Osnove o kripto valuti!

Ali vas zanima kaj so kripto valute, pa se nikoli niste resno poglobili v to tematiko? Brez skrbi, v tem članku vam bomo na enem mestu pojasnili vse potrebne osnove, ki vam bodo pomagale do boljšega razumevanja kripto valut.

Začeli bomo z osnovnim vprašanjem glede tega, kaj so kripto valute, potem pa si bomo tematiko razdelili na bolj "prebavljive" kose informacij. Za boljše razumevanje moramo namreč razložiti pojme, kot so digitalna valuta, pojem rudarjenje, decentralizacija,"blockchain" in kriptografija.

Pa začnimo!

Kaj je digitalna valuta?

Kripto valute so digitalne valute. Obstajajo samo na računalnikih, saj v sistemu ni nobenih oprijemljivih bankovcev ali kovancev. Virtualni denar je lahko centraliziran, kjer obstaja centralna točka nadzora nad ponudbo denarja, ali pa decentraliziran, kjer nadzor nad ponudbo denarja prihaja iz različnih virov. Verjetno ste uganili, da kripto valute spadajo med decentralizirano vrsto virtualnega denarja.

Kaj je rudarjenje?

Rudarjenje je razpršen sistem doseganja soglasja (angl. "distributed consensus system"). Ko želi nekdo opraviti transakcijo, vsakdo v decentralizirani mreži prejme kopijo te transakcije. Vsi člani omrežja morajo potrditi to transakcijo, s tem pa se zmanjša ali celo odpravlja možnost goljufije. To pomeni, da več ljudi po vsem svetu sodeluje pri vzdrževanju omrežja. Rudarjenje je izraz, ki se uporablja za potrjevanje transakcij, ki čakajo na vključitev v verigo blokov oziroma "blockchain".

Tako se v verigi blokov doseže kronološka razvrstitev transakcij. Za potrditev mora biti transakcija zapakirana v blok, ki mora zadoščati strogim pravilom šifriranja, ki jih preverijo in potrdijo rudarji v omrežju. Pri tem ni nobenega uradnega ali vladnega organa, ki bi celoten proces kontroliral. Tako se zaščiti nevtralnost omrežja.

Na hitro naredimo primerjavo s tradicionalnim sistemom elektronskega denarja, recimo z uporabo kreditnih kartic. Ob vsakem plačilu s kartico mora izdajatelj kreditne kartice (npr. MasterCard) potrditi in evidentirati transakcijo. Pri kriptovalutah imajo to vlogo rudarji.

Proces nastajanja novih kripto valut se imenuje rudarjenje, saj ima veliko vzporednic z rudarjenjem zlata. V obeh primerih gre za vlaganje velike količine dela in "energije" za proizvodnjo dragocenega izdelka.

Pri večini kripto valut ni nobene tretje osebe ali centralne organizacije, ki bi potrjevala transakcije. To delo opravljajo rudarji kovancev, ob tem pa tudi ustvarjajo nove kovance!

Kaj je decentralizacija?

Večinoma gre pri kripto valutah za decentralizirane valute, saj sistem deluje brez centralne banke ali enega samega administratorja. Vrednost in zalogo teh digitalnih valut ne ureja noben osrednji organ, ampak uporabniki sami.

Za boljše razumevanje si poglejmo sledeči primer. Ko obiščete spletni brskalnik in vnesete "www.google.com", računalnik začne pogovor z Googlovimi strežniki. Brskalnik vam nato

prikaže iskane rezultate. Če Googlovi strežniki slučajno ne bi bili dosegljivi, potem vam ne bi prikazali nobenih rezultatov. Podatki so namreč shranjeni v centraliziranem omrežju – torej na enem mestu (oziroma so pod nadzorom ene organizacije). V decentraliziranem omrežju se med drugim izognemo točno takšnim problemom.

Osnovna značilnost kripto valut je, da jih ne izdaja noben osrednji organ, zaradi česar so teoretično imune na vmešavanje ali manipulacijo vlade.

Kaj je "blockchain"?

Ali ste kdaj prek e-maila poslali kakšno datoteko (recimo sliko s potovanja) svojemu prijatelju ali prijateljici? V takšnem primeru ste naredili digitalno kopijo datoteke. Verjetno si predstavljate, da ne bi bilo prav dobro, če bi lahko isto počeli z digitalnim denarjem. Narava digitalnih datotek je namreč taka, da jih ni težko podvajati v nedogled. S tem se npr. spopadajo vsi glasbeniki, v finančnem svetu pa temu rečemo problem dvojne porabe (ang. "Double-spending problem"). Kako odpraviti možnost, da bi nekdo isto vsoto poslal dvakrat in tako ustvaril nov denar?

