Šta su kripto valute - kako funkcionišu, istorijat i Bitcoin alternative

Kripto valute ili virtuelne valute su digitalni načini razmjene koje kreiraju i koriste privatni pojedinci ili grupe. Budući da većinu kriptovaluta ne regulišu nacionalne vlade, smatraju se alternativnim valutama - medijima razmjene finansija koji postoje izvan granica državne monetarne politike.

Bitcoin je vodeća kriptovaluta. Međutim, postoje stotine kriptovaluta i pojavljuju se gotovo svakog mjeseca.

Šta su kriptovalute?

Kripto valute koriste kriptografske protokole ili izuzetno složene kodne sisteme koji kriptuju osjetljive podatke, da bi se osigurala jedinica razmjene.

Developeri kripto valuta kreiraju ove protokole na naprednim principima matematike i računarskog inženjerstva zbog kojih ih je gotovo nemoguće "probiti" te na taj način duplicirati ili krivotvoriti valute. Ovi protokoli takođe maskiraju identitet korisnika kripto valute, čineći da se transakcije i tokovi sredstava teško pripisuju određenim pojedincima ili grupama.

Decentralizovana kontrola

Kripto valute se takođe karakterišu decentraliziranom kontrolom. Snabdijevanje i vrijednost kriptovaluta se kontrolišu aktivnostima njihovih korisnika i visoko složenim protokolima, a ne zavise od odluka centralnih banaka ili drugih regulatornih tijela. Posebno su aktivnosti rudara, korisnika kripto valute koji koriste moćne računare za zapisivanje transakcija, primajući novostvorene jedinice kripto valute i naknade za transakcije koje drugi korisnici plaćaju za uzvrat, ključne za stabilnost valuta i nesmetano funkcionisanje.

Razmjena sa *fiat* valutama

Kripto valute mogu biti zamijenjene za *fiat* valute na posebnim *online* tržištima, što znači da svaka ima promjenjivi kurs s glavnim svjetskim valutama (poput američkog dolara, britanske funte, evropskog eura, japanskog jena…). Razmjene kriptovaluta su ponekad osjetljive na hakovanje i predstavljaju najčešće mjesto zloupotreba od strane hakera i *cyber* kriminala.

Ograničena količina

Za većinu, ali ne sve, kripto valute karakteriše ograničena ponuda. Njihovi izvorni kodovi sadrže upute koji preciziraju tačan broj jedinica koje mogu postojati. S vremenom, rudarima postaje teže proizvesti jedinice kriptovalute, sve dok se gornja granica ne dosegne i nova valuta prestane kreirati u potpunosti. Konačna ponuda kriptovaluta čini ih inherentno deflacionim, više nalik zlatu i drugim plemenitim metalima - kod kojih postoje ograničene zalihe - nego *fiat* valutama, koje centralne banke u teoriji mogu proizvesti u neograničenim količinama.

Prednosti i nedostaci

Zbog svoje političke nezavisnosti i u osnovi neprobojne sigurnosti podataka, korisnici kripto valute uživaju pogodnosti koje nisu dostupne korisnicima tradicionalnih *fiat* valuta, poput američkog dolara, i finansijskim sistemima koje te valute podržavaju. Na primjer, iako vlada može lako zamrznuti ili čak zaplijeniti bankovni račun koji se nalazi u njenoj nadležnosti, veoma je teško to učiniti sa sredstvima koja se drže u kripto valuti - čak i ako je vlasnik državljanin ili legalni rezident.

S druge strane, kripto valute dolaze s mnoštvom rizika i nedostataka, poput nelikvidnosti i volatilnosti vrijednosti, koji ne utiču na mnoge *fiat* valute. Uz to, kripto valute se često koriste za olakšavanje transakcija na sivom i crnom tržištu, pa ih mnoge zemlje gledaju s nepovjerenjem ili animozitetom. I dok neki zagovornici prikazuju kripto valute kao potencijalno unosna alternativna ulaganja, malo ozbiljnih finansijskih profesionalaca ih smatra prikladnim za bilo šta drugo osim za čista nagađanja.

Kako kruptovalute funkcionišu?

Izvorni kodovi i tehničke kontrole koje podržavaju i osiguravaju kripto valute vrlo su složene. Međutim, laici su više nego sposobni razumjeti osnovne koncepte i postati informisani korisnici kripto valute.

U funkcionalnom smislu, većina kripto valuta predstavlja varijacije Bitcoin-a, prvoj široko korištenoj kripto valuti. Kao i tradicionalne valute, vrijednost kriptovaluta izražena je u jedinicama - na primjer, može se reći „Imam 2,5 bitkoina“, baš kao što bi rekli, „imam 2,50 dolara“.

