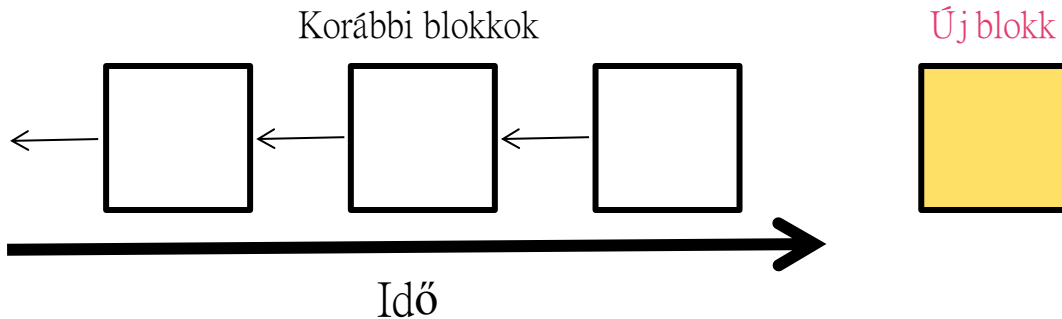
Az infrastruktúra (blockchain) és a pénz (BTC) nem válik el egymástól

Bitcoin eszközök

- [Bitcointicker.com](https://www.bitcointicker.com)
- [Bitcoinwisdom.com](https://www.bitcoinwisdom.com)
- [Btcpredictions.com](https://www.btcpredictions.com)
- [Btcbalance.net](https://www.btcbalance.net)
- [Blockchain.info](https://www.blockchain.info)
- [Bitaddress.org](https://www.bitaddress.org)
- [bit2factor.org](https://www.bit2factor.org)
- [Tradingview.com](https://www.tradingview.com)
- [thebitcoinpage.com](https://www.thebitcoinpage.com)
- [Coinmetrics.com](https://www.coinmetrics.com)
- [Coinmap.org](https://www.coinmap.org)
- [Fiatleak.com](https://www.fiatleak.com)
- [shinrai.com](https://www.shinrai.com)

Hogyan működik? (leegyszerűsítve)

1. Az új tranzakciók továbbításra kerülnek az összes szereplőhöz.
2. Minden "felhasználó" készít egy új blokkot a tranzakciókból (validál).



Hogyan működik? (leegyszerűsítve)

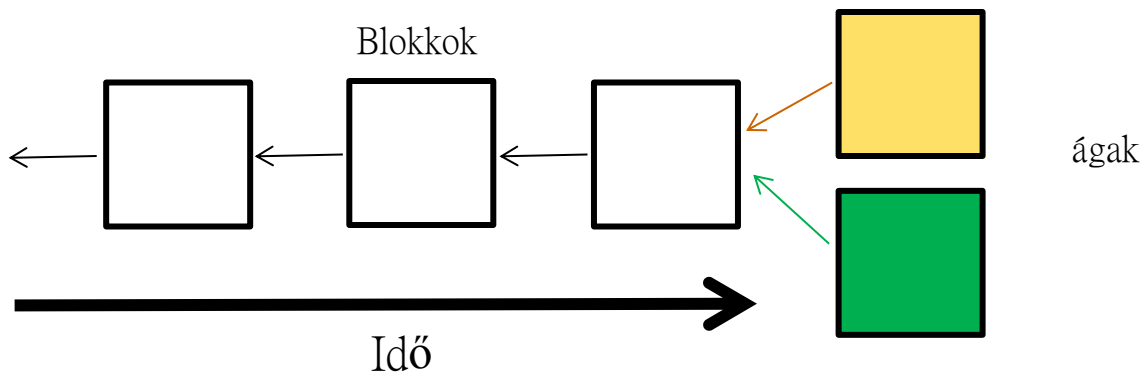
3. Minden felhasználó próbál új proof-of-work megoldást találni.

