Шта је биткоин и шта нам доноси

ДА ЛИ ЈЕ БУДУЋНОСТ КРЕНУЛА КА НАМА

Пише **Томислав УНКАШЕВИЋ**

Дугогодишњи раст вредности дигиталне валуте биткоин изазвао је велико интересовање јавности за ту тему, као и поплаву информација у вези са дигиталним валутама. Као и за сваку нову технологију, терминологија најчешће није формирана и уједначена те се појављују непрецизности различите врсте и значаја, мада, генерално гледано, за ширу јавност та шароликост нема превелики значај. Тако се, на пример, термин биткоин користи и као назив за дигиталну валуту и као назив технологије на којој та валута почива. Такође неретко се и термин блокчејн (Blockchain) користи као синоним за биткоин технологију, а та техника је позната и развијена много пре дефинисања биткоин валуте. За читаоце магазина „Одбрана" доносимо одговор на основно питање шта је биткоин, као и покушај наговештаја онога што нам доноси.

Интересовање за стварање дигиталне валуте погодне за употребу у трговању у мрежном окружењу јавило се још пре нешто више од четрдесет година. Једна од основних карактеристика финансијских система је да процес емисије валута, исправности и поузданости трговања почива на контролним механизмима које спроводе треће стране од поверења. У основи треће стране од поверења у случају класичних валута представљају емисиона тела која управљају емисијом валуте и банке као гаранти валидности трансакција и плаћања.

Основна замисао креирања дигиталних валута је елиминација трећих страна од поверења тако да емитовање јединица валуте буде децентрализовано, а трговање директно. Поред децентрализације, трговање мора бити анонимно и поуздано, трансакције непорециве, монопол на емисију валута, организациони или индивидуални – неостварив. Систем би почивао на формално доказивим чињеницама о својим карактеристикама те би поверење у дефинисану валуту било засновано на доказивим чињеницама, а не на репутацији и снази емитера одређене валуте. Услови за то су се стекли открићем асиметричне криптографије, али је прошло доста времена до реализације жељених концепата и појаве оперативно употребљиве дигиталне валуте биткоин 2009. године.

Систем за креирање, употребу и управљање дигиталном валутом биткоин описан је у раду „Bitcoin: A Peer-to-Peer Electronic Cash System", чији је аутор потписан као Сатоши Накамото. До данас није утврђено ко стоји иза тог псеудонима, чак ни да ли је у питању појединац или група аутора. Да бисмо описали биткоин технологију и процесе који стоје иза биткоин валуте биће нам неопходно познавање неких криптографских механизама, њихова намена и функција.

КРИПТОГРАФСКИ МЕХАНИЗМИ

Све до половине седамдесетих година прошлог века криптографски алгоритми били су симетрични у смислу да су учесници у заштићеној комуникацији користили исти криптографски кључ за шифровање и дешифровање. На предајној страни кључ је коришћен за шифровање, а на пријемној за дешифровање. Средином седамдесетих година прошлог века, тачније 1976, Дифи и Хелман открили су асиметричне криптографске системе, код којих се разликовати кључеви користе за шифровање и дешифровање. Отуда и потиче назив – асиметрични. Есенцијална особина ових кључева је да познавањем једног од њих није могу-

ће добити онај други. Кључ за шифровање означава се са *p*, а кључ за дешифровање са *d*, јавни и тајни кључ респективно. Зашто су ови системи значајни? Како из једног кључа није могуће добити други, сваки учесник у систему може свој кључ за шифровање и алгоритам шифровања обзнанити јавно. Потом свако може да му пошаље шифровану поруку, али ту поруку може да дешифрује само он јер једино он поседује одговарајући кључ за дешифровање. Откриће ових система унело је праву револуцију у криптографију и, поред других постигнућа, омогућило је проверу порекла и интегритета података, као и дефинисање идентитета субјеката у дигиталном свету људи и уређаја.