Nekoliko koncepata reguliše vrijednosti, sigurnost i integritet kriptovaluta.

Blockchain

Blok-lanac kripto valute je glavni zapis koji bilježi i čuva sve prethodne transakcije i aktivnosti, ovjeravajući vlasništvo nad svim jedinicama valute u bilo kojem trenutku. Kao do sada zabilježena čitava istorija transakcija kriptovalute, *blockchain* ima ograničenu dužinu - koja sadrži ograničen broj transakcija - koja se vremenom povećava.

Identične kopije *blockchain*-a čuvaju se u svakom čvorištu mreže kripto valute - mreže decentralizovanih farmi servera, kojom upravljaju pojedinci ili grupe pojedinaca poznatih kao rudari, a koji kontinuirano bilježe i potvrđuju transakcije s kripto valutama.

Transakcija kriptovaluta tehnički se ne dovršava sve dok se ne doda u *blockchain*, što se obično događa u roku od nekoliko minuta. Jednom kada je transakcija finalizovana, obično je nepovratna. Za razliku od tradicionalnih procesora plaćanja, poput PayPala i kreditnih kartica, većina kripto valuta nema ugrađenu funkciju povrata ili povrata sredstava, iako neke novije kripto valute imaju rudimentarne osobine povrata.

Za vrijeme između pokretanja i finalizacije transakcije, jedinice nisu dostupne za upotrebu nijednoj strani. Umjesto toga, oni se drže u svojevrsnom *escrow – limbo* stanju, za sve namjere i svrhe. Blok lanac na taj način sprečava dvostruko trošenje, ili manipulaciju kripto valuta kodom kako bi se omogućilo dupliciranje i slanje istih jedinica valute višestrukim primaocima.

Privatni ključevi

Svaki vlasnik kripto valute ima privatni ključ koji potvrđuje njegov identitet i omogućava mu razmjenu jedinica. Korisnici mogu kreirati svoje privatne ključeve, koji su formirani kao cijeli brojevi dužine od 1 do 78 cifara, ili ih mogu dobiti pomoću generatora slučajnih brojeva. Jednom kada dobiju ključ, mogu nabaviti i trošiti kriptovalute. Bez ključa, vlasnik ne može potrošiti ili pretvoriti svoju kripto valutu - čineći svoje udjele bezvrijednim osim ako i dok ključ ne povrati.

Iako ova sigurnosna osobina smanjuje krađu i neovlašćenu upotrebu, ona je takođe drakonska. Gubitak privatnog ključa digitalni je ekvivalent bacanju gomile novca u smeće. Iako se može kreirati još jedan privatni ključ i ponovo početi akumulacija kripto valuta, ne mogu se povratit udjeli zaštićeni starim izgubljenim ključem. Korisnici kripto valute pažljivo štite svoje privatne ključeve, obično ih čuvauju na više digitalnih (zbog sigurnosnih razloga uglavnom nisu povezani s internetom) i analognih (tj. papirnih) lokacija.

Novčanici

Korisnici kripto valute imaju "novčanike" s jedinstvenim informacijama koje ih potvrđuju kao privremene vlasnike svojih jedinica. Dok privatni ključevi potvrđuju autentičnost transakcije kriptovaluta, novčanici smanjuju rizik krađe za jedinice koje se ne koriste. Novčanici su osjetljivi na hakovanje. Na primjer, japanska berza Bitcoin Mt. Gox je proglasila bankrot nekoliko godina unazad, nakon što su je hakeri sistematski “oslobodili” za više od 450 miliona dolara u Bitcoinima, razmjenjenim preko njenih servera.

Novčanici se mogu čuvati na *cloud*-ima, internim *hard* diskovima ili eksternim uređajima za čuvanje. Bez obzira na način čuvanja novčanika, preporučuje se barem jedna sigurnosna kopija.

Treba imati na umu da sigurnosno kopiranje novčanika ne duplicira stvarne jedinice kripto valute, već samo evidenciju njihovog postojanja i trenutnog vlasništva.

Rudari

Rudari služe kao čuvari zapisa u zajednicama kripto valuta i indirektni arbitri vrijednosti valuta. Koristeći ogromne količine računarske moći, koja se često manifestuje na privatnim farmama u vlasništvu rudničkih kolektiva, koji broje desetine pojedinaca, rudari koriste visoko-tehničke metode da provjere kompletnost, tačnost i sigurnost blokovskih lanaca valuta. Opseg operacije nije različit od potrage za novim primarnim brojevima, što takođe zahtijeva ogromne količine računarske moći.