4. Ha talál egye megoldást továbbítja a hálózaton a többi felhasználónak.



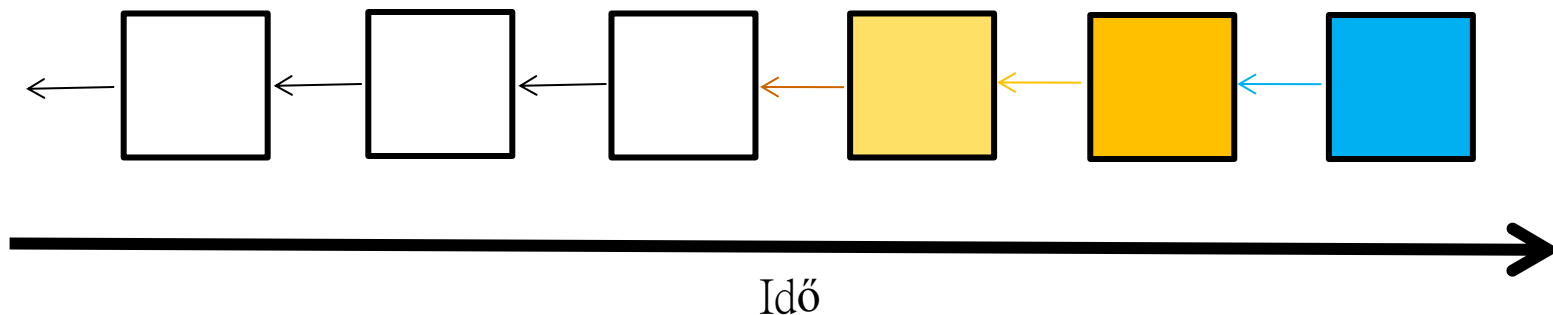
Hogyan működik? (leegyszerűsítve)

5. "Minden felhasználó elfogadja" a kapott új blokkot, ha minden tranzakció valid (digitálisan aláírt).
6. Ha két különböző blokkot is kap, akkor az elsőt tekinti érvényesnek, de a második ágat is eltárolja.



Hogyan működik? (leegyszerűsítve)

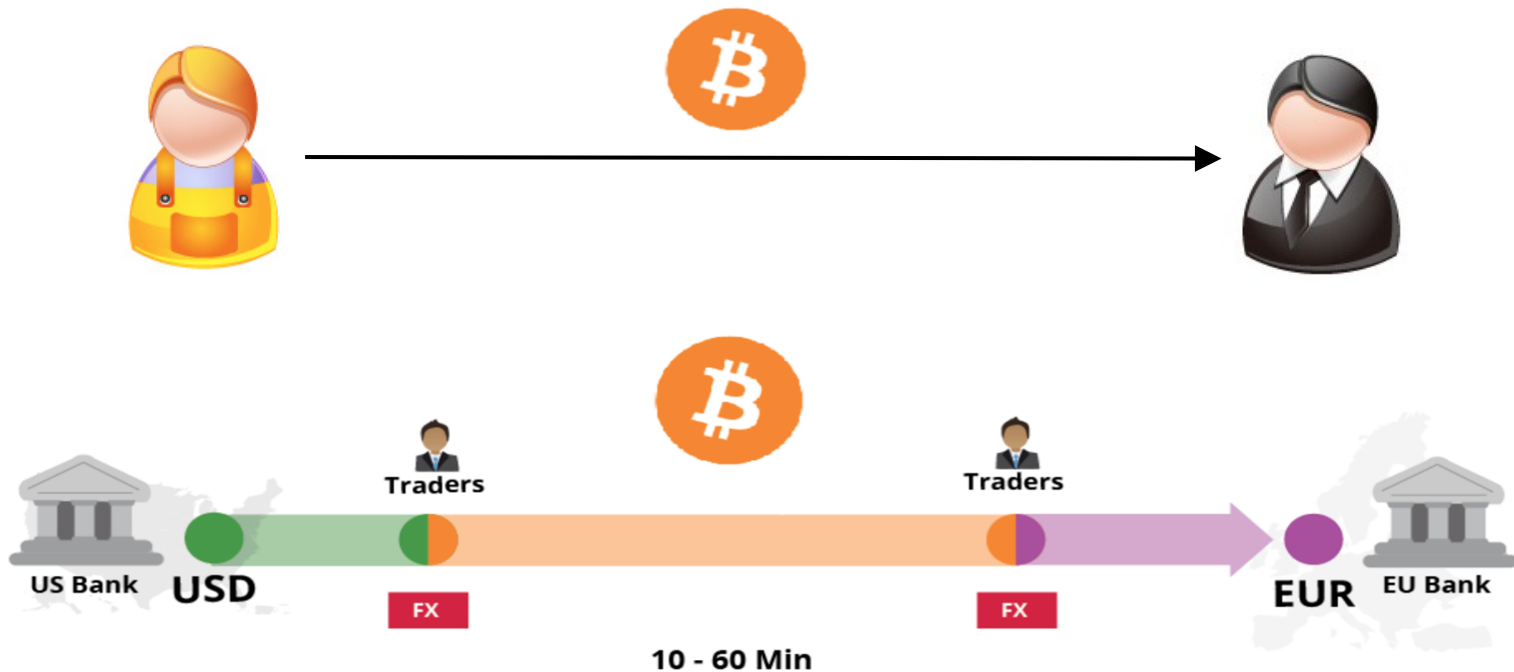
7. Ha új blokkot kap, a hosszabb ágat tekinti érvényesnek.
8. Mindig a legújabban elfogadott blokkhoz készítjük a következő blokkot. Ezért lesz blokklánc.



