

BlockChain

Vojtěch Kloda

Obsah

- Úvod
- Jak funguje
- Aplikace
- Pro a proti

Úvod

- Distribuovaná databáze
 - Decentralizované sdílení dat (DLT)
 - Odstranění zprostředkovatelů
 - Pravda je sdílená, nikoli diktovaná autoritou
- Bezpečnost dat
 - Data nelze jednoduše zfalšovat
 - Data nelze zpětně měnit
- Rovnocennost
 - Všichni účastníci mají stejné možnosti
- Rychlost
 - Transakce probíhají okamžitě

Jak funguje (PoW) - koncept

- Všechny transakce se rozesílají do sítě
- Mineři vytváří z transakcí bloky
- Bloky se zapojují do řetězce (block chain)
- Každý účastník má kopii řetězce
- Řetězec slouží jako historie všech transakcí

Jak funguje - tvorba transakce

- Uživatel vytvoří transakci
- Transakce je podepsána majiteli účtu
- Transakce je rozeslána do sítě

Jak funguje (PoW) - tvorba bloku

- Mineři odposlouchávají transakce
 - Z určitého množství transakcí a odkazu na předchozí blok v řetězci vytvoří nový blok
 - K novému bloku se snaží vygenerovat určitý hash (Proof of Work)
 - První miner, který vygeneroval správný hash, rozesílá nový blok do sítě a získá odměnu
-
- PoW slouží jako opatření proti tvorbě podvodných bloků

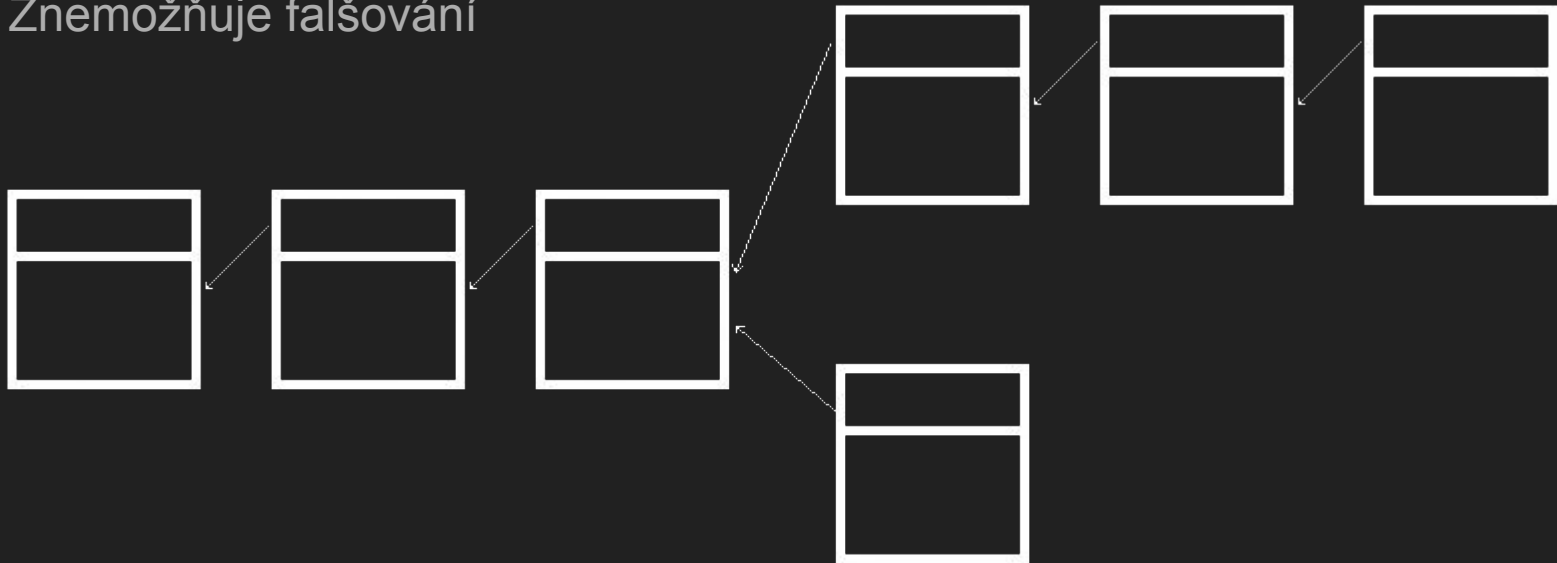
Link to previous Block

Transactions

Proof of Work

Jak funguje - přidání do řetězce

- Uživatelé si přidávají nové bloky do svého řetězce
- V případě větvení se preferuje delší větev
- Uživatelé i mineři mají motivaci pokračovat v nejdelší větvi
- Znemožňuje falšování