Rudarski rad periodično stvara nove kopije *blockchain*-a, dodajući nedavne, prethodno neprovjerene transakcije koje nisu uključene u nijednu prethodnu *blockchain* kopiju - efektivno dovršavajući te transakcije. Svaki dodatak poznat je kao blok. Blokovi se sastoje od svih transakcija izvršenih od trenutka kada je stvorena posljednja nova kopija *blockchain*-a.

Izraz "rudari" odnosi se na činjenicu da rad rudara bukvalno stvara bogatstvo u obliku potpuno novih kripto-valutnih jedinica. U stvari, svaka novostvorena *blockchain* kopija dolazi s dvodijelnom novčanom nagradom: fiksnim brojem novo „pronađenih“ kripto-valutnih jedinica i varijabilnim brojem postojećih jedinica prikupljenih od neobaveznih naknada za transakcije (obično manje od 1% od vrijednost transakcije) koju plaćaju kupci.

Napomena: Nekada je rudarenje kriptovaluta bilo potencijalno unosan sporedni posao za one koji imaju resurse za ulaganje u intenzivne rudarske operacije. Danas je nepraktično za hobiste koji nemaju hiljade dolara da ulažu u rudarsku opremu profesionalnog kvaliteta. Ako je cilj jednostavna dopuna dohotka, puno freelance koncepata nudi bolji povrat.

Iako se naknada za transakcije ne naplaćuje prodavačima, rudarima je dozvoljeno da prilikom kreiranja novih *blockchain*-a daju prednost transakcijama “filovanim” naknadama umjesto transakcijama bez plaćanja naknade, čak i ako su transakcije bez naknade nastupile prve. To prodavačima daje pdsticaj za naplatu naknada za transakcije, jer im se brže plaća, pa je prilično uobičajeno da transakcije dolaze s naknadama. Iako je teoretski moguće da prethodno neprovjerene transakcije nove kopije *blockchain*-a u potpunosti budu besplatne, to se u praksi gotovo nikada ne događa.

Kroz upute u izvornim kodovima kripto valute se automatski prilagođavaju količini rudarske snage koja radi na stvaranju novih *blockchain* kopija - kopije je teže stvoriti s povećanjem snage rudarenja i lakše ih je stvoriti s padom snage rudarenja. Cilj je održati stabilan prosječni interval između novih kreacija *blockchain*-a na unaprijed zadanom nivou. Na primjer, za Bitcoin to traje 10 minuta.

Ograničena količina

Iako rudarenje periodično proizvodi nove jedinice kripto valute, većina je kripto valuta dizajnirana tako da ima ograničenu količinu - ključni garant vrijednosti. Generalno, to znači da rudari dobijaju manje novih jedinica po novom *blockchain*-u kako vrijeme prolazi. Na kraju će rudari za svoj rad dobijati samo naknadu za transakcije, iako se to još nije dogodilo u praksi i možda neće još neko vrijeme. Ako se trenutni trendovi nastave, predviđanja su da će posljednja Bitcoin jedinica biti izrudarena negdje sredinom 22. vijeka.

Kripto valute sa ograničenom količinom su zato sličnije plemenitim metalima, poput zlata, nego *fiat* valutama - kod kojih, teoretski, postoje neograničene zalihe.

Razmjena kriptovaluta

Mnogo manje korišćenih kripto valuta može se razmijeniti samo privatnim, *peer-to-peer* transferima, što znači da nisu baš likvidne i teško ih je vrednovati u odnosu na druge valute, i kripto i *fiat*.

Popularnije kripto valute, poput Bitcoina i Ripplea, trguju se na posebnim sekundarnim berzama sličnim Forexovim za *fiat* valute. (Sada van funkcije Mt. Gox je jedan primjer) Ove platforme omogućuju vlasnicima da razmjenjuju svoje kripto-valute sa glavnim *fiat* valutama, kao što su američki dolar i euro, i drugim kripto valutama (uključujući manje popularne valute). U zamjenu za svoje usluge, oni uzimaju malu vrijednost svake transakcije - obično manje od 1%.

Berze kriptovaluta igraju važnu ulogu u stvaranju likvidnih tržišta za popularne kripto valute i određivanju njihove vrijednosti u odnosu na tradicionalne valute. Međutim, cijene razmjene i dalje mogu biti krajnje nestabilne. Američki kurs Bitcoina pao je za više od 50% nakon bankrota Mt. Gox-a, a zatim se tokom 2017. godine povećao otprilike deset puta kako je potražnja za kripto valutama eksplodirala. Može se čak i trgovati derivatima kripto-valute na određenim kripto-berzama ili pratiti široko zasnovane portfolije kripto-valute u kripto indeksima.