Bizánci generális problémája



Bitcoin tranzakció





De...

Natív pénznem - árfolyamkockázat,
volatilitás

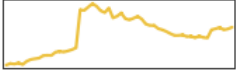
Bányászat - energia

Idealista (naív) gazdaságfilozófia

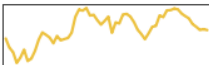
Alternatívák: <https://coinmarketcap.com/>

▲#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	 Bitcoin	\$ 9,083,846,908	\$ 575.17	15,793,188 BTC	\$ 167,418,000	3.74 %	
2	 Ethereum	\$ 852,917,223	\$ 10.32	82,640,611 ETH	\$ 41,770,000	8.02 %	
3	 Steem	\$ 229,491,429	\$ 2.20	104,322,347 STEEM	\$ 261,944	6.17 %	
4	 Ethereum Cla...	\$ 223,062,721	\$ 2.71	82,407,058 ETC	\$ 60,291,000	-1.22 %	
5	 Ripple	\$ 203,639,365	\$ 0.005728	35,550,137,658 XRP *	\$ 1,125,020	1.03 %	
6	 Litecoin	\$ 174,483,456	\$ 3.72	46,957,929 LTC	\$ 1,714,980	2.66 %	
7	 Dash	\$ 62,110,394	\$ 9.36	6,636,527 DASH	\$ 519,633	-0.22 %	
8	 NEM	\$ 49,487,580	\$ 0.005499	8,999,999,999 XEM *	\$ 420,194	7.15 %	
9	 MaidSafeCoin	\$ 34,360,087	\$ 0.075925	452,552,412 MAID *	\$ 455,187	10.05 %	
10	 Nxt	\$ 26,776,197	\$ 0.026803	998,999,999 NXT *	\$ 397,146	4.67 %	

2016.08.04.

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	 Bitcoin	\$ 9,314,760,855	\$ 589.37	15,804,660 BTC	\$ 86,523,700	0.06 %	
2	 Ethereum	\$ 1,021,765,684	\$ 12.33	82,839,373 ETH	\$ 33,066,800	4.83 %	
3	 Ripple	\$ 220,073,784	\$ 0.006189	35,557,883,251 XRP *	\$ 1,263,200	2.82 %	
4	 Steem	\$ 202,209,222	\$ 1.84	109,837,219 STEEM	\$ 367,228	-5.24 %	
5	 Litecoin	\$ 176,728,684	\$ 3.76	47,046,979 LTC	\$ 1,231,940	-0.16 %	
6	 Ethereum Cla...	\$ 151,295,252	\$ 1.83	82,820,276 ETC	\$ 22,812,600	-6.16 %	
7	 Dash	\$ 69,290,498	\$ 10.41	6,656,979 DASH	\$ 387,167	-1.07 %	
8	 NEM	\$ 53,233,470	\$ 0.005915	8,999,999,999 XEM *	\$ 754,229	18.36 %	
9	 MaidSafeCoin	\$ 41,688,811	\$ 0.092119	452,552,412 MAID *	\$ 1,271,130	0.92 %	
10	 Nxt	\$ 31,640,228	\$ 0.031672	998,999,999 NXT *	\$ 545,826	6.03 %	

2016.08.10.

