POHÃ•DKA O BITCOINU - 1. DÃ•L

ÄŒtvrtek, 25 listopad 2021

Minule jsem vÃ¡m tu psala, jak vÅ¯bec nechÃ¡pu, co to je BITCOIN, kde se vzal, kde se bere, a proÄ• pÅ™edstavuje kupu penÄ›z. Tak jsem zaÄ•ala hledat... TakÅ¾e, byl jednou jeden... ZaÄ•neme slovem blockchain. KdyÅ¾ se Å™ekne slovo blockch spousta lidÃ- se zasekne a zjistÃ-, Å¾e vlastnÄ› vÅ¯bec nevÃ-, o co se jednÃ¡. Blockchain je v doslovnÃ©m pÅ™ekladu Å™etÄ›z z blokÅ¯. Bloky v tomto pÅ™Ã-padÄ› nejsou nic jinÃ©ho, neÅ¾ virtuÃ¡lnÃ- ÃºÄ•etnÃ- knihy. V Bitcoinu mÃ¡ jedna takovÃ¡ kniha prÅ¯mÄ›rnou Å¾ivotnost 10 minut a mÃ¡ omezenÃ© mÃ-sto.

Bitcoin provozuje mnoho poÄ•Ã-taÄ•Å¯ a Å¾Ã¡dnÃ½ z nich neÅ™Ã-dÃ- ostatnÃ-. CentrÃ¡lnÃ- Å™Ã-zenÃ- nenÃ- potÅ™eba, protoÅ¾e pravidla vedenÃ- bitcoinovÃ© ÃºÄ•etnÃ- knihy jsou veÅ™ejnÃ¡ a kaÅ¾dÃ½ poÄ•Ã-taÄ• si nezÃ¡visle ovÄ›Å™uje, Å¾e je vedena sprÃ¡vnÄ›. TakÅ¾e jeÅ¡tÄ› jednou: StrÃ¡nky tÃ©to ÃºÄ•etnÃ- knihy se tedy oznaÄ•ujÃ- jako bloky a celÃ¡ kniha jako blockchain, tedy Å™etÄ›zec blokÅ¯. NahlÃ-Å¾et do nÃ- mÅ¯Å¾ete na blockchain.info.

JejÃ- obsah tvoÅ™Ã- v naprostÃ© vÄ›tÅ¡inÄ› pohyby mezi adresami (tomu se Å™Ã-kÃ¡ transakce), avÅ¡ak jsou zde i dvÄ› vÄ›ci navÃ-c:

Nonce a hash pÅ™edchozÃ-ho bloku. JednÃ¡ se o dva velmi dÅ¯leÅ¾itÃ© pojmy, a proto je dÅ¯leÅ¾itÃ©, abyste nÃ¡sledujÃ-cÃ- definici pochopili. ProzatÃ-m si vystaÄ•Ã-me s vysvÄ›tlenÃ-m, Å¾e

nonce je urÄ•itÃ© Ä•Ã-slo,
kterÃ© se pÅ™idÃ¡vÃ¡ na konec kaÅ¾dÃ©ho bloku.

PÅ™Ã-kladem nonce mÅ¯Å¾e bÃ½t Ä•Ã-slo: 147 483 646.

Hash uÅ¾ je lehce sloÅ¾itÄ›jÅ¡Ã-. Pokud vezmeme nÄ›jakÃ½ soubor dat, pomocÃ- speciÃ¡lnÃ- funkce jej mÅ¯Å¾eme pÅ™eloÅ¾it na jedno Ä•Ã-slo.

Asi jako kdyÅ¾ si vezmeme nÄ›jakÃ½ text a pÅ™eloÅ¾Ã-me ho do morseovky. RozdÃ-l je, Å¾e hash v pÅ™Ã-padÄ› Bitcoinu nelze pÅ™evÃ©st zpÄ›t do dat, ze kter vytvoÅ™en, zatÃ-mco morseovka ano. A navÃ-c pokud v tomto souboru dat zmÄ›nÃ-me byÅ¥ jen jedinÃ½ Ãºdaj, celÃ½ hash bude mÃ-t ÃºplnÄ› jinou podobu.

PÅ™Ã-kladem hashe mÅ¯Å¾e bÃ½t: 000000000000000000007643ed71fcf50b3a2d27ca978f653771b854b8e947e08.