Istorijat kriptovaluta

Kripto valuta je postojala kao teorijski konstrukt mnogo prije nego što je prva digitalna alternativna valuta debitovala. Pristalice rane kriptovalute dijelile su cilj primjene vrhunskih matematičkih i računarskih nauka kako bi se riješilo ono što su smatrali praktičnim i političkim nedostacima „tradicionalnih“ *fiat* valuta.

Tehnološke osnove

Tehnološke osnove kriptovalute datiraju iz ranih 80-ih, kada je američki kriptograf po imenu David Chaum izumio algoritam „zaslјepljivanja“ koji i dalje ostaje središnji deo moderne enkripcije na webu. Algoritam je omogućavo sigurnu, razmjenu informacija između strana, postavljajući temelje za buduće elektronske transfere valute. To je bilo poznato kao "zaslijepljeni novac".

Krajem osamdesetih godina Chaum, nakon preseljenja u Nizozemsku, osniva DigiCash, profitnu kompaniju koja je izrađivala jedinice valute na osnovu zaslјepljujućeg algoritma. Za razliku od Bitcoina i većine drugih modernih kriptovaluta, kontrola DigiCash-a nije bila decentralizovana. Kompanija Chaum imala je monopol nad kontrolom snabdijevanja, sličan monopolu centralnih banaka na *fiat* valute.

DigiCash se u početku bavio direktno pojedincima, ali je centralna banka Holandije zabranila tu ideju. Suočen s ultimatumom, DigiCash je pristao da prodaje samo bankama s licencom, ozbiljno umanjivši svoj tržišni potencijal. Microsoft se kasnije obratio DigiCash-u u vezi potencijalno unosnog partnerstva koje bi omogućilo ranim Windows korisnicima da kupuju u njegovoj valuti, ali dvije se kompanije nisu mogle dogovoriti oko uslova.

Otprilike u isto vrijeme softverski inženjer po imenu Wei Dai objavio je bijelu knjigu o b-*money*-u, arhitekturi virtuelne valute, koja je uključivala mnoge osnovne komponente modernih kripto valuta, poput složene zaštite anonimnosti i decentralizacije. Međutim, b- *money* nikada nije bio raspoređen kao sredstvo razmjene.

Ubrzo nakon toga, Chaumov saradnik po imenu Nick Szabo razvio je i izdao kriptovalutu zvanu Bit Gold, koja je bila prepoznatljiva po korišćenju *blockchain* sistema koji podupire većinu modernih kripto valuta. Poput DigiCash-a, Bit Gold nikad nije stekao popularnost i više se ne koristi kao sredstvo razmjene.

Pre-Bitcoin virtuelne valute

Nakon DigiCash-a, veći dio istraživanja i ulaganja u elektronske finansijske transakcije prešao je na konvencionalnije, iako digitalne posrednike, poput PayPal-a (glavni nosilac mobilnih platnih tehnologija koje su u posljednjih 10 godina eksplodirale). Nekoliko imitatora DigiCash-a, poput ruske WebMoney, pojavilo se u drugim dijelovima svijeta.

U Sjedinjenim Državama najznačajnija virtuelna valuta s kraja 1990-ih i 2000-ih bila je *e-gold*, koju je kreirala i kontrolisala istoimena kompanija sa sjedištem na Floridi. *E-gold*, kompanija je u osnovi funkcionisala kao digitalni kupac zlata. Njeni kupci ili korisnici poslali bi svoj stari nakit, sitnice i kovanice u skladište *E-golda*, primajući digitalno „e-zlato“ - jedinice valute

denominirane u uncima zlata. Korisnici *e-golda* tada su mogli trgovati sa drugim korisnicima, unovčiti novce za fizičko zlato ili zamijeniti svoje e-zlato za američke dolare.

Na vrhuncu, sredinom 2000-ih, *e-gold* je imao milione aktivnih računa i obrađivao je milijarde dolara transakcijama godišnje. Nažalost, relativno jednostavni sigurnosni protokoli *e-golda* učinili su ga popularnim metom za hakere i prevare sa krađom identiteta, ostavljajući korisnicima financijske gubitke. I sredinom 2000-ih, veliki deo transakcionih aktivnosti *e-golda* bio je pravno sumnjiv - njegove utvrđene politike poštovanja zakona učinile su ga privlačnim za pranje novca. Platforma se suočila sa sve većim pravnim pritiskom sredinom i krajem 2000-ih, a konačno je prestala s radom 2009. godine.

Bitcoin i savremeni bum kriptovaluta

Bitcoin slovi kao prva moderna kripto valuta - prvo javno korišćeno sredstvo razmjene za kombinovanje decentralizirane kontrole, anonimnosti korisnika, vođenja evidencije putem *blockchain*-a i ugrađene limitirane količine. Prvi put je objavljen u *white paper*-u 2008. godine, koju je objavio Satoshi Nakamoto, pseudonimna osoba ili grupa.