#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	 Bitcoin	\$18,359,367,204	\$1129.61	16,252,837 BTC	\$672,909,000	4.26%	
2	 Ethereum	\$4,279,018,447	\$47.35	90,368,069 ETH	\$233,458,000	-6.94%	
3	 Ripple	\$1,678,228,687	\$0.044735	37,514,472,563 XRP *	\$230,873,000	16.32%	
4	 Dash	\$439,153,900	\$60.96	7,203,472 DASH	\$48,070,700	-11.43%	
5	 Litecoin	\$433,261,924	\$8.58	50,470,257 LTC	\$128,193,000	15.38%	
6	 Monero	\$285,275,122	\$20.05	14,229,321 XMR	\$7,435,320	-3.98%	
7	 Ethereum Classic	\$248,889,848	\$2.76	90,327,700 ETC	\$13,776,600	1.16%	
8	 NEM	\$181,306,800	\$0.020145	8,999,999,999 XEM *	\$3,013,850	14.16%	
9	 Augur	\$121,968,000	\$11.09	11,000,000 REP *	\$2,701,170	-9.59%	
10	 MaidSafeCoin	\$83,159,674	\$0.183757	452,552,412 MAID *	\$1,182,290	11.38%	



PROTECTION.

We are a fraud detection system, overlaying big data from closed sources like insurers and law enforcement.

BBC on Bitcoin & The Blockchain



FinTech

Digital & Mobile payments



Bitcoin & Cryptocurrency



Capital Markets & Investing



Banking & Corporate Finance



Big Data & Analytics



Financial platforms



Crowdfunding & peer-to-peer lending



Personal financial management



Blockchain technology





Blockchain

Blockchain - röviden

Csak hozzáfűzést
megengedő adatbázis, a
teljes hálózattal
megosztva*

Elosztott
főkönyv



Biztonság

Biztonságos, azonosított
és verifikált tranzakciók



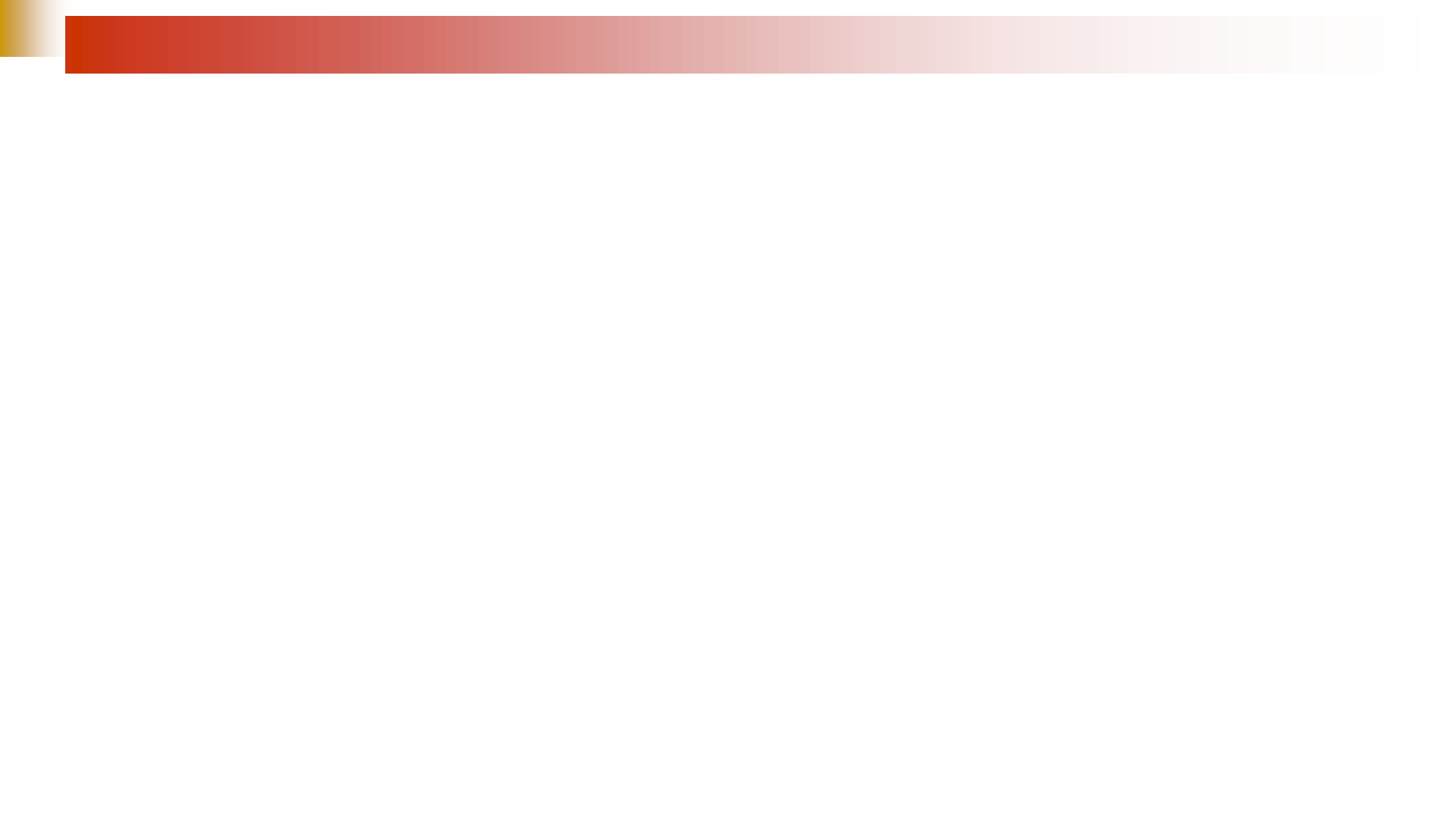
Minden szereplő elfogadja
a validált tranzakciókat.