Z toho plyne nÃ¡sledujÃ-cÃ-: kaÅ¾dÃ½ blok mÃ¡ svÅ¯j specifickÃ½ hash. A jeÅ¡tÄ› nÄ›co velice dÅ¯leÅ¾itÃ©ho: Pro takzvanou tÄ›Å¾bu kryptomÄ›ny nestaÄ•Ã- bÄ›Å¾nÃ¡ domÃ¡cÃ- poÄ•Ã-taÄ•ovÃ¡ sestava, je potÅ™eba o mnoho vÃ½konn Ty obÃ¡vanÃ© bitcoiny s malÃ½m b si mÅ¯Å¾ete pÅ™edstavit jako odmÄ›nu za Ä•innost, kterÃ¡ udrÅ¾uje v chodu decentralizovanou sÃ-Å¥ poÄ•Ã-taÄ•Å¯ pojmenovanou Bitcoin s velkÃ½m B. ÃšÄ•el tÃ©to sÃ-tÄ› je jedinÃ½: starat se o

vedenÃ- veÅ™ejnÃ© ÃºÄ•etnÃ- knihy vÅ¡ech bitcoinovÃ½ch transakcÃ-. MoÅ¾nÃ¡ je to takto pÅ™Ã-liÅ¡ abstraktnÃ-, ale pokusÃ-m se toho napsat vÃ-c.

Inu, nevÃ-m jak vy, ale jÃ¡ uÅ¾ jsem ponÄ›kud mimo â€“

pÅ™esto budu pokraÄ•ovat:

TÄ›Å¾aÅ™i bitcoinÅ¯ majÃ- ve svÃ© podstatÄ› naprosto primitivnÃ- prÃ¡ci. Jejich Ãºkolem je najÃ-t konkrÃ©tnÃ- nonce (Ä•Ã-selnÃ½ kÃ³d), kterÃ½ pÅ™idajÃ- k transakcÃ-m v aktuÃ¡lnÄ› otevÅ™enÃ©m bloku, a z toho celÃ©ho vytvoÅ™it hash, kterÃ½ mÃ¡ pÅ™edem urÄ•enÃ© parametry â€“ poÄ•et nul na zaÄ•Ã¡tku.

A protoÅ¾e se hash nedÃ¡ zpÄ›tnÄ› â€žpÅ™eÄ•Ã-stâ€œ a rozluÅ¡tit, nikdo vlastnÄ› nevÃ-, jakÃ¡ kombinace dat je potÅ™ebnÃ¡ k tomu, aby danÃ½ hash, kterÃ½ vÅ¡ichni tÄ›Å¾aÅ™i hledajÃ-, vznikl.

TÄ›Å¾aÅ™ tak musÃ- vzÃ-t nÃ¡hodnÃ½ nonce, vypoÄ•Ã-tat hash a doufat, Å¾e je to sprÃ¡vnÃ½ hash.

KdyÅ¾ se mu to nepovede, vÅ¡e dÄ›lÃ¡ znovu a znovu. Je to hra o Å¡tÄ›stÃ-. O vytrvalosti.O tom, jak sehnat levnou elektÅ™inu.A nemuset to platit (tÅ™eba Å™Ã-ct, Å¾e tÃ-m topÃ-).

No, a pokud i tomuhle nerozumÃ-te, jsme na tom stejnÄ›.

OvÅ¡em pro ty, kteÅ™Ã- jeÅ¡tÄ› vnÃ-majÃ-, oÄ• jde:

Povedlo se nÃ¡m, dejme tomu, najÃ-t (uhÃ¡dnout) sprÃ¡vnÃ½ nonce a zÃ-skali jsme tak sprÃ¡vnÃ½ hash celÃ©ho bloku.

Super, vytÄ›Å¾ili jsme tento blok!
ZÃ¡vod o tento blok skonÄ•il a my jsme jeho vÃ-tÄ›zem. Jako odmÄ›nu zÃ-skÃ¡me nÄ›kolik novÄ› vytvoÅ™enÃ½ch bitcoinÅ¯, kterÃ© pÅ™edtÃ-m nikdo nevlastnil.

My jsme je vytÄ›Å¾ili.

ZaÄ•Ã-nÃ¡ hned ale novÃ½ zÃ¡vod â€“ o blok nÃ¡sledujÃ-cÃ-!NÃ¡mi vytÄ›Å¾enÃ½ blok pÅ™idÃ¡me do nÃ¡sledujÃ-cÃ-ho bloku na zaÄ•Ã¡tek a znovu hledÃ¡me nonce. Je to prostÄ› hra s Ä•Ã-slÃ-Ä•ky... Tak - za chvÃ-li jdu dÃ¡l hledat a napÃ-Å¡u vÃ¡m zas nÄ›jakÃ½ to pokraÄ•ovÃ¡nÃ-. Tohle berte jako prvnÃ- kapitolku z mnoha...

ZdravÃ-m vÅ¡echny pÅ™Ã-padnÃ© budoucÃ- bitcoinovÃ© tÄ›Å¾aÅ™e, vaÅ¡e chudÃ¡ d@niela
:-)))