Kriptovaluta

Kriptovaluta je digitalni novac koji ne kontroliše neka centralna banka ili vlada. Koristi se u decentralizovanoj P2P mreži gde su svi jednaki i trguju kriptovalutom. Sam pojam digitalnog novca pojavio se tokom osamdesetih godina dvadesetog veka. Nažalost, ovako nešto nije zaživelo sve do 2009. godine kada je čovek ili grupa ljudi pod imenom Satoshi Nakamoto pustio u rad Bitcoin. Bitcoin je danas jedan od najvrednijih kriptovaluta na svetu.

Kriptovalutu možemo objasniti kroz sledeće pojmove: zapisnik, digitalni potpis, identifikacioni broj, provera stanja na računu, veza sa pravim novcem, decentralizacija, kriptografske hash funkcije, blockchain, rudari.

U zapisniku se drže sve transakcije poredjane po redu, svako može da doda liniju u isti što ga čini javnim jer je to i poenta kriptovalute, da bude pristupačna i da niko ne može da je kontroliše. Nažalost uz samo ovaj pojam za sad imamo veliki problem, bilo ko može dodati liniju u zapisnik, pa može doći do prevare.

Kako bi sprečili zloupotrebu zapsnika, uvode se digitalni potpisi, koji se kreiraju uz pomoć javnog i tajnog ključa. Javni i tajni ključ su brojevi od 256 bitova, kako bi ta dva broja napravila specijalan broj koji će biti potpis za neku transakciju potrebno je da prodju kroz dve kriptografske funkcije. Prva funkcija će biti NapraviPotpis koja za ulaz ima tajni ključ i poruku tj. neku transakciju i na izlazu treba da dobijemo traženi potpis, koji će za svaku transakciju biti drugačiji. Druga funkcija će samo potvrditi da li je potpis koji je napravljen validan, za ulaz prima potpis,poruku i javni ključ, na izlaz izbacuje istina ili laž. Problem sa kojim se srećemo ovde jeste da sada u zapisnik može da se doda ista linija transakcije više puta i da to bude validno.

Identifikacioni broj dodaje se na početku svake linije transakcije u zapisniku i tako nikada nećemo imati transakciju koja glasi isto kao neka druga. Potpis koji se dobija biće različit sada za bilo koju transakciju.

Da ne bi bilo dugovanja, u zapisnik se upisuju ljudi samo ako ulože neki novac sa kojim će trgovati i pratiće se svaka transakcija od kako zapisnik postoji kako bi znali da li korisnik ulazi u dug pri nekoj transakciji ili ne. Ako ulazi u dug transakcija neće biti validna.

Kako ostvarili vezu sa pravim novcem, mora da postoji dogovor izmedju ljudi koja će biti vrednost kriptovalute. Obično se to ostvaruje kada kriptovaluta izadje na legalnu berzu.

Do sada ovi pojmovi su se odnosili na centralizovani sistem, gde se zapisnik nalazio na jednom mestu. Kako bi decentralizovali ceo sistem zapisnik saljemo svima koji su deo sistema. Problem koji se sad nazire jeste kako održavati taj zapisnik tako da bude onaj pravi i koje transakcije da zapisujemo na naš zapisnik? Blockchain i kriptografske hash funkcije su odgovor.

Krptografske hash funkcije su funkcije koje primaju za ulaz neku poruku ili fajl i ispisuju broj od 256 bitova što je u slučaju sa SHA256. Ovaj broj izgleda kao da je nasumičan, ali ako propustite istu poruku kroz istu funkciju dobićete opet isti broj. Ovo koristimo kako bi dobili neki dokaz o radu na našem zapisniku kako bi bili sigurni da je to onaj pravi.

Kada se sada zapisnik podeli u blokove, to bi bio blockchain. Blockchain sadrži ograničen broj transakcija koje su potpisane, na dnu specijalan broj koji kada se poveže sa svim transakcijama i prosledi hash funkciji dobije se broj sa 30 nula na početku. Mogućnost da se pronadje taj broj je 1:. Da bi se pronašao potrebna je ogromna kompjuterska moć. Broj koji dobijemo zovemo hash i dodajemo ga na vrh u sledećem bloku i tako u krug. Ako se kojim desi da dobijemo dva bloka istovremeno onda ćemo sačekati malo da vidimo na koji će se blok najviše istih dovezati i izabrati da pratimo onaj najduži.

Da bi ceo sistem funkcionisao potrebna je velika kompjuterska moć, pa se u priču uvode rudari koji će pronaći onaj specijalan broj na dnu bloka, zbog uloženog rada rudar kada pronadje specijalan broj dobija odredjen broj kriptovalute. Vremenom se smanjuje nagrada za rudare sve dok ona nestane. Kada nagrada nestane, onda se uvodi obavezan deo koji mora da se plati rudaru kako bi se transakcija izvršila.

Ovo su glavni pojmovi koji čine kriptovalutu ono što jeste. Danas postoji ogroman broja različitih kriptovaluta i neke imaju neki novitet ali se u suštini ne odvajaju od pojmova napomenutih do sad.