Konszenzus



Megosztott
szerződések

Az üzleti tranzakciók
"adatbázis" oldalon
validáltak és
végrehajtnak.





ETHEREUM

- Több mint kriptovaluta (éter)
- Okos szerződések leírása
- ~15 másodpercenként keletkező blokkok
- Programozható - Solidity programozási nyelv
- Platformot biztosít blockchain alapú szolgáltatások készítésére

JavaScript példa program

```
var ethbase = require('blockapps-js').ethbase
var Transaction = ethbase.Transaction;
var Int = ethbase.Int;
var ethValue = ethbase.Units.ethValue;

var addressTo = "0x4eF003330a50dE8f63250FBA7e2Bc74fb4A43d14";
var privkeyFrom = "privatkulcs";

var valueTX = Transaction({"value" : ethValue(1).in("ether")});

valueTX.send(privkeyFrom, addressTo).then(function(txResult) {
});
```

Ebatka utalás

Ethereum Wallet

Ethereum WalletAccountsEditViewDevelopWindow

WALLETS

SEND

13 peers | 2,354,600 | 7s since last block

CONTRACTS

BALANCE

1.82 ETHER

Send funds

FROM

 Main account (Etherebase) - 1.82 ETHER

TO

 0x27020a0ff6214BBd92C0318b62F67CA7866D4e02

AMOUNT

100

☐ Send everything

You want to send **100 ETHER**.

SHOW MORE OPTIONS

SELECT FEE

0.000798882080136 ETHER

CHEAPER

FASTER

TOTAL

100.000798882080136 ETHER

This is the most amount of money that might be used to process this transaction. Your transaction will be mined **probably within 30 seconds**.

Partnerek

- Microsoft Azure
- Barclays, BMO Financial Group, Credit Suisse, Commonwealth Bank of Australia, HSBC, Natixis, Royal Bank of Scotland, TD Bank, UBS, UniCredit, Wells Fargo, stb.



peers | 854,560 blocks left | 22%

BALANCE
0.00 **ETHER**

Accounts Overview

ACCOUNTS

Accounts are password protected keys that can hold ether, secure ethereum-based tokens or coins and control contracts. Accounts can't display incoming transactions.

[ACCOUNT 1](#)

0.00 ether

0xa8A00FB318c54f52B...

[ACCOUNT 2](#)

0.00 ether

0xEF341363616BdCF5...

[ACCOUNT 3](#)

0.00 ether

0xBAE8BB0E42b21E14...

[MAIN ACCOUNT \(ETHERBASE\)](#)

0.00 ether

0x4eF003330a50dE8f63250FBA7e2Bc74fb4A43d14

[ADD ACCOUNT](#)

WALLET CONTRACTS

Once you have more than 1 ether you can create more sophisticated contracts. Wallets are one type of basic smart contract, that allows your funds to be controlled by multiple accounts and have an optional daily limit on withdrawals, to increase security. To create your own custom contracts go to the *Contracts* tab.