Декларисање порекла електронског податка/документа реализује се процедуром електронског потписа, а провера интегритета и порекла документа процедуром верификације електронског потписа. Наведене процедуре заснивају се на одговарајућем асиметричним криптографским алгоритмима. Назовимо актере овог процеса Алиса и Боб. Алиса поседује пар асиметричних кључева (*pA*, *dA*) одговарајућих за процедуре генерисања електронског потписа и његове верификације и жели да Бобу пошаље поруку *m,* али тако да се Боб може уверити, по пријему, да је поруку послала Алиса и да порука на преносном путу није промењена. Алиса креира дигитални потпис поруке *m* применом процедуре потписа: *Sign*(*m, dA*) = *sig*(*m*) и Бобу шаље поруку (*m, sig*(*m*), *pA*). Боб спроводи проверу електронског потписа за добијену поруку, *Verify*(*m, sig*(*m*), *pA*) и ако добије резултат да је верификација успешна, зна да порука потиче од Алисе, јер је верификована њеним јавним кључем, кључем за проверу електронског потписа и да на преносном путу порука није измењена. Бобово уверење у вези са пореклом и интегритетом добијене поруке почива на математичкој чињеници да је вероватноћа успешне верификације електронског потписа неодговарајућим јавним кључем занемарљиво мала. Последица ове чињенице је да алгоритам за електронски потпис и њему одговарајући пар кључева (*p*, *d*) представљају јединствен скуп података и могу послужити за креирање идентитета субјеката у електронском свету. Свој идентитет Алиса доказује Бобу његовом верификацијом њеног електронског потписа за договорени документ. То је основни принцип, али ту има још доста техничких детаља чија разматрања нису предмет овог текста.

Основна замисао креирања дигиталних валута је елиминација трећих страна од поверења, тако да емитовање јединица валуте буде децентрализовано, а трговање директно. Поред децентрализације, трговање мора бити анонимно и поуздано, трансакције непорециве, монопол на емисију валута, организациони или индивидуални – неостварив.

Процедуре за креирање и верификацију дигиталног потписа могу користити и такозване хеш (hash) функције, које податак произвољне дужине у битима пресликавају у податак фиксне дужине у битима. Хеш функција се уобичајено означава са *H*, трансформација податка *m*, а добијање његове хеш вредности *hm* са *H*(*m*) = *hm*.

Употребна вредност хеш функција лежи у чињеници да је вероватноћа реконструкције *m* на основу познавања *hm* безначајна, те се вредност *hm* може сматрати дигиталним отиском податка *m*.

Биткоин (B) представља прву дигиталну валуту која је обезбедила анонимност учесницима у трансакцијама и ослободила се присуства треће стране од поверења у њима. То је постигнуто, као што смо напоменули, употребом јавних кључева као идентитета у трансакцијама. Свака трансакција састоји се од две листе, улаза (Input) и излаза (Output). Сваки излаз садржи идентитет/адресу, јавни кључ, коме је вредност трансакције намењена.

Илуструјмо начин функционисања следећим примером:

Претпоставимо да је неко раније Алиси платио 3B а да она жели да плати неку услугу Бобу 2B. Трансакција којом је Алиса добила новац има неку идентификацију, рецимо 3. У тренутку када жели да плати Бобу, Алиса креира нову трансакцију са идентификацијом, рецимо 4, којој је улаз излаз са индексом 0 трансакције 3 и дигитално потписује тај улаз својим тајним кључем. Лако се проверава да ли Алиса има право да користи тај излаз трансакције 3 јер он садржи јавни кључ којим се верификује Алисин дигитални потпис овог улаза. Сада Алиса подели своје власништво над 3B на два излаза, један адресиран на Боба и други адресиран на себе и овај део представља кусур од употребљеног улаза. Основно правило приликом дефинисања трансакције је да збир улазних трансакција не сме бити већи од збира излазних трансакција. Тако се спречава трошење непостојећег новца, нема кредита. Пример је илустрован сликом 1.

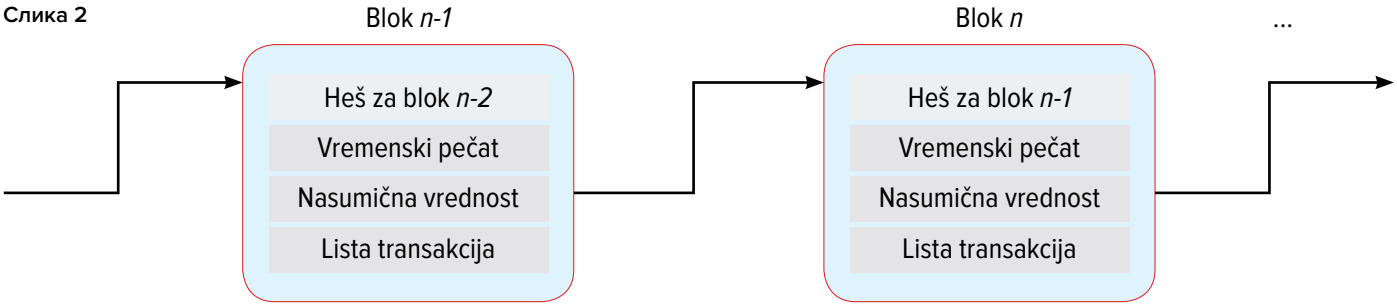
У систему постоји листа трансакција која садржи све трансакци-

