BITCOIN. O NOUĂ REVOLUTIE IN LUMEA VIRTUALĂ ȘI FINANCIARĂ

Ion SAMOIL; student C-162

Universitatea Tehnica a Moldovei

Bitcoin (din limba engleză bit: unitate de informație binară și coin: monedă), este un sistem de plată electronică descentralizat și o monedă digitală (criptomonedă) opensource creată în 2009 de Satoshi Nakamoto. Bitcoin (BTC) a fost creat pentru a asigura protecția investițiilor și finanțarea liberă a afacerilor, fără a face apel la instituții financiare și în afara oricărei constrângeri și reglementări. Numele Bitcoin se referă de asemenea și la programul opensource pentru folosirea acestor monede, cât și la rețeaua peer-to-peer (de la egal la egal) pe care acesta o formează.

Spre deosebire de majoritatea monedelor, Bitcoin nu se bazează pe încrederea într-un emitent central. Bitcoin folosește o bază de date distribuită peste noduri ale unei rețele de la egal la egal (peer-to-peer) pentru a inventaria tranzacțiile și se folosește de criptografie pentru a furniza funcții de bază pentru securitate cum ar fi asigurarea că bitcoinii nu pot fi cheltuiți decât de cel care îi deține și doar o singură dată.

Construcția monedei Bitcoin permite deținerea și transferul anonim de valoare. Bitcoinii pot fi salvați pe un computer personal sub forma unui fișier portofel sau pot fi stocați cu un serviciu de portofel al unei terțe părți, iar în ambele cazuri bitcoinii pot fi trimiși prin intermediul internetului oricărei persoane cu o adresă Bitcoin. Topologia de la egal la egal și lipsa unei administrații centrale fac nefezabil ca o autoritate, un guvern, etc. să manipuleze valoarea Bitcoinului sau să introducă inflație prin producerea lor.

Bitcoin este una din primele implementări a conceputului numit „criptomonedă" (cryptocurrency), prima dată descris în 1998 de Wei Dai pe mailing listul Cyperpunk.

Bitcoin există totuși și în formă fizică, prin „Casascius Bitcoin" creată de întreprinzătorul american Mike Caldwell, codul unic al unui Bitcoin fiind încorporat într-o monedă care poate fi placată cu aur.

Spre deosebire de majoritatea monedelor, Bitcoin nu se bazează pe încrederea într-un emitent central. Bitcoin folosește o bază de date distribuită peste noduri ale unei rețele de la egal la egal (peer-to-peer) pentru a inventaria tranzacțiile și se folosește de criptografie pentru a furniza funcții de bază pentru securitate cum ar fi asigurarea că bitcoinii nu pot fi cheltuiți decât de cel care îi deține și doar o singură dată.

Sistemul Bitcoin funcționează pe baza unei rețele peer-to-peer și a criptografiei asimetrice. Criptografia asimetrică utilizează o pereche de chei asimetrice (publică și privată). Termenul de „asimetric" provine de la utilizarea de chei diferite pentru a îndeplini două funcții opuse (criptare și decriptare), fiecare fiind inversul celeilalte. Transferul de sume între conturile publice folosește cheile criptografice publice pentru a confirma tranzacțiile și a preveni dubla-cheltuire.

Cheia publică este utilizată pentru criptarea unui text, care apoi nu poate fi decodificat decât folosind cheia privată corespunzătoare. Criptarea cu cheie publică este folosită în tranzacțiile cu Bitcoin pentru a asigura confidențialitatea.

Cheia privată este utilizată pentru a decripta textul cifrat și pentru a crea o semnătură digitală. Un mesaj creat cu cheia privată a emițătorului poate fi verificat de oricine, prin acces la cheia publică corespunzătoare, astfel asigurându-se autenticitatea mesajului.

Caracteristicile criptomonedelor

Proof-of-work

Criptomonedele folosesc protocoale proof-of-work pe bază de algoritmi de hashing. Cele mai utilizate se bazează pe algoritmul SHA-256, introdus de Bitcoin, și scrypt, cel mai utilizat, având cel puțin 480 de implementări confirmate. Alți algoritmi care sunt folosiți pentru proof-of-work includ CryptoNight, Blake, X11, și combinații.