Početkom 2009. Nakamoto je objavio Bitcoin za javnost, a grupa oduševljenih pristalica počela je razmjenu i rudarstvo valute. Krajem 2010. godine, počela se pojavljivati prva od desetak sličnih kriptovaluta - uključujući popularnu alternativu poput Litecoin-a. Prve javne razmjene Bitcoin-a pojavile su u datom periodu.

Krajem 2012. godine WordPress je postao prvi veliki trgovac koji je prihvatio plaćanje u Bitcoin-u. Slijedili su drugi, uključujući Newegg.com (*online* trgovac elektronikom), Expedia i Microsoft. Desetine trgovaca sada najpopularniju kripto valutu u svijetu vide kao legitiman način plaćanja. A nove aplikacije za kripto valute koriste se uz impresivnu učestanost.

Iako je malo kripto valuta osim Bitcoina široko prihvaćeno za plaćanje trgovaca, sve aktivnije razmjene omogućavaju vlasnicima da ih razmjenjuju u valute Bitcoin ili *fiat* valute - pružajući kritičnu likvidnost i fleksibilnost. Od kraja 2010. godine, veliki poslovni i institucionalni investitori pažljivo su posmatrali i ono što nazivaju „kripto-prostorom“. Facebook-ov usko zaštićeni LIBRA projekt mogao bi biti prva istinska kriptovaluta, alternativa fiatnim valutama.

Prednosti kriptovaluta

1. Ugrađena ograničenost može podržati vrijednost

Većina kripto valuta ima limitiranu količine - izvorni kod određuje koliko jedinica ikada može postojati. Na taj način su kripto valute više poput plemenitih metala nego *fiat* valuta. Kao i plemeniti metali, oni mogu ponuditi zaštitu od inflacije koja nije dostupna korisnicima fiatnih valuta.

2. Slabljenje državnog monopola

Kripto valute nude pouzdano sredstvo razmjene izvan direktne kontrole nacionalnih banaka, poput američkih Federalnih rezervi i Evropske centralne banke. Ovo je posebno privlačno za ljude koji se brinu da će kvantitativno ublažavanje („štampanje novca“ centralnih banaka kupovinom državnih obveznica) i drugi oblici labave monetarne politike, poput skoro nultih među-bankarskih kamatnih stopa, dovesti do dugoročne ekonomske nestabilnost.

Dugoročno gledano, mnogi ekonomisti i politikolozi očekuju da svjetske vlade zajednički optimizuju kripto valute ili barem uključe aspekte kripto valute (poput ugrađenih protokola nedostatka i provjere autentičnosti) u *fiat* valute. To bi potencijalno moglo zadovoljiti brige zagovornika kriptovaluta zbog inflatorne prirode fiatnih valuta i inherentne nesigurnosti fizičke gotovine.

3. Samoinicijativne zajednice koje samoinicijativno djeluju

Rudarstvo je ugrađeni mehanizam kontrole kvaliteta i rada za kripto valute. Budući da su plaćeni za svoj trud, rudari imaju finansijski ulog u čuvanju tačnih, ažurnih evidencija o transakcijama - čime se obezbeđuje integritet sistema i vrijednost valute.

4. Robustna zaštita privatnosti

Privatnost i anonimnost bili su glavna briga za rane zagovornike kriptovalute, a ostaju takvi i danas. Mnogi korisnici kripto valute koriste pseudonime nepovezane s bilo kojim informacijama, računima ili pohranjenim podacima koji bi ih mogli prepoznati. Iako je sofisticiranim članovima zajednice moguće zaključiti identitet korisnika, novije kripto valute (post-bitcoin) imaju dodatnu zaštitu koja to znatno otežava.

5. Teže je institucijama da naplate finansijsku nadoknadu

U represivnim državama vlade mogu lako zamrznuti ili iskoristiti domaće bankovne račune ili preokrenuti transakcije u lokalnoj valuti. Ovo posebno zabrinjava u autokratskim zemljama.

Za razliku od *fiat* valuta koje podržavaju centralne banke, kripto valute su gotovo imune od autoritarnih vlastodržaca. Sredstva za kripto valute i evidencije transakcija čuvaju se na brojnim lokacijama širom svijeta, zbog čega je državna kontrola - čak i ako se pretpostavlja međunarodna saradnja - krajnje nepraktična. Možda je previše pojednostavljenje, ali korišćenje kripto valute je dijelom kao pristup teoretski neograničenom broju *offshore* bankovnih računa.