Слика 1

Transakcija 3	
Ulaz: Trans. 1, Izlaz 1 El. Potpis: Potpisao X	Iznos: 10B Za: javni ključ Z
Ulaz: Trans. 2, Izlaz 0 El. Potpis: Potpisao Y	Iznos: 3B Za: javni ključ Alisa

Transakcija 4	
Ulaz: Trans. 3, Izlaz 1 El. Potpis: Potpis Alisa	Iznos: 2B Za: javni ključ Bob
	Iznos: 1B Za: javni ključ Alisa

Слика 2



је чији износ није потрошен, UTXO (Unspent Transaction Output). Валидност генерисане трансакције проверава се тако што се провери да се улазне трансакције налазе на UTXO листи, да су генерисани електронски потписи исправни и да је збир улазних трансакција већи или једнак од збира излазних трансакција. Но процес реализације трансакције још није готов. Трансакција се сматра реализованом тек када буде унета у главну књигу (Ledger). Копије главне књиге као и UTXO налазе се на хиљадама рачунара који партиципирају у биткоин мрежи. Садржај главне књиге чине блокови трансакција. Блокови главне књиге имају свој специфичан формат и начин конструкције. Сви чланови мреже који то желе могу покушати да конструишу валидан блок трансакција. Припадник мреже који покушава да конструише валидан блок започиње процес тако што из UTXO одабере скуп трансакција над којима ће покушати да конструише валидан блок за упис у главну књигу. Припадници биткоин мреже који се баве покушајима конструкције блокова називају се рударима (miners), а сам процес рударење (mining). На почетку рудар конструише заглавље блока (BlockHeader), које поред фиксираних података садржи хеш вредност последњег блока из копије главне књиге коју рудар поседује и један насумице одабран број (nonce). За тако формирано заглавље израчуна његову хеш вредност и ако је добијена вредност већа од унапред дефинисане вредности, фактор тежине, бира нову насумичну вредност и понавља поступак. Ако је добијена вредност мања од тежинског фактора, тада обзнањује свој блок осталим члановима. Када неки припадник биткоин заједнице добије блок који је кандидат за упис у главну књигу прво проверава његову исправност, електронске потписе, баланс трансакција, испуњеност услова за фактор тежине и друго. Приликом рачунања хеш вредности онај који проверава блок користи своју верзију главне књиге. Ако је провера неуспешна, блок се одбацује као неисправан. Ако је провера успешна, блок се уписује у главну књигу а онај ко га је конструисао добија награду од 6.25B према данашњем вредновању. Периодично ова вредност се преполовљује. Уланчавање је приказано на слици 2.

Награда за проналажење блока један је од мотива за рударење и начин за емисију биткоина. Други начин добијања биткоина је награда рудару за одабир неке трансакције. Наиме, када неко жели да стимулише рударе да одаберу његову трансакцију за блок који ће генерисати, он у својој трансакцији остави збирни излаз мањим од збирног улаза. Тада разлика у балансу улаза и излаза припада рудару који обради ту трансакцију. Мотив креатора трансакције је да његова трансакција буде што пре обрађена. По уласку блока у главну књигу трансакције садржане у том блоку сматрају се реализованим. На први поглед изгледа да је лако креирати валидне блокове и емитовати биткоине, али то је само привид. Данас сви рудари на свету морају да обраде преко 1.021 блокова кандидата пре него што нађу један исправан.

Анонимност, толико жељена у финансијским трансакцијама, са собом носи и етичку дилему јер омогућава промет нелегално стеченог новца и отежава борбу против прања новца

Може се десити да се у биткоин мрежи појаве два различита исправна кандидата за упис у главну књигу у исто време. Биткоин технологија поседује механизме за разрешење те ситуације, али њихов опис је превише обиман и превазилази обим и намену овог текста. Грубо говорећи, прати се раст сваке од инкарнација главне књиге и када једна постане дужа од друге, дужи низ блокова се уписује у главну књигу, а краћи низ блокова се одбацује као неисправан.

Ова техника уланчавања блокова (BlockChain) у формирању главне књиге и чињеница да главна књига постоји у великом броју примерака на различитим местима у оквиру биткоин мреже онемогућава двоструко трошење, ситуацију да неко употреби трансакцију биткоина која му је намењена за плаћање два пута. Наиме, једном употребљена и реализована трансакција налази се у главној књизи са подацима када је потрошена. Да би је поново користио, бивши власник мора да поседује рачунарску снагу да реорганизује и фалсификује главну књигу како би ту трансакцију поново превео у UTXO. Ако је та трансакција у последњем уписаном блоку, онда му за то треба 1.021 покушаја, што је еквивалент целокупне светске биткоин заједнице. Што је предметна трансакција даље од краја главне књиге, то му је потребна све већа рачунарска снага и њен раст је експоненцијалан. Децентрализовано

проверавање и генерисање блокова и њихов упис у дистрибуиране примерке главне књиге представљају вид децентрализованог постизања консензуса о стању главне књиге и спроведеним трансакцијама.