Aplikace

- DeFi
 - Odstranění prostředníků a regulací
- Kryptoměny
- NFTs
- Smart Contracts
 - Program, který se automaticky vyhodnocuje v závislosti na podmínkách smlouvy
 - Zaručené vykonání a transparentnost kódu

Smart Contracts - příklady

[Introduction to smart contracts | ethereum.org](#)

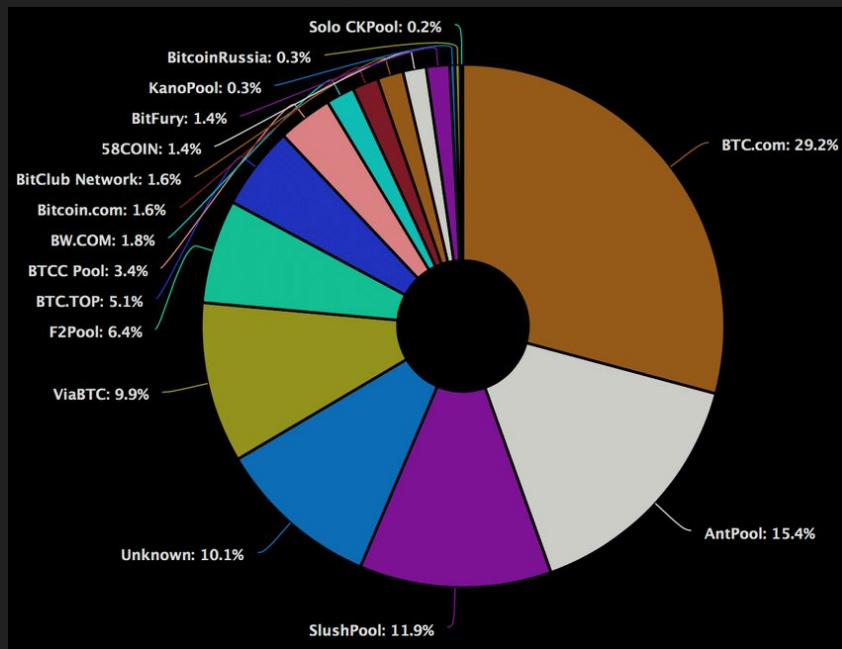
[Get started with Marlowe | cardano.org](#)

Pro a proti

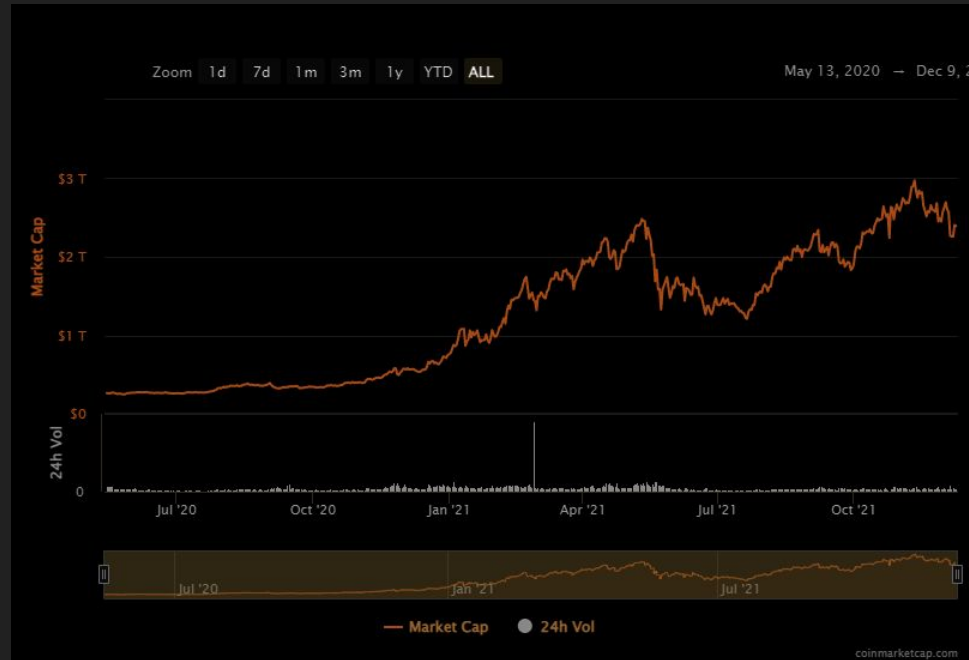
- Decentralizace
 - Transakce nemusí být schváleny bankovními systémy
 - Transakce nemusí být závislé na legislativě
 - Hodnota tokenů není přímo závislá na inflaci (Venezuela, Afrika)
- Rychlejší a levnější vyřízení transakce
- Nutnost uchovávat klíče
- Spotřeba energie
 - Možné řešení pomocí PoS (Proof of Stake)