Decentralizacija je problematična za vlade koje su navikle da koriste finansijske poluge kako bi problematične elite držale pod kontrolom. Krajem 2017. godine CoinTelegraph izvijestio je o multinacionalnoj inicijativi za kriptovalute pod vođstvom ruske vlade. Ako bude uspješna, inicijativa bi imala dva ishoda: slabljenje dominacije američkog dolara kao *de facto* svjetskog sredstva razmjene i omogućavanje vladama učesnicama čvršće kontrole nad sve obimnijim i vrijednijim zalihama kriptovaluta

6. Jeftinije od tradicionalnih elektroskih transakcija

Koncept *blockchain*-a, privatnih ključeva i novčanika efikasno rješava problem dvostrukog trošenja, osiguravajući da nove kripto valute ne zloupotrebljavaju tehnološki pametni prevaranti sposobni da dupliciraju digitalna sredstva. Sigurnosne karakteristike kriptovaluta također uklanjaju potrebu za trećim procesorima plaćanja - poput Visa ili PayPal – koji treba da potvrde svaku elektronsku finansijsku transakciju.

S druge strane, to eliminiše potrebu za obveznim naknadama za transakcije kako bi podržali rad tih procesora plaćanja - budući da rudari, ekvivalent kriptovalute platnih procesora, za svoj rad, osim neobaveznih naknada za transakcije, zarađuju i nove valutne jedinice. Naknade za transakcije kripto valute uglavnom su manje od 1% vrijednosti transakcije, nasuprot 1,5% do 3% za procesore plaćanja kreditnom karticom i PayPal.

7. Manji broj prepreka i troškova za međunarodne transakcije

Kripto valute ne tretiraju međunarodne transakcije drugačije od domaćih transakcija. Transakcije su besplatne ili dolaze s nominalnom naknadom za transakciju, bez obzira gdje se pošiljalac i primalac nalaze. To je velika prednost u odnosu na međunarodne transakcije koje uključuju *fiat* valutu, a koje gotovo uvijek imaju posebne naknade koje se ne primjenjuju na domaće transakcije - poput međunarodnih kreditnih kartica ili naknada za bankomate. A direktni međunarodni novčani transferi mogu biti skupi, s naknadama koje ponekad prelaze 10% ili 15% od prenesenog iznosa.

Nedostaci kriptovaluta

1. Nedostatak propisa olakšava aktivnosti crnog tržišta

Vjerovatno je najveći nedostatak i regulatorna zabrinutost oko kripto-valuta njihova sposobnost da olakšaju nelegalne aktivnosti. Mnoge *online* transakcije na sivom i crnom tržištu denominirane su u Bitcoin-u i drugim kripto valutama. Na primjer, zloglasna *dark* web lokacija Silk Road koristila je Bitcoin da bi olakšala nelegalnu kupovinu droge i druge nezakonite aktivnosti prije nego što je zatvorena u 2014. god. Kriptovalute su također sve popularnije oruđe za pranje novca - paralelno sa nezakonito dobijenim novcem putem „čistog“ posrednika kako bi se prikrilo izvor.

Iste prednosti koje vladama kripto valutama otežavaju pribavljanje i praćenje omogućavaju kriminalcima da djeluju relativno lako - premda, treba napomenuti, osnivač Silk Road-a je sada iza rešetaka, zahvaljujući dugogodišnjoj istrazi DEA.

2. Potencijal za utaju poreza u nekim nadležnostima

Budući da kripto valute ne regulišu nacionalne vlade i obično postoje izvan njihove direktne kontrole, prirodno privlače utajivače poreza. Mnogi manji poslodavci plaćaju zaposlene u Bitcoin-ima i drugim kripto valutama kako bi izbjegli odgovornost za plaćanje poreza ili pomogli svojim radnicima da izbjegnu obvezu poreza na dohodak, dok *online* prodavači često prihvataju kriptovalute kako bi izbjegli obveze od prodaje i poreza na dohodak.

Američka vlada primjenjuje iste smjernice za oporezivanje na sve isplate kriptovaluta od strane američkih osoba i poduzeća. Međutim, mnoge zemlje nemaju takvu politiku. A urođena anonimnost kriptovaluta čini teškim za zapažanje poreznih kršenja zakona, posebno onih koja uključuju pseudonimne online prodavače (za razliku od poslodavaca koji na W-2 stavljaju pravo ime radnika, što ukazuje na njihovu Bitcoin zaradu).

3. Potencijal za finansijski gubitak zbog gubitka podataka

Rani zagovornici kriptovalute vjerovali su da će, ako se pravilno osiguraju, digitalne alternativne valute obećati potporu odlučnom otklonu od fizičkog novca, kojeg smatraju nesavršenim i suštinski rizičnim. Pod pretpostavkom da se praktično ne može provaliti izvorni kod, neprobojni protokoli za provjeru autentičnosti (ključevi) i odgovarajuće hakerske odbrane (kojih je nedostajalo Mt. Goxu), sigurnije je skladištiti novac u *cloud*-u ili čak fizičkom uređaju za čuvanje podataka nego u gotovini.