Систем је тако реализован да је величина блока ограничена на 1MB, а укупан број емитованих биткоина на 21 милион биткоина.

ШТА НАМ ДОНОСИ БИТКОИН

Са појавом електронског потписа многи истраживачи су сањали сан о стварању децентрализоване дигиталне валуте и анонимности у тим процесима. После нешто више од 25 година тај сан се остварио појавом биткоина. Настао је поуздан финансијски систем у којем учесници остају анонимни и нема утицаја трећих страна од поверења. Трансакције се реализују на поуздан начин, за шта гарантују примењени криптографски механизми, немогућност фалсификовања главне књиге и дистрибуирани консензус. Јединице валуте могу се емитовати једино радом, рударењем, и што је више биткоина у оптицају, то је емитовање нове јединице теже. Треба уложити више рада, односно енергије. Са друге стране тежински фактор за креирање блокова се динамички мења у зависности од просечне брзине појављивања нових блокова. Систем је конципиран тако да вредност тежинског фактора омогућава појављивање нових блокова у просеку на десет минута. То значи да ће се просечно чекати на реализацију трансакције најмање десет минута, што у неким финансијским трансакцијама представља недозвољено време.

КАДА СЕ ПРЕДНОСТ АНОНИМНОСТИ ПРЕТВОРИ У СУПРОТНОСТ

Још једна од значајних карактеристика трансакција у биткоин окружењу је њихова иреверзибилност. Када једном за неку робу или услуге платите биткоинима, не постоји начин да их у случају рекламације повратите. Та чињеница отвара врата за преваре на овом тржишту где се жељена особина анонимности претвара у своју супротност јер онемогућава детектовање идентитета преваранта и примену правних механизама против преваре. Наравно, поступак праћења токова биткоина није немогућ, али захтева доста техничких средстава, знања и времена па проналажење кривца није увек исплативо.

Када једном за неку робу или услуге платите биткоинима, не постоји начин их да у случају рекламације повратите. Та чињеница отвара врата за преваре на овом тржишту где се жељена особина анонимности претвара у своју супротност јер онемогућава детектовање идентитета преваранта и примену правних механизама против преваре. Наравно, поступак праћења токова биткоина није немогућ, али захтева доста техничких средстава, знања и времена, па проналажење кривца није увек исплативо.

Анонимност, толико жељена у финансијским трансакцијама, са собом носи и етичку дилему јер омогућава промет нелегално стеченог новца и отежава борбу против прања новца.

Биткоин као технологија одиграо је генеричку улогу у стварању дигиталних валута. Коришћењем идеја насталих у биткоину са другачијим техничким решењима и финесама у организацији и имплементацији настале су многе дигиталне валуте. Биткоин је постао доминантна валута за конверзију класичних валута у дигиталне валуте и обратно. И поред тога постоји још доста простора, и у обиму и у начину употребе ове валуте.

БУДУЋНОСТ БИТКОИНА

О томе каква будућност очекује биткоин, мишљења су подељена.

Једна група економиста и мислилаца поздравља појаву биткоин валуте као прве децентрализоване валуте која обезбеђује анонимност, директно трговање без посредника, као и онемогућавање манипулације емисијом новчаних јединица. Са друге стране постоје мишљења да је дигитална валута без централне контроле темпирана бомба и да је читав пројекат темпиран и промовисан као још један финансијски мехур у недостатку производних ефеката на потребној брзини повећања профита и промета. Другим речима, профит у финансијској сфери је и већи и бржи него у производној и стога се капитал сели ка финансијама, те производња не прати пропорционално раст финансијског капитала. Такође, постоји известан број теоретичара који тврде да је стварање и употреба дигиталног новца пут ка елиминацији класичних валута. Потпуни прелазак на дигиталне валуте они виде као стварање услова за потпуну контролу људи и стварање инструментализованог друштва.

Остаје питање како ће економија и финансије функционисати када се изрудари последњи биткоин, што се очекује до 2034. године... Чињеница која ће такође утицати на судбину биткоина је енормна потрошња енергије која се троши у процесу рударења. Процењује се да је годишња потрошња струје за рударење биткоина на нивоу 122 TWh, што је упоредиво са годишњом потрошњом у Аргентини, Холандији, Уједињеним Арапским Емиратима и Норвешкој појединачно. Како енергија постаје дефицитарна, није јасно како ће се та чињеница одразити на биткоин.

Свака од претходно набројаних ставки, а и неке непоменуте, могу бити предмет занимљиве дискусије. У сваком случају будућност је кренула ка нама. Отворимо очи да бисмо видели шта носи.