Pro a proti - Bitcoin pools

- Bezpečnost
 - Transakce nelze zpětně upravovat, jsou navždy viditelné
 - Transparentnost
 - Problém 51 %



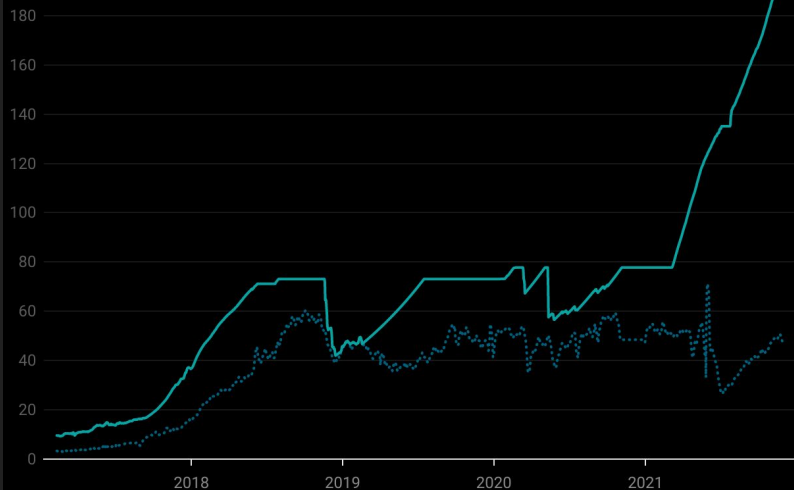
Bitcoin - market cap



Bitcoin - spotřeba energie

Bitcoin Energy Consumption

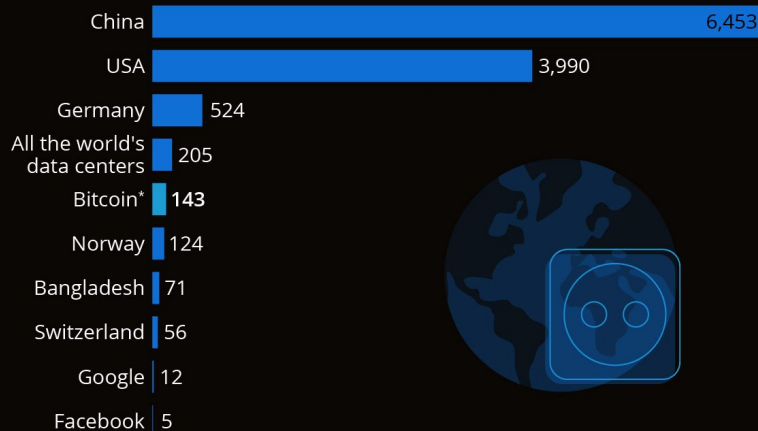
— Estimated TWh per Year - - - Minimum TWh per Year



Source: BitcoinEnergyConsumption.com • Created with Datawrapper

Bitcoin Devours More Electricity Than Many Countries

Annual electricity consumption in comparison (in TWh)



* Bitcoin figure as of May 05, 2021. Country values are from 2019.
Sources: Cambridge Centre for Alternative Finance, Visual Capitalist



statista

Zdroje

<https://www.investopedia.com/terms/b/blockchain.asp>

<https://www.investopedia.com/terms/s/smart-contracts.asp>

<https://www.investopedia.com/decentralized-finance-defi-5113835>

<https://www.sec.gov/news/statement/crenshaw-defi-20211109>

<https://ethereum.org/en/developers/docs/smart-contracts/anatomy/>

<https://developers.cardano.org/docs/smart-contracts/marlowe>

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

Zdroje

<https://www.statista.com/chart/18632/estimated-annual-electricity-consumption-of-bitcoin/>

<https://www.ncsl.org/research/financial-services-and-commerce/blockchain-2021-legislation.aspx>

<https://101blockchains.com/pros-and-cons-of-blockchain/>

https://www.researchgate.net/figure/Bitcoin-Mining-Distribution-3_fig3_328150068

<https://www.youtube.com/watch?v=bBC-nXj3Ng4>

https://www.youtube.com/watch?v=M3EFi_POhps

<https://www.youtube.com/watch?v=ZE2HxTmxfrl>