Portofele digitale

Un portofel digital este, în general, echivalentul unui cont bancar: permite primirea de criptomonede, stocare și trimitere către alte conturi. Portofelele stochează parola privată necesară pentru a accesa adresa bitcoin.

Fiecare utilizator instalează o aplicație software, care este un fișier portofel digital, pe calculator sau pe telefonul mobil, sau de pe o pagină web. Folosindu-se de acest portofel digital, utilizatorul poate să trimită sau să primească criptomonede de la alți utilizatori.

Portofelele digitale pot fi dedicate, pentru o singură criptomonedă (exemple: Bitcoin, Etherium, Ripple, Litecoin), sau pot fi multimonede (Coinomi, CoinSpot, CoinVault, Cryptonator multi-cryptocurrency wallet, Exodus, Gatehub, Holy Transaction, Jaxx Wallet, UberPay Wallet

Tranzacții

Tranzacțiile în criptomonede sunt securizate cu ajutorul criptografiei între portofele virtuale. Fiecare portofel virtual va primi o „cheie privată" care rezultă în urma criptografiei. Această cheie privată împiedică alterarea, modificarea tranzacției de către o altă persoană, acest lucru făcând ca tranzacțiile să fie extrem de sigure.

Tranzacțiile se fac pe baza unei adrese alfanumerice sub forma unui string de genul 1FfmbHfnpaZjKFvyi1okTjJJusN455paPH derivat din porțiunea publică a uneia sau a mai multor perechi de chei criptografice, generate gratuit. O cheie criptografică reprezintă un algoritm ce necesită două chei individuale, una secretă și una publică legate prin algoritm. Pentru a beneficia de criptomonedele trimise către o adresă, utilizatorul trimite un mesaj, semnat digital, cu plata împreună cu cheia privată asociată.

Minare

Criptomoneda poate fi cumpărată, dar și creată. Procesul de creare a monedei se numește „minare". Participanții în rețea sunt cunoscuți sub numele de mineri (engleză: miners). Aceștia verifică, datează tranzacțiile și le partajează într-o bază de date publică, numită blockchain(lanț de blocuri). Există noduri specializate care validează tranzacțiile și blocurile și le conectează între punctele tranzacției

Operațiunea de minare este deosebit de complexă și este foarte dificil de realizat pe cont propriu, de un singur utilizator. Astfel, s-au dezvoltat grupuri de mineri, numite mining pools. Un grup de mineri combină puterea lor de procesare pentru rezolvarea algoritmilor producători de criptomonede.

Hardware

Minatul de criptomonedă presupune folosirea puterii de calcul a sistemelor PC pentru operațiunea de mining. Sunt dezvoltate mai multe sisteme dedicate pentru mineritul de criptomonede. Aceste dispozitive se numesc ASIC (Application Specific Integrated Circuit) și reprezintă niște circuite integrate cu cipuri programate în mod permanent și cu o aplicație integrată în cipurile respective. Două companii populare ce oferă instalații de minerit tip ASIC sunt Avalon Asics și Butterfly Labs.

Software

În timp ce procesul de minare în sine este făcut de hardware, este nevoie de software special pentru a conecta minerii la blockchain și mining pool. Software-ul poate să ruleze pe aproape orice sistem de operare, cum ar fi Mac OS X, Windows, Linux. Programul transmite informații și rezultate către miner, dar și monitorizează statisticile generale cum ar fi temperatura, hashrate-ul, viteza ventilatorului, viteza medie a minerului etc.

Avantaje și dezavantaje

Avantaje

- este un sistem descentralizat, nu există o autoritate centrală, cum ar fi o bancă centrală
- datele personale despre utilizatori sunt ascunse
- se poate crea o copie de rezervă criptată a monedei virtuale
- plata se poate face fără ca datele personale să fie asociate cu tranzacția
- utilizatorii au în permanență controlul tranzacțiilor
- transfer foarte rapid oriunde în lume
- nu există limită de sumă pentru transferuri
- comisioane variabile

Dezavantaje

- utilizare redusă
- volatilitatea datorită faptului că moneda este în cantitate limitată, iar valoarea ei este dată de cerere și ofertă
- ireversibilitatea tranzacțiilor, anularea fiind imposibilă
- interdicția utilizării anumitor criptomonede în unele țări
- distribuția neuniformă a criptomonedei între primii utilizatori și cei actuali
- necesită un înalt nivel de securitate
- nu toți comercianții acceptă cripomoneda ca metodă de plată.