Tukaj nastopi tehnologija veriženja podatkovnih blokov, ki namesto kopiranja omogoča distribucijo sredstev.

Veriženje blokov torej predstavlja rešitev problema dvojne porabe. Transakcij tako ni možno podvajati, s čimer se prepreči ustvarjanje novih kovancev iz nič.

Kaj je kriptografija?

Kriptografija se uporablja za pretvorbo podatkov o transakcijah. Med najbolj slavne naprave za kriptografirano komunikacijo spada "Enigma", ki se je uporabljala med drugo svetovno vojno. Za razliko od Enigme, pri kateri so zavezniki uspeli najti rešitev za dekodiranje sporočil, je kriptografija kripto valut še nezlomljiva. Vsaj trenutno, čeprav se pričakuje, da bo tako ostalo še zelo dolgo, razen če pride do nepredvidenega skoka v računski moči (pri tem se pogosto omenjajo t.i. kvantni računalniki, ki pa so še daleč od prave realizacije). Lahko bi jo poimenovali tudi kriptografija javnega in zasebnega ključa. Ta tehnologija omogoča dokazovanje identitete s parom kriptografskih ključev: to sta zasebni ključ in javni ključ.

Kako uporabiti in hraniti kripto valute?

Kripto valute obstajajo samo v digitalni obliki, zato si morda predstavljate, da plačevanje z njimi poteka na podoben način kot plačevanje s kreditnimi ali debetnimi karticami. Na prvi pogled morda že izgleda tako, v ozadju pa stvari seveda delujejo precej drugače.

Kripto valute namreč obstajajo samo na verigi podatkovnih blokov, uporabniki pa do svojih kovancev dostopajo s tako imenovanimi javnimi in zasebnimi ključi. Kripto valute namreč niso shranjene na enem mestu v obliki datoteke. Za hranjenje kripto valut potrebujete posebno vrsto digitalne denarnice.

Kripto denarnice so vedno sestavljene iz dveh ključev oziroma iz dveh delov. Prvi del je javni naslov denarnice, ki ga lahko brez skrbi delite z ostalimi. Drugi del je zasebni ključ, ki ga nikoli ne smete razkriti.

Lahko si predstavljate, da kripto valute v osnovi delujejo podobno kot e-mail. Če želite od neke osebe prejeti e-mail, potem morate z njo najprej deliti svoj e-mail naslov. Pri kripto valutah je enako, le da v tem primeru delite svoj javni ključ (naslov svoje denarnice). Če želite dostopati do e-mail sporočil, potem morate poznati geslo svojega uporabniškega računa. Podobno je pri kripto valutah, kjer morate za dostop do svojih kripto valut poznati privatni ključ (geslo) svoje denarnice.

Zasebni ključ se uporablja za šifriranje transakcij, medtem ko se javni ključ uporablja za dešifriranje. Zato mora biti zasebni ključ vedno varen. Kdor ima dostop do zasebnega ključa,

je tudi lastnik denarnice. Javni ključ je namenjen izmenjavi s tretjimi osebami in sporoča, da ste lastnik naslova, ki lahko prejema sredstva.

Javne ključe lahko zato delite z drugimi, zasebni ključ pa mora ostati v vaši lasti.

Svet je vse bolj digitalen in povezan, kripto valute pa pri tem igrajo zelo zanimivo vlogo. BTC in druge kripto valute za nekatere predstavljajo prihodnost denarja, za katere napovedujejo, da bodo spremenile svetovni finančni sistem. Vsekakor imajo kripto valute potencial, da za vedno spremenijo naša življenja in nam pomagajo pri tem, da prevzamemo nadzor nad svojimi sredstvi. Kripto valute namreč omogočajo novo ureditev finančnega sistema, ponujajo pa zanimive rešitve na številnih področjih. Obstajajo namreč različne vrste kripto valut, in vsaka predstavlja neko unikatno idejo ali rešitev.

Pazite na vaše Pi-je, prihaja čas, ko boste morali pametno in preudarno razpolagati z njimi! Srečno slovenski Pionirji!

Vaša ekipa Pi Slovenije, vedno z Vami!