NFT

Mihael Petrinjak

6. siječnja 2024.

Sadržaj

1 Uvod

NFT je nedavno izazvao veliko komešanje na internetu. Koliko u svijetu novaca toliko i mišljenja ljudi. Radi se o pojmu srodnom kriptovalutama. Na neki način njihovo multimedijsko proširenje.

Kako bismo mogli razumjeti virtualizaciju vrijednosti proučit ćemo *blockchain* paradigmu te kako se NFT sustavi koriste njenim alatima. Na kraju će biti jasno da je to samo prva stranica u ekonomskoj i kulturološkoj evoluciji čovjeka.

2 Blockchain

Blockchain je dostupan svima. Funkcionira kao javni zapisnik u koji korisnici mogu napisati neki podatak. Glavna karakteristika je „nepromjenjivost" podataka nakon unosa.

2.1 Arhitektura

Blockchain je vezana lista podatkovnih struktura — **blokova** sa sadržajem podjeljenim u tri dijela:

- podaci
- hash prethodnog bloka
- hash

Podaci su u svijetu kriptovaluta, na primjer informacije o pošiljatelju, primatelju i količina novaca. Točno ono što opisuje transakcije.

hash je slika neke funkcije h za hashiranje čija praslika je sadržaj bloka bez te vrijednosti. Preciznije, hash $= h(\text{podaci} * \text{hash\_prethodnog\_bloka})$, gdje $*$ označava neki oblik konkatenacije teksta. Očito, argument funkcije može biti proizvoljan tekst. hash je neki dugačak niz bitova. Poznata implementacija je SHA256 čija kodomena su svi nizovi od 256 bitova. Nazovimo spomenute dijelove **hash, data, pbHash** radi lakoće pisanja.

Primjer 1. Neka su u lancu tri bloka start, b_2, b_3. U tablici 1 je prikazan njihov sadržaj. Pretpostavimo da netko želi retroaktivno promijeniti sadržaj u b_2. Blok će gotovo sigurno imati novi hash. Treći blok više ne pokazuje na svog prethodnika i time je lanac prekinut.

	start	b_2	b_3
data	abc	def	ghi
pbHash	000	h_1	h_2
hash	h_1	h_2	h_3

Tablica 1: Primjer lanca

	start	b_2	b_3
data	abc	bad	ghi
pbHash	000	h_1	h_2
hash	h_1	h_2'	h_3

Tablica 2: Promjena lanca

♢

2.2 Sigurnost

Postavlja se pitanje što sprječava nekoga da izmjeni sadržaj nekog bloka b_j i svih idućih blokova u lancu $(b_0, b_1, b_2, \ldots, b_j, \ldots, b_n)$ i tako *validira* laž. Sve što treba napraviti nakon promjene u bloku b_j je izračunati

$$\{\text{hash}_i = h(\text{data}_i * \text{hash}_{i-1}) : i \geq j\}$$

po redu od najmanjeg do najvećeg indeksa na kraju lanca. Uz snagu današnjih računala to se ne čini kao jako zahtjevan zadatak.

2.2.1 Hash funkcije

Ulaz algoritma je proizvoljan tekst, a povratna vrijednost neki dugalčak niz bitova. Za danu vrijednost *kriptografske* hash funkcije algoritamksi je jako skupo pronalaženje njene praslike. Do sad nije nađen pametniji način od pogađanja o kojoj se vrijednosti radi. Naime, za dva proizvoljna argumenta `String s1, s2` koji se razlikuju u samo jednom slovu, vrijednosti $h(s_1)$ i $h(s_2)$ su neusporedivo različite. Čini se kao da su vrijednosti nasumične.