Saját kriptopénz (szerződés, részvény) kibocsátása

SOLIDITY CONTRACT SOURCE CODE

CONTRACT BYTE CODE

```
1 contract tokenRecipient { function receiveApproval(address _from, uint256 _value, address _token, by
2
3 contract ebatka {
4     /* Public variables of the token */
5     string public standard = 'Token 0.1';
6     string public name;
7     string public symbol;
8     uint8 public decimals;
9     uint256 public totalSupply;
10
11     /* This creates an array with all balances */
12     mapping (address => uint256) public balanceOf;
13     mapping (address => mapping (address => uint256)) public allowance;
14
15     /* This generates a public event on the blockchain that will notify clients */
16     event Transfer(address indexed from, address indexed to, uint256 value);
17
18     /* Initializes contract with initial supply tokens to the creator of the contract */
19     function ebatka(
20         uint256 initialSupply,
21         string tokenName,
22         uint8 decimalUnits,
23         string tokenSymbol
24     ) {
25         balanceOf[msg.sender] = initialSupply; // Give the creator all initial tokens
26         totalSupply = initialSupply; // Update total supply
27         name = tokenName; // Set the name for display purposes
28         symbol = tokenSymbol; // Set the symbol for display purposes
29         decimals = decimalUnits; // Amount of decimals for display purposes
30
```

SELECT CONTRACT TO DEPLOY

ebatka

CONSTRUCTOR PARAMETERS

Initial supply - 256 bits unsigned integer

1000000

Token name - string

ebatka

Decimal units - 8 bits unsigned integer

2

Token symbol - string

XEB



Egy másik lehetséges út: Ripple

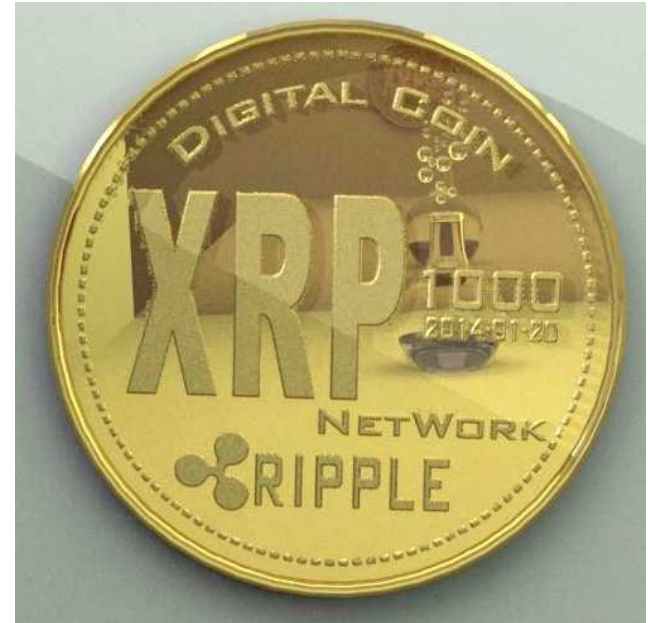
- Szoros gazdasági integráció
 - A bankok mint partnerek
 - Pénzügyi szabályozások figyelembe vétele
- Pénznem független (XRP + IOU)
- Valós idejű fizetés (realtime payment)
- Osztott közös könyvelés (shared common ledger)
- Konszenzus alapú tranzakció validálás
- Nyílt platform és forráskód