Un bitcoin se poate diviza până la 8 cifre decimale. Partea bună este că poți cumpăra sau vinde sume mici (adică sub 1 bictoin) până la 0.00000001 BTC.

Denimirele pe care le vei întâlni sunt:

1 BTC = 1 bitcoin

0,01 BTC = 1 cBTC = 1 centibitcoin (denumit și bitcent)

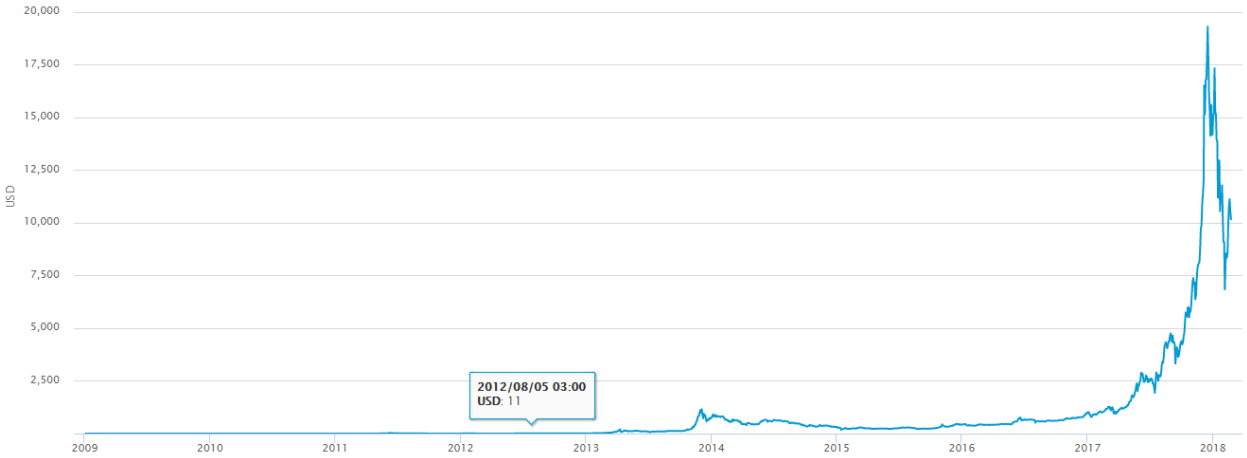
0,001 BTC = 1 mBTC = 1 milibitcoin (denumit și mbit sau milibit sau chiar bitmil)

0,000 001 BTC = 1 μBTC = 1 microbitcoin (denumit și ubit (pronunțat iu-bit) sau microbit)

Există mai mult de 700 de criptomonede disponibile pentru comerțul pe piețele online, dar numai aproximativ 20 dintre acestea au avut capitalizări de piață de peste 10 milioane USD.

La momentul prezentării lucrării date valoare unui bicoin este de 1 BTC = 7828.54 USD, valoare inițială în 2009 fiind de de 16 cenți= 0.16$

Evolutia Monedei BICOIN



Bibliografia

1. https://laurentiumihai.ro/investitiile-in-bitcoin/
2. http://businessflowtools.blogspot.md/2017/10/bitcoin-intrebari-frecvente-ce-este.html
3. https://www.ziarulnational.md/banii-virtuali-cautati-in-r-moldova-1/
4. http://www.bursa.ro/sfarsitul-sau-evolutia-bitcoin-monedele-alternative-prind-interesul-statelor-325078&s=print&sr=articol&id_articol=325078.html
5. https://goanadupabitcoin.ro/pentru-incepatori/moneda-bitcoin.html
6. https://ro.wikipedia.org/wiki/Criptomonedă