2.2.2 Proof of work

Kako bi se iskoristila opisana svojstva, u svakom bloku se pojavljuje i *proof of work*. Nadograđeni izgled bloka, odnosno lanca prikazan je u tablici 3. hash se računa slično kao u primjeru 1: $h(\text{data} * \text{pbHash} * \text{POW})$. Vrijednosti h_i sada imaju svojstvo da je prvih k bitova jednako nuli. k ovisi o tome koliko želimo da bude skupo računanje POW. Promotrimo slučaj kada je $k = 30$. Vjerojatnost da je prvih 30 bitova od $h(\text{rand})$ za `String rand` nasumičan input jednako nuli je $1/2^{30} \approx 1/10^9$. Preciznije, ako funkcija $\text{start}_{30}(x)$ vraća prvih 30 bitova od x u binarnom zapisu duljine 256,

$$\mathbb{P}(\text{start}_{30}(h(\text{rand})) = 0) \approx 1/10^9.$$

To znači da je osoba koja je pronašla proof of work za dani blok morala proći kroz milijardu nasumičnih brojeva x i provjeravati traženo svojstvo $h(\text{data} * \text{pbHash} * x)$

Vratimo se sada na pokušaj prijevare opisan na početku poglavlja 2.2. Kako bi lanac nakon promjene u bloku j postao valjan potrebo je izračunati

$$\{\text{POW}_i : \text{start}_{30}(h(\text{data}_i * \text{hash}_{i-1} * \text{POW}_i)) = 0, i \geq j\}.$$

	start	b_2	b_3
data	abc	def	ghi
pbHash	000	h_1	h_2
POW	p_1	p_2	p_3
hash	h_1	h_2	h_3

Tablica 3: Primjer lanca s POW

Ako se radi lancu duljine n za takav pothvat potrebno je napraviti $n \cdot 10^9$ provjera za POW. Stare blokove u lancu jako je skupo mijenjati.

3 Kriptovalute

Sada imamo dovoljno resursa za dizajn sustava kriptovaluta. Neka je $\mathcal{K}$ skup korisnika. Radi jednostavnosti pretpostavimo da se za svaku transakciju dodaje novi blok u blockchain. data komponenta bloka je (pošiljatelj, primatelj, količina_novaca). Vrijednost novaca izražena je u izmišljenoj valuti. U stvarnosti postoji i digitalni potpis pošiljatelja, ali ovdje se nećemo baviti tom implementacijom. Dovoljno je reći da svaki korisnik može dodavati transakcije u kojima je on naveden kao pošiljatelj. Odnosno ne može u tuđe ime slati sebi novce. Svaki korisnik ima lokalnu kopiju cijelog lanca. Ako je $A \in \mathcal{K}$, onda s L_A označavamo lokalnu kopiju lanca od A.

3.1 Algoritam

Nakon dodavanja transakcije i hash-a prethodnog lanca radi se broadcast na mrežu sustava. Nakon toga netko mora izračunati proof of work tako da početni komad od hash vrijednosti bude jednak nuli. Tek tada će blok biti validan član lanca. Za to postoji skup $\mathcal{M}$ čiji članovi paralelno računaju POW.

Primjer 2. Ako Alice $A \in \mathcal{K}$ želi poslati 10 jedinica valute Bobu $B \in \mathcal{K}$ i zadnji blok u lancu ima hash jednak h_l, ona mora pripremiti blok b_{new} kako je prikazano u tablici 4. Tako pripravljeni podaci broadcastaju se svim članovima $\mathcal{M}$.

	...	b_l	b_{new}
data	...	...	(Alice, Bob, 10)
pbHash	...	h_{l-1}	h_l
POW	...	p_l	?
hash	...	h_l	?

Tablica 4: Priprema transakcije

♢

Nakon što jedan „miner” iz $\mathcal{M}$ nađe „dobitnu” kombinaciju, blok je potpun i izračunate su vrijednosti p_l i h_l. Takav potpuni blok broadcasta se svima iz $\mathcal{K}$. Za svakog $K \in \mathcal{K}$

L_K se nadograđuje s novim blokom. Tada je sustav opet u stanju u kojem svi posjeduju jednaku kopiju lanca.

3.2 Prijevara

Analizirajmo što sve treba napraviti netko tko se želi obogatiti varanjem drugih korisnika. Budući da si ne može slati novce u tuđe ime, može pokušati podmetnuti nekome krivotvorenu verziju lanca.