Međutim, to pretpostavlja da korisnici kriptovalute preduzimaju odgovarajuće mjere opreza kako bi izbjegli gubitak podataka. Na primjer, korisnici koji čuvaju svoje privatne ključeve na pojedinačnim fizičkim uređajima za čuvanje, trpe nepovratnu finansijsku štetu kada se uređaj izgubi ili ukrade. Čak se i korisnici koji čuvaju svoje podatke pomoću jedne usluge *cloud*-a mogu suočiti sa gubitkom ako je server fizički oštećen ili isključen iz globalnog interneta (mogućnost za servere koji se nalaze u zemljama s uskom internet kontrolom, poput Kine).

4. Potencijal za visoku volatilnost i manipulaciju cijenama

Mnoge kripto valute imaju određeni broj jedinica koncentriranih od individualaca (često stvaraoci valuta i bliski saradnici). Ovi vlasnici efikasno kontrolišu zalihe tih valuta, čineći ih osjetljivim na divlje promjene vrijednosti i direktu manipulaciju. Međutim, čak i kripto valute kojima se često trguje podložne su kolebljivosti cijena: vrijednost Bitcoina udvostručila se nekoliko puta u 2017. godini, a zatim prepolovila tokom prvih nekoliko sedmica 2018. godine.

5. Često se ne može razmenjivati za *fiat* valutu

Generalno, samo najpopularnije kripto valute - one s najvećom tržišnom kapitalizacijom u dolarima - imaju namjenske *online* berze koje dopuštaju direktnu razmjenu za *fiat* valute. Ostali nemaju namjenske *online* razmjene i stoga ih nije moguće direktno zamijeniti za *fiat* valute. Umjesto toga, korisnici ih moraju pretvoriti u češće korištene kripto valute, poput Bitcoina, prije konverzije u *fiat* valute. Povećavanjem troškova transakcija smanjuje se potražnja, a samim tim i vrijednost za neke manje korišćene kripto valute.

6. Ograničenost na *No Facility for Chargebacks or Refunds*

Iako su rudari kripto valute posluži kao kvazi posrednici za transakcije s kripto valutama, oni nisu odgovorni za arbitražu sporova između ugovornih strana. Zapravo, koncept takvog arbitra krši decentralizovani impuls u srcu savremene filozofije kriptovaluta. To znači da ne postoji neko kome se žali, ako dođe do prevare u transakciji s kripto valutama. Npr. plaća se unaprijed

za stavku koja nikad ne stigne. Iako neke novije kripto valute pokušavaju riješiti problem povraćaja novca, rješenja ostaju nepotpuna i uglavnom nedokazana.

Za razliku od toga, tradicionalni procesori plaćanja i mreže kreditnih kartica poput Visa, MasterCard i PayPal često stupaju u rješavanja sporova između kupca i prodavača. Pravila povrata ili vraćanja novca posebno su dizajnirana kako bi se spriječile prevare prodavača.

7. Nepovoljni uticaji rudarstva kriptovaluta na životnu okolinu

Rudarenje kriptovaluta vrlo je energetski intenzivno. Najveći krivac je Bitcoin, najpopularnija svjetska kriptovaluta. Prema procjenama rudarstvo Bitcoin-a troši više struje nego cijela Danska. Neki od najvećih svjetskih rudnika Bitcoin-a su smješteni u zemljama bogatim ugljem poput Kine.

Iako često negiraju, stručnjaci za kriptovalute priznaju da rudarstvo predstavlja ozbiljnu prijetnju po okolinu pri trenutnim stopama rasta. Tri moguća kratkoročna i srednjoročna rješenja su:

- Snižavanje cijene Bitcoina kako bi rudarstvo učinilo manje unosnim, što bi vjerovatno zahtijevalo usklađeno uplitanje u ono što je do sada predstavljalo *laissez-faire* tržište
- Smanjivanje nagrade za rudarstvo brže od trenutno predviđene stope (prepolovljava se svake četiri godine)
- Prelazak na algoritam koji zahtjeva manje energije

Dugoročno, najbolje rješenje je napajanje rudnika kriptovaluta s izvorima energije bez ugljenika, uz propratne podsticaje za premještanje rudnika u države s niskim udjelom ugljenika poput Kostarike i Holandije.

