TERMINOLOGIJA ULANČANIH BLOKOVA NA HRVATSKOME JEZIKU

Andro Babić

DODATAK - TERMINOLOŠKA BAZA

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
address	character string used as an unique identifier denoting senders and receivers in a transaction	Addresses are unique identifiers that are used in a transaction on the blockchain to denote senders and recipients. An address is usually a public key or derived from a public key. - Bashir, Mastering blockchain These identities are called addresses, in Bitcoin jargon. You'll frequently hear the term address used in the context of Bitcoin and cryptocurrencies, and that's really just a hash of a public key. - Narayanan et al, Princeton Bitcoin book Their ownership of bitcoins was associated with digital addresses (long strings of numbers) that had two components: a public key that served as an address, and a private key that gave its owner exclusive access to any coins associated with That address. -Tapscott and Tapscott, Blockchain revolution	RT: Public key	adresa	niz znakova koji služe kao jedinstveni identifikator u označavanju pošiljatelja i primatelja unutar neke transakcije	Adrese su jedinstveni identifikatori koji se koriste u transakcijama u sustavu ulančanih blokova kako bi označili pošiljatelje i primatelje. Adresa je najčešće javni ključ ili proizlazi iz javnog ključa. - Bashir, Mastering blockchain Takvi identifikatori se nazivaju adresama u žargonu bitcoina. Termin adresa često se spominje u kontekstu bitcoina i kriptovaluta, u stvari je to hash vrijednost javnog ključa. - Narayanan et. al, Princeton Bitcoin book Njihovo vlasništvo nad bitcoinima povezano je s digitalnom adresom (dugim nizom znamenki) koja ima dvije komponente: javni ključ koji služi kao adresa i privatni ključ koji vlasniku daje pristup njegovom novcu povezanom s tom adresom. -Tapscott and Tapscott, Blockchain revolution

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
altcoin	cryptocurrency alternative to bitcoin, usually with a specific purpose	The vast majority of alt coins are derived from bitcoin's source code, also known as "forks." Some are implemented "from scratch" based on the blockchain model but without using any of bitcoin's source code. Alt coins and alt chains (in the next section) are both separate implementations of blockchain technology and both forms use their own blockchain. The difference in the terms is to indicate that alt coins are primarily used as currency, whereas alt chains are used for other purposes, not primarily currency. - Antanopulous, Mastering Bitcoin	BT: cryptocurrency	alternativna kriptovaluta, *altcoin*	kriptovaluta različita od bitcoina, često ima specifičnu svrhu	Većina alternativnih kriptovaluta nastale su iz izvornog koda bitcoina, još ih se naziva i račvama. Neki su implementirani iz potpuno novog koda koji se temelji na modelu ulančanih blokova ali ne koriste izvorni kod bitcoina. Alternativne kriptovalute i alternativni ulančani blokovi različite su implementacije tehnologije ulančanih blokova te obje koriste vlastiti sustav ulančanih blokova. Razlika između pojmova ukazuje na to da se alternativne kriptovalute koriste kao novac, dok se alternativni ulančanih blokovi koriste za neke druge, ne novčane, svrhe. Antanopulous, Mastering Bitcoin
asymmetrical cryptography, asymmetric cryptography	cryptographic system which uses a pair of keys, the public key to encrypt dana and the private key to decrypt it	Asymmetric cryptography refers to a type of cryptography whereby the key that is used to encrypt the data is different form the key that is used to decrypt the data. Also known as public key cryptography, it uses public and private keys in order to encrypt and decrypt data, respectively. - Bashir, Mastering blockchain	Syn: public key cryptography RT: public key, private key	asimetrična kriptografija	kriptografski sustav koji koristi par ključeva, javni ključ da kriptira podatke i privatni ključ da ih dekriptira	Asimetrična kriptografija odnosi se na vrstu kriptografije u kojoj je ključ koji se koristi za kriptiranje podataka različit od ključa koji se koristi za dekriptiranje podataka. Također poznata i pod nazivom kriptografija javnog ključa, ona koristi javne i privatne ključeve kako bi kriptirala i dekriptirala podatke. - Bashir, Mastering blockchain

