**Bitcoin Cash Hard Fork**

Bitcoin je digitální měna, založená v roce 2009 skupinou nebo jedincem pod pseudonymem „Satoshi Nakamoto“. Design Bitcoinu byl příslibem nízkonákladové nezávislé a anonymní měny, založené na principu přímého převodu peněžních prostředků mezi dvěma obchodujícími osobami, bez potřeby prostředníka. Tyto převody peněžních prostředků přitom měly být kolektivně všemi uživateli v rámci P2P sítě.[[1]](#footnote-1)

Dnes se jedná o nejrozšířenější a nejužívanější digitální měnu na světě, zabírající největší část celosvětového trhu se všemi existujícími digitálními měnami. Okolo ekosystému Bitcoinu je také postavena celá řada podnikatelů, burz, platform, bank a jiných účastníků trhu.[[2]](#footnote-2)

1. 8. 2017 se však Bitcoin rozdělil na dvě samostatné digitální měny, a sice klasický Bitcoin (BTC) a Bitcoin Cash (BCH).[[3]](#footnote-3) Jaké byly příčiny tohoto rozdělení? Bylo rozdělení jedinou variantou řešení těchto příčin? A jaké jsou důsledky tohoto rozdělení? To jsou otázky, kterými se budu v této práci zabývat.

Hlavní příčina rozdělení této digitální měny dlí v opatření, které Satoshi Nakamoto zavedl/i v roce 2010. Bitcoin totiž funguje na principu tzv. blockchainu, tedy řetězci bloků, přičemž každý blok obsahuje veškeré transakce, které v síti Bitcoinu proběhly za určitou dobu, a tento blok je následně připojen na konec blockchainu tak, aby každý mohl sledovat historii jednotlivých transakcí.[[4]](#footnote-4)

Každý blok je zašifrován pomocí hashovací funkce a je k němu přidána časová známka a tzv. kryptografická nonce, což je v podstatě důkaz o tom, že uvedené transakce byly skutečně ověřeny tzv. minery, a že se tudíž nejedná např. o podvodné jednání. Kryptografická nonce je totiž číslo, které (velmi zjednodušeně) umožňuje splnit jednotlivým blokům podmínky proto, aby mohly být umístěny do blockchainu, a které je velmi jednoduše ověřitelné, ovšem extrémně obtížné ke generaci.[[5]](#footnote-5) Obtížnost spočívá v tom, že číslo, které vznikne po finálním hashování, musí být numericky nižší, než kolik ukládá obtížnostní limit. A přirozeně, čím nižší počet číslic může takové číslo obsahovat, tím menší počet takových čísel bude existovat.

A zde se nachází zdroj problému. Objevit jeden blok je totiž tak obtížné, že to zabere přibližně 10 minut. V roce 2010 přitom byl, jako prevence zahlcení blockchainu obrovským množstvím miniaturních transakcí, které by museli mineři ověřovat, zaveden limit na velikost jednoho bloku na 1 MB. V té době byl takový limit v pořádku, neboť samotných transakcí v té době nebylo tolik, ale s postupem času tyto 1 MB bloky přestaly stačit, což má v současnosti za následek hned dva problémy. Jednak objevené bloky přestávají dostačovat množství transakcí, které jsou v síti Bitcoin prováděny, a uživatelé tak musejí čekat na ověření transakcí i celé hodiny. Zároveň jsou s Bitcoinovými transakcemi spojovány mnohem větší poplatky, neboť při takovém objemu transakcí a pouze limitovanému množství těch, které lze zařadit do bloku, si mineři vyberou pochopitelně ty transakce, které pro ně přináší větší zisk.[[6]](#footnote-6)

Tento problém vedl k rozdělení Bitcoinové komunity na dva tábory. Jeden tábor chtěl Bitcoinový blockchain optimalizovat zavedením funkce Segregated Witness (z bloku by byla odstraněna podpisová data, která tvoří velkou část samotného transakčního kódu) a zvýšením kapacity jednoho bloku.[[7]](#footnote-7) Druhý tábor byl odpůrcem tohoto řešení z důvodu hrozby centralizace moci v rámci sítě.[[8]](#footnote-8)

Z tohoto důvodu se po letech dohadování vyčlenila z komunity Bitcoin skupina uživatelů, která založila vlastní digitalní měnu Bitcoin Cash, jejíž bloky jsou na rozdíl od klasického Bitcoinu limitovány na 8 MB, a který nepoužívá k optimalizaci kódů transakcí funkci Segregated Witness.[[9]](#footnote-9) Důležité je také zmínit, že vzhledem k duplicitě blockchainu obou zmiňovaných měn v době jejich oddělení získal každý vlastník Bitcoinů stejné množství Bitcoin Cash, které uživatelům vývojáři Bitcoin Cash poskytli zadarmo.

V první řadě je třeba hodnotit survivibilitu Bitcoin cash. Ten se totiž zejména v počátečních měsících potýkal s celou řadou problémů. Prvním problémem je vůbec podpora Bitcoin Cash burzami, platformami, bankami atd. Například jedna z největších burz s kryptoměnami, CoinBase, se rozhodla, že Bitcoin Cash podporovat nebude a nabádala své uživatele ke zbavení se této měny.[[10]](#footnote-10) Druhým problémem je samotný fakt, že uživatelé dostali množství Bitcoin Cash zadarmo. Tím pádem vývojáři Bitcoin Cash vytvořili hodnotu z ničeho, čímž umožnili jeho uživatelům zbavovat se Bitcoin Cash za velmi nízkou cenu, neboť při žádné investici byli schopni generovat zisk.