Primjeri kripto valute

Upotreba kriptovalute eksplodirala je od izdavanja Bitcoina. Iako tačni brojevi aktivnih valuta variraju, a vrijednosti pojedinih valuta izrazito su nestabilne, ukupna tržišna vrijednost svih aktivnih kripto valuta uglavnom se povećava. U bilo kojem trenutku stotine kriptovaluta aktivno trguju. Ovdje opisane kripto valute obilježene su stabilnim prihvatanjem, robustnom korisničkom aktivnošću i relativno velikom tržišnom kapitalizacijom (većom od 10 miliona dolara, u većini slučajeva, mada procjene mogu biti podložne promjenama):

1. Bitcoin

Bitcoin je najveća svjetska kripto valuta koja se najčešće koristi. Bitcoin ima programirano ograničenu količinu od 21 miliona Bitcoina.

Bitcoin se sve više posmatra kao legitimno sredstvo razmjene. Mnoge poznate kompanije prihvataju Bitcoin plaćanja, iako je većina partnera za pretvaranje Bitcoina u američke dolare prije nego što dobiju sredstva.

2. Litecoin

Objavljen 2011. godine, Litecoin koristi istu osnovnu strukturu kao Bitcoin. Ključne razlike uključuju veće programirano ograničenje (84 miliona jedinica) i kraće vrijeme stvaranja blok-lanca (dvije i po minute). Algoritam šifrovanja takođe je malo drugačiji. Litecoin je često druga ili treća najpopularnija kriptovaluta po tržišnoj kapitalizaciji.

3. Ripple

Objavljen 2012. godine, Ripple je poznat po sistemu „konsenzus knjige“ koji dramatično ubrzava potvrđivanje transakcija i vremena stvaranja *blokchain*-a, nema formalnog ciljanog vremena, ali prosjek je svakih nekoliko sekundi. Ripple se takođe lakše konvertuje u odnosu na ostale kripto valute, uz internu razmjenu valuta koja Ripple jedinice može pretvoriti u američke dolare, jene, eure i druge uobičajene valute.

Međutim, kritičari su primijetili da su Ripple-jeva mreža i kod podložniji manipulacijama od strane sofisticiranih hakera i možda neće nuditi iste zaštite anonimnosti kao kripto valute koje zasnovane na Bitcoin-u

4. Ethereum

Pokrenut 2015. godine, Ethereum donosi značajna poboljšanja u osnovnoj arhitekturi Bitcoina. Konkretno, koristi „pametne ugovore“ koji nameću izvršavanje određene transakcije, primorava strane da poštuju svoje sporazume i sadrže mehanizme za povraćaj novca ako jedna strana prekrši sporazum. Iako su "pametni ugovori" važan korak u pravcu rješavanja nedostatka povrata i povrata u kripto valutama, ostaje da se vidi da li su dovoljni za potpuno rješavanje problema.

5. Dogecoin

Dogecoin, označen njegovom odmah prepoznatljivom maskotom Shiba Inu, varijacija je na temu Litecoin-a. Ima kraće vrijeme stvaranja blok-lanaca (jedan minut) i znatno veći broj kovanica u optjecaju - cilj kreatora da se do do jula 2015. godine izrudari 100 milijardi jedinica je ispunjen, a ograničenje je da se količina od 5,2 milijardi jedinica može izrudariti svake godine nakon toga, bez poznatog limita ukupne količine. Dogecoin je stoga zapažen kao eksperiment u „inflatornoj kripto valuti“, a stručnjaci pažljivo posmatraju kako se njegova dugoročna vrijednost razlikuje od ostalih kriptovaluta.

6. Coinye

Coinye, polu-nefunkcionalnu kripto valutu, vrijedi spomenuti zbog njene bizarne prošlosti. Coinye je razvijen pod originalnim nazivom "Coinye West" 2013. godine, a identifikovana je nepogrešiva sličnost sa hip-hop superzvijezdom Kanye West-om. Ubrzo prije objavljivanja Coinye-a, početkom 2014. godine, West-ov pravni tim uočio je postojanje valute i poslao njenim autorima opomenu o prekidu daljih aktivnosti.

Da bi izbjegli zakonsku tužbu, tvorci su izbacili „West“ iz naziva, promijenili logotip u hibrid „pola čovjeka, pola riba“ koji podsjeća na West-a (referenca na *South Park* epizodu u kojoj se potencira ego West-a) i pustili Coinye-a po planu. S obzirom na i ironični humor oko njegovog objavljivanja, valuta je privukla kult koji je uslijedio među ljubiteljima kripto valuta. West-ov pravni tim podnio je tužbu, primoravši tvorce da prodaju svoje vlasništvo i zatvore web sajt.

Iako je Coinye-ova *peer-to-peer* mreža i dalje aktivna i tehnički je još uvijek moguće rudariti valutu, transferi s lica na lice i rudarske aktivnosti su propadale do te mjere da je Coinye u osnovi bezvrijedna valuta.