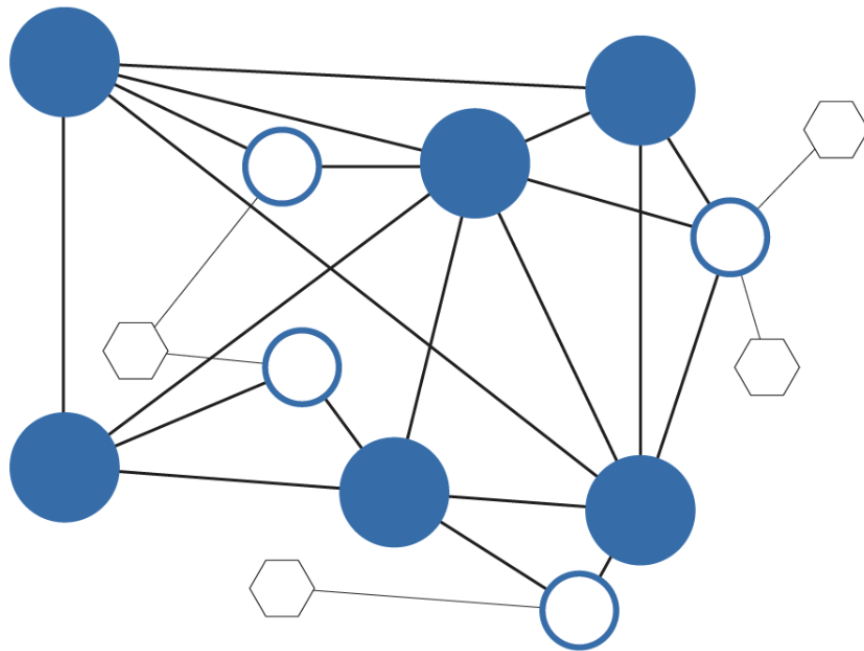
XRP

- A hálózat natív pénzneme
- Már létrejött a teljes állomány, új XRP nem keletkezik
- Cél:
 - ☐ Hálózati biztonság (spam csökkentése)
 - ☐ Bridge currency
- Árfolyam: 2,30 XRP/HUF (120 USD/XRP)
- Költségek
 - ☐ Számla: 20 XRP
 - ☐ Tranzakciós díj: 0,01 XRP
 - ☐ Trust line: 5 XRP