Ačkoliv však byla situaci pro Bitcoin Cash v předchozích měsících velmi vážná, v listopadu 2017 začala cena Bitcoin Cash opět stoupat a to tak, že od konce října 2017, kdy se hodnota Bitcoin Cash pohybovala okolo 400 USD, překročila hodnota Bitcoin Cash hranici 1 000 USD a nad touto hranicí se stále drží. Jednou z možností tohoto růstu je zejména technologie těžby Bitcoin Cash. Tato technologie funguje na principu, že pokud se za určitý časový úsek nevytěží určité množství bloků, obtížnost těžby se procentuálně sníží (nejde tedy o časovou fixaci jako u klasického Bitoinu).[[11]](#footnote-11) Závěrem tak lze shrnout, že tzv. hard fork Bitcoinu byl nakonec úspěšnou iniciativou, neboť je dnes kombinovaná hodnota klasického Bitcoinu a Bitcoin Cash vyšší, že byla hodnota samotného Bitcoinu původně.

IV.

1. BENNINGTON, Ash. $700 and Rising: What's Driving the Price of Bitcoin Cash? [online] CoinDesk, publikováno 18. 7. 2017 [cit. 20. 11. 2017]. Dostupný z: <https://www.coindesk.com/700-rising-whats-driving-price-bitcoin-cash/>
2. HERTIG, Alyssa. Bitcoin Cash: Why It's Forking the Blockchain And What That Means. [online] CoinDesk, publikováno 26. 7. 2017 [cit. 20. 11. 2017]. Dostupný z <https://www.coindesk.com/coindesk-explainer-bitcoin-cash-forking-blockchain/>
3. KARAME, Ghassan a Elli ANDROULAKI. *Bitcoin and blockchain security*. Boston: Artech House, 2016. ISBN 1630810134
4. MOW, Samson. The Bitcoin Cash Fork Was a Dangerous Trick. *Fortune.Com*. [online] IN. EBSCOhost, publikováno 7. 8. 2017 [cit. 20. 11. 2017]. Dostupné z: search.ebscohost.com/login.aspx?direct=true&db=bth&AN=124514491&lang=cs.
5. SMITH, Jake. The Bitcoin Cash Hard Fork Will Show Us Which Coin Is Best. *Fortune.Com* [online] IN. EBSCOhost, publikováno 11. 8. 2017, s. 14 [cit. 20. 11. 2017]. Dostupný z: search.ebscohost.com/login.aspx?direct=true&db=bth&AN=124579398&lang=cs.
6. The Economist Group Limited. The great chain of being sure about things. [online] The Economist. publikováno 31. 10. 2015 [cit. 20. 11. 2017]. Dostupný z: <https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable>

1. KARAME, Ghassan a Elli ANDROULAKI. *Bitcoin and blockchain security*. Boston: Artech House, 2016., s. 1 [↑](#footnote-ref-1)
2. KARAME, Ghassan a Elli ANDROULAKI. Op. cit., s. 3 [↑](#footnote-ref-2)
3. SMITH, Jake. The Bitcoin Cash Hard Fork Will Show Us Which Coin Is Best. *Fortune.Com* [online] IN. EBSCOhost, publikováno 11. 8. 2017, s. 14 [cit. 20. 11. 2017]. Dostupný z: search.ebscohost.com/login.aspx?direct=true&db=bth&AN=124579398&lang=cs. [↑](#footnote-ref-3)
4. The Economist Group Limited. The great chain of being sure about things. [online] The Economist. publikováno 31. 10. 2015 [cit. 20. 11. 2017]. Dostupný z: <https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable> [↑](#footnote-ref-4)
5. Ibid. [↑](#footnote-ref-5)
6. SMITH, Jake. Op. cit. [↑](#footnote-ref-6)
7. HERTIG, Alyssa. Bitcoin Cash: Why It's Forking the Blockchain And What That Means. [online] CoinDesk, publikováno 26. 7. 2017 [cit. 20. 11. 2017]. Dostupný z <https://www.coindesk.com/coindesk-explainer-bitcoin-cash-forking-blockchain/> [↑](#footnote-ref-7)
8. SMITH, Jake. Op. cit. [↑](#footnote-ref-8)
9. HERTIG, Alyssa. Op. cit. [↑](#footnote-ref-9)
10. MOW, Samson. The Bitcoin Cash Fork Was a Dangerous Trick. *Fortune.Com*. [online] IN. EBSCOhost, publikováno 7. 8. 2017 [cit. 20. 11. 2017]. Dostupné z: search.ebscohost.com/login.aspx?direct=true&db=bth&AN=124514491&lang=cs. [↑](#footnote-ref-10)
11. BENNINGTON, Ash. $700 and Rising: What's Driving the Price of Bitcoin Cash? [online] CoinDesk, publikováno 18. 7. 2017 [cit. 20. 11. 2017]. Dostupný z: <https://www.coindesk.com/700-rising-whats-driving-price-bitcoin-cash/> [↑](#footnote-ref-11)