Primjer 3. Recimo da Alice $A \in \mathcal{K}$ želi prevariti Boba $B \in \mathcal{K}$ tako da manipuliranjem mreže samo njemu pošalje krivotvoreni potpuni blok b_k takav da `b_k.data == (Alice, Bob, 10)`. Potpuni znači da je ona izračunala POW i hash komponente. Iz Bobove perspektive algoritma sve je u redu. ♢

Problem nastaje u održavanju laži kroz vrijeme. Naime, sustav i dalje koriste svi ostali korisnici, ali u njihovim kopijama lanca ne postoji podmetnuti blok b_k. Kada neki drugi korisnik C napravi transakciju u L_C se na mejstu b_k nalazi b_{l+1} i takav lanac dolazi do Boba. Bobova lokalna kopija sada ima račvanje:

$$\text{blockchain} = b_0, \ldots, b_{l-1}, b_l, \begin{cases} b_k \\ b_{l+1} \end{cases}.$$

Kad bi u ovom trenutku Alice prestala održavati laž, zbog aktivnosti drugih korisnika, nakon nekog vremena bi lanac izgledao ovako:

$$\text{blockchain} = b_0, \ldots, b_{l-1}, b_l, \begin{cases} b_k \\ b_{l+1}, b_{l+2}, \ldots, b_{l+m} \end{cases}.$$

Algoritam prihvaćanja lanaca za dovoljno veliku m odbacuje verziju koja sadrži b_k. Dakle, u tom slućaju prijevara ne uspjeva. Ako želi zaraditi, Alice mora imati procesorsku moć veću od cijelog skupa $\mathcal{M}$.

Vidimo da prolaskom vremena stariji blokovi postaju vjerodostojni i u ono što je zapisano u njima možemo sa sigurnošću vjerovati.

4 NFT

NFT je kratica za *Non Fungable Token* što znači *nezamjenjivi* token. Za razliku od novčanica koje se smatraju *zamjenjivima*, NFT smatramo jedisntvenom jedinkom. Iz skupa svih novčanica od 10 eura nije bitno koju imamo dok god ona prikazuje broj 10. NFT jednom kad nastane definira sam svoju klasu ekvivalencije. Najčešće se radi o slikama, fotografijama, videozapisima i glazbi.

4.1 Integracija u blockchain

Sada se postavlja pitanje kako neku datoteku koju svatko može bez poteškoća kopirati i distribuirati učiniti jedinstvenom. U idealnom slučaju postoji servis za pohranu

kojem svi vjeruju. To znači da je uvijek i javno dostupan te da njegove poveznice zauvijek pokazuju na iste datoteke. U takvim uvjetima davanje vrijednosti multimedijskim „tokenima" svodi se na zapisivanje uređene četvorke `(ID_kupca, ID_prodavača, web_link_datoteke, novčani_iznos)` u blockchain. Za proizvoljnu osobu iz $\mathcal{K}$ koja prihvaća vrijednosni sustav, referencirana datoteka pripada navedenom kupcu i ima vrijednost `novčani_iznos` jer je toliko plačeno za njeno posjedovanje. Može se usporediti s kupovinom materijalne slike nekog slikara na aukciji. Ako netko drugi pokuša glumiti vlasnika i prodati NFT, jedino što potencijalni kupac mora provjeriti informacije je u blockchainu. SItuacija nije idealna i postoje mnoga otvorena pitanja. Kako, na primjer centralizirati servis za pohranu podataka za sve korisnike i spriječiti *link rot*, odnosno osigurati dugovječnost podataka?

5 Budućnost

Trenutno ne postoji jasna integracija NFT-jeva u zakone o autorskim pravima i vlasništvu. Zlonamjerna osoba lako može preko reference zapisane u blockchain-u pronaći datoteku i kopirati na svoje računalo. Ne postoji mehanizam za sprječavanje takvog ponašanja.

Dostupnost, sigurnost i decentralizaciju koje nudi blockchain doimaju se obečavajućima. Polagano se otvaraju vrata nove ekonomske organizacije svijeta. Nema razloga stati na multimediji. U blockchain bi se uz još malo nadogradnje moglo zapisati sve što čovjeku padne na pamet. Jedino teško pitanje je suglasnost korisnika sustava.