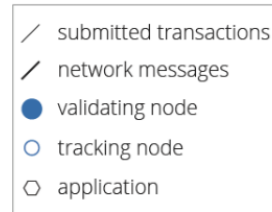




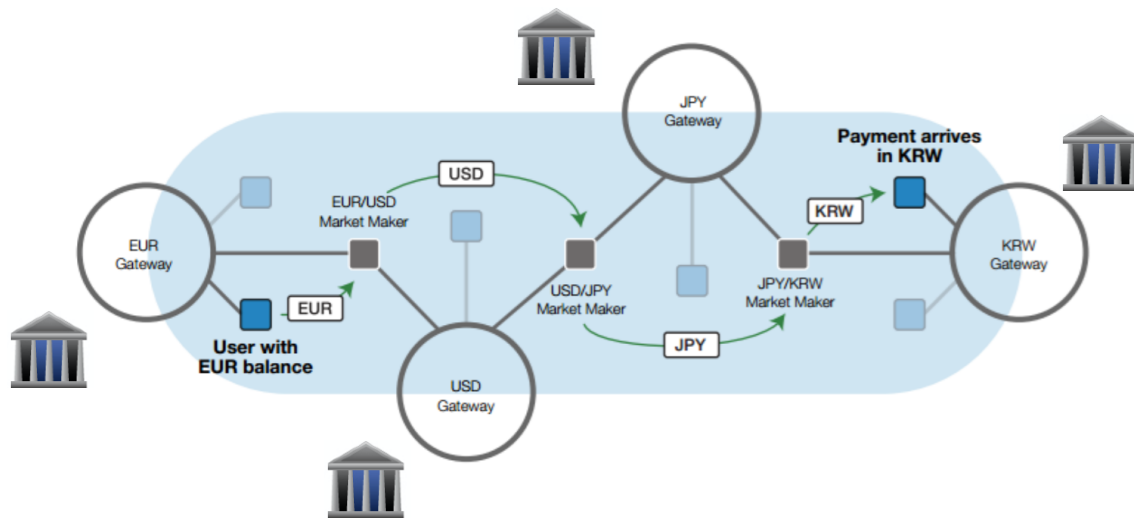
Hálózati architektúra



Konszenzuson alapuló tranzakció
validáció
Ledgerek zárása 2-5 mp-enként

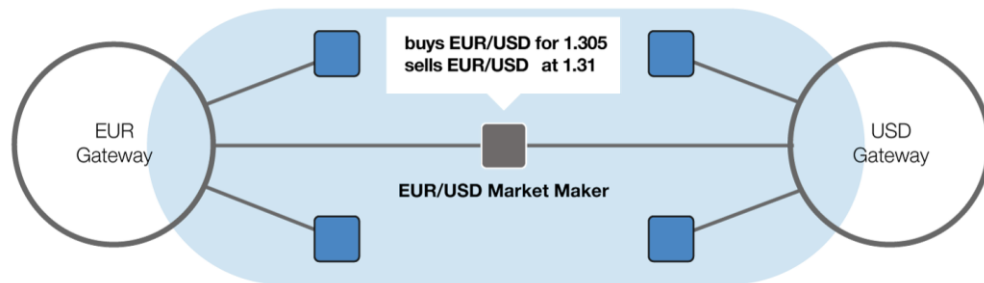


Szereplők

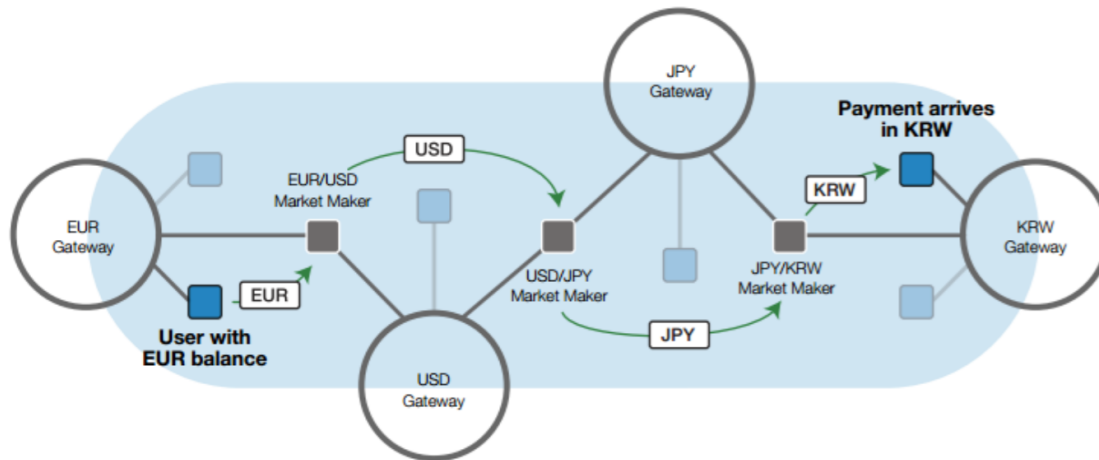


- Bank
- Gateway
- Market Maker
- User

Konverziós fizetés (pathfinding)

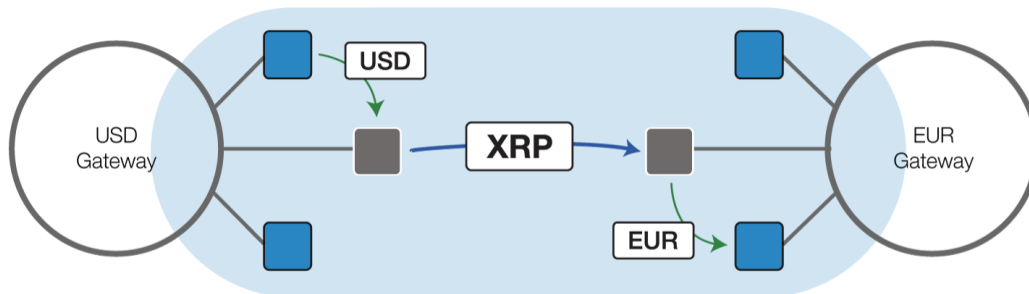
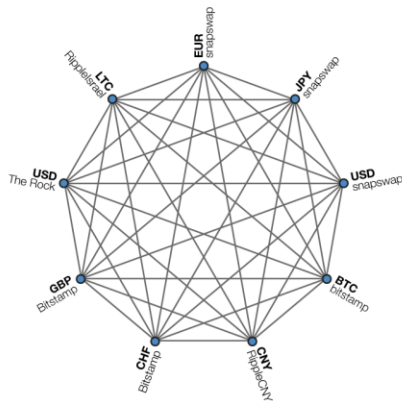


- Automatikus útkeresés
- Atomi tranzakció





Konverzió XRP-vel





Hozzáférés

- Websocket API
- JSON-RPC API
- Command line
- RippleAPI - javascript library
- Github - rippled