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
bitcoin, BTC	cryptocurrency in the form of digital decentralized money which uses the blockchain to record transactions	In a precise and technical definition, Bitcoin is digital cash that is transacted via the Internet in a decentralized trustless system using a public ledger called the blockchain. -Swan, Blockchain: Blueprint for a new economy Bitcoin can be defined in various ways; it's a protocol, a digital currency, and a platform. It is a combination of peer-to-peer network, protocols and software that facilitate the creation and usage of the digital currency named bitcoin. Note that Bitcoin with a capital B is used to refer to the Bitcoin protocol, whereas bitcoin with a lowercase b is used to refer to bitcoin, the currency. -Bashir, Mastering blockchain	BT: cryptocurrency	bitcoin	kriptovaluta u obliku digitalnog decentraliziranog novca koja koristi ulančane blokove kako bi zapisivala podatke o transakcijama	Precizna i tehnička definicija bitcoina glasi: digitalna gotovina koja se prenosi putem interneta koristeći decentralizirani sustav bez povjerenja i javnu glavnu knjigu koja se naziva ulančanim blokovima. -Swan, Blockchain: Bluepring for a new economy Bitcoin se može definirati na više načina; to je protokol, digitalna valuta i platforma. To je spoj *peer-to-peer* mreže, protokola i softvera koji omogućavaju stvaranje i korištenje digitalne valute po imenu bitcoin. Potrebno je primijetiti da je Bitcoin s velikim početnim slovom ime za protokol, a bitcoin s malim početnim slovom ime za kriptovalutu. -Bashir, Mastering blockchain

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
block	set of cryptographically recorded data with a header containing the hash of the previous block, a timestamp, a hash pointer and a nonce	A block is composed of multiple transactions and some other elements such as the previous block hash (hash pointer), timestamp and nonce. -Bashir, Mastering blockchain A block is a container data structure that aggregates transactions for inclusion in the public ledger, the blockchain. The block is made of a header, containing metadata, followed by a long list of transactions that make up the bulk of its size. The block header is 80 bytes, whereas the average transaction is at least 250 bytes and the average block contains more than 500 transactions. A complete block, with all transactions, is therefore 1,000 times larger than the block header. - Antanopulous, Mastering blockchain	NT: Genesis block RT: block header, timestamp, nonce	blok	niz kriptografski zapisanih podataka sa zaglavljem koje sadrži hash vrijednost prijašnjeg bloka, vremensku oznaku, hash pokazivač i jednokratni niz	Blok se sastoji od više transakcija i nekih drugih elemenata poput hash vrijednosti prijašnjeg bloka (hash pokazivača), vremenske oznake i jednokratnog niza. -Bashir, Mastering blockchain Blok sadrži podatkovne strukture koje grupiraju i sažimaju transakcije za upis u javnu glavnu knjigu, odnosno ulančane blokove. Blok sadrži zaglavlje, koje sadrži metapodatke, nakon kojih slijedi dugačak niz transakcija koje zauzimaju većinu prostora bloka. Zaglavlje bloka veličine je 80 bajta, dok je prosječna transakcija veličine 250 bajta, a prosječni blok sadrži 500 transakcija. Blok, sa svim transakcijama, je stoga 1000 puta veći od zaglavlja bloka. - Antanopulous, Mastering blockchain
block difficulty	measure of computation power required to generate proof-of-work	To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases. - Nakamoto, Bitcoin whitepaper A network-wide setting that controls how much	BT: Block	zahtjevnost bloka	mjera računalne snage potrebne da se proizvede dokaz o radu	Kako bi mrežu prilagodili rastućoj brzini hardvera i promjenjivom interesu za održavanje čvorišnih računala tijekom vremena, zahtjevnost dokaza o radu određuje se pomoću kliznog prosjeka čiji je cilj omogućiti stvaranje prosječne količine bloka po satu. Ako se blokovi proizvode prebrzo, zahtjevnost raste. - Nakamoto, Bitcoin whitepaper

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
		computation is required to produce a proof of work. - Antanopulous, Mastering bitcoin				
block header	data located at the beginning of a block, contains information on the previous block, the nonce, a timestamp and the merkle tree root	The block header consists of three sets of block metadata. First, there is a reference to a previous block hash, which connects this block to the previous block in the blockchain. The second set of metadata, namely the difficulty, timestamp, and nonce, relate to the mining competition, as detailed in Chapter 8. The third piece of metadata is the merkle tree root, a data structure used to efficiently summarize all the transactions in the block. - Antanopulous, Mastering bitcoin	BT: Block	zaglavlje bloka	podaci na početku bloka, sadrži informacije o prijašnjem bloku, jednokratnom zapisu, vremensku oznaku i Merkleovo stablo	Zaglavlje bloka sastoji se od tri seta metapodataka. Prvi set sastoji se od reference na prijašnju hash vrijednost bloka koja povezuje trenutni i prijašnji blok u sustavu ulančanih blokova. Drugi set sastoji se od metapodataka, zahtjevnosti bloka, vremenske oznake i jednokratnog niza koji su povezani s rudarenjem, kao što je opisano u poglavlju 8. Treći set metapodataka je Merkleovo stablo, struktura podataka koja efikasno sažima sve transakcije unutar bloka. - Antanopulous, Mastering bitcoin
block height	position of a block within the blockchain	A second way to identify a block is by its position in the blockchain, called the block height. The first block ever created is at block height 0 (zero) - Antanopulous, Mastering bitcoin		visina bloka	pozicija bloka unutar ulančanih blokova	Drugi način na koji se može identificirati blok je njegova pozicija u ulančanim blokovima, naziva visinom bloka. Prvi blok ikad stvoren ima visinu 0 (nula). - Antanopulous, Mastering bitcoin

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
block reward	recompense rewarded to the miner for the calculation of a new block	By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended. -Nakamoto, Bitcoin whitepaper An amount included in each new block as a reward by the network to the miner who found the Proof-Of-Work solution. It is currently 25BTC per block. -Antanopulous, Mastering bitcoin	BT: Block	nagrada bloka	kompenzacija koju prima rudar čije je računalo izračunalo novi blok	Prema konvenciji, prva transakcija u bloku je posebna transakcija koja stvara novčić čiji je vlasnik stvaratelj bloka. To je poticaj čvorišnim računalima da održavaju mrežu, i nudi način da se novčići inicijalno distribuiraju i puste u cirkulaciju budući da nema središnjeg autoriteta koji bi ih izdavao. Stalno dodavanje konstantne količine novih novčića može se usporediti s rudarenjem zlata u kojem rudari troše sredstva kako bi dodali zlato u cirkulaciju. U slučaju kriptovaluta, troši se procesorsko vrijeme računala i struja. -Nakamoto, Bitcoin whitepaper Svota pridodana svakom novom bloku kao nagrada mreže za rudara koji je ponudio izračun za dokaz o radu. Trenutno je riječ o 25 bitcoina po bloku. -Antanopulous, Mastering bitcoin

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
blockchain	database in the form of a distributed ledger which stores unmutable records organized in cryptographically secured blocks	blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. -Iasiti and Lakhani, Harvard Business Review, The truth about blockchain A blockchain is a type of distributed ledger that is shared across a business network. Business transactions are permanently recorded in sequential, append-only, tamper-evident blocks to the ledger. All the confirmed and validated transaction blocks are hash-linked from the genesis block to the most current block, hence the name blockchain. -IBM, Blockchain basics It is the blockchain that replaces this trusted third party. A database that contains the payment history of every bitcoin in circulation, the blockchain provides proof of who owns what at any given juncture. This distributed ledger is replicated on thousands of computers—bitcoin's "nodes"—around the world and is publicly available. -Economist, The great chain of being sure about things		ulančani blokovi, *blockchain*	baza podataka u obliku distribuirane glavne knjige u kojoj se bilježe nepromjenjivi zapisi organizirani u kriptografski osigurane blokove	Ulančani blokovi su otvorena, distribuirana glavna knjiga koja bilježi transakcije između stranaka efikasno, provjerljivo i trajno.- Iasiti i Lakhani, Harvard Business Review, The truth about blockchain Ulančani blokovi su vrsta distribuirane glavne knjige koju dijeli cijela mreža. Poslovne transakcije dugoročno se bilježe u nanizanim blokovima na koje se mogu isključivo dodavati novi blokovi te u kojima je svaka promjena jasno vidljiva. Svi potvrđeni i provjereni transakcijski blokovi povezani su hash vrijednostima od početnog bloka do najrecentnijeg bloka, pa upravo zbog toga nose ime ulančani blokovi. -IBM, Blockchain basics Upravo ulančani blokovi zamjenjuju povjerenje u treću stranu. Baza podataka koja sadrži povijest plaćanja svakog bitcoina u cirkulaciji - ulančani blokovi nude dokaz o vlasništvu u bilo kojem trenutku. Distribuirana glavna knjiga replicirana je na tisućama računala, bitcoinovim "čvorovima", diljem svijeta i dostupna je javnosti. -Economist, The great chain of being sure about things

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
Byzantine General's Problem	mathematical problem dealing with consensus on a distributed network	Satoshi Nakamoto's invention is also a practical solution to a previously unsolved problem in distributed computing, known as the "Byzantine Generals' Problem." Briefly, the problem consists of trying to agree on a course of action by exchanging information over an unreliable and potentially compromised network. -Antanopulous, Mastering bitcoin In this classic problem, the Byzantine army is separated into divisions, each commanded by a general. The generals communicate by messenger in order to devise a joint plan of action. Some generals may be traitors and may intentionally try to subvert the process so that the loyal generals cannot arrive at a unified plan. The goal of this problem is for all of the loyal generals to arrive at the same plan without the traitorous generals being able to cause them to adopt a bad plan. It has been proven that this is impossible to achieve if one-third or more of the generals are traitors. -Narayanan et al, Princeton Bitcoin book	RT: Distributed consensus	Problem bizantskih generala	matematički problem konsenzusa u distribuiranoj mreži	Izum Satoshija Nakamote također je praktično rješenje za do tada neriješeni problem u distribuiranom računarstvu, poznat pod imenom 'problem bizantskih generala'. Ukratko, problem se bavi dogovaranjem o zajedničkom djelovanju razmjenjujući informacije preko nepouzdane i potencijalno kompromitirane mreže. -Antanopulous, Mastering bitcoin U ovom klasičnom problemu, Bizantska vojska podijeljena je na divizije kojima zapovijedaju generali. Generali komuniciraju putem glasnika kako bi napravili zajednički plan djelovanja. Neki generali mogu biti izdajnici i mogu namjerno narušiti proces dogovora kako lojalni generali ne bi mogli dogovoriti zajednički plan. Cilj problema je koordinirati sve lojalne generale da dogovore zajednički plan, bez da izdajnički generali mogu natjerati lojalne generale da se dogovore za loš plan. Dokazano je nemoguće postići dogovor ako je više od jedne trećine izdajničkih generala. -Narayanan et al, Princeton Bitcoin book

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
collision resistant hash function	cryptographic function in which two inputs cannot produce the same output	The first property that we need from a cryptographic hash function is that it's collision-resistant. A collision occurs when two distinct inputs produce the same output. -Narayanan et al. Princeton bitcoin book	BT: hash function	hash funkcija otporna na koliziju	kriptografska funkcija u kojoj dva ulaza ne mogu proizvesti isti izlaz	Prvo svojstvo koje se zahtijeva od kriptografske hash funkcije je otpornost na koliziju. Kolizija nastaje kada dva različita ulaza nude isti izlaz. -Narayanan et al. Princeton bitcoin book
consenus mechanism, consensus protocol	set of rules governing agreement on the blockchain network	This is guaranteed by the mixture of mathematical subtlety and computational brute force built into its "consensus mechanism"—the process by which the nodes agree on how to update the blockchain in the light of bitcoin transfers from one person to another. -Economist, The great chain of being sure about things		konsenzusni mehanizam, konsenzusni protokol	skup pravila koje uređuju suglasnost u mreži ulančanih blokova	To je zagarantirano spojem matematičke suptilnosti i čiste računalne sile ugrađene u "konsenzusni mehanizam" - proces u kojem se čvorišna računala usuglašavaju o tome kako će ažurirati ulančane blokove u kontekstu prijenosa bitcoina s jedne osobe na drugu. - Economist, The great chain of being sure about things
crpytocurrency	digital money based on the blockchain	Bitcoin is the first and largest decentralized cryptocurrency. There are hundreds of other "altcoin" (alternative coin) cryptocurrencies, like Litecoin and Dogecoin, but Bitcoin comprises 90 percent of the market capitalization of all cryptocurrencies and is the de facto standard. -Swan, Blockchain - blueprint for a new economy		kriptovaluta	digitalni novac utemeljen na ulančanim blokovima	Bitcoin je prva i najveća decentralizirana kriptovaluta. Postoje stotine drugih alternativnih kriptovaluta, poput Litecoina i Dogecoina, no Bitcoin drži 90 posto kapitaliziranog tržišta svih kriptovaluta te je *de facto* standard. -Swan, Blockchain - blueprint for a new economy

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
cryptograhic hash function	mathematical computationl algorithm which encrypts an input into a hiding output	Cryptographic hashes, such as the SHA256 computational algorithm, ensure that any alteration to transaction input — even the most minuscule change — results in a different hash value being computed, which indicates potentially compromised transaction input. -IBM, Blockchain basics		kriptografska funkcija sažimanja	matematički, računalni algoritam koji enkriptira neki ulaz u zakriveni izlaz	Kriptografska hash funkcija, kao što je računalni algoritam SHA256, osigurava da bilo kakva promjena transakcijskog unosa, čak i najmanja promjena, uzrokuje promjenu hash vrijednosti, koja ukazuje na potencijalnu kompromitiranost ulazne vrijednosti. -IBM, Blockchain basics
cryptography	the practice of mathematically ensuring secure communication	Cryptographers use mathematics to define primitives, protocols, and their desired security properties in a formal way, and to prove them secure based on widely accepted assumptions about the computational hardness of specific mathematical tasks. - Narayanan et al, Princeton bitcoin book		kriptografija	praksa matematičke uspostave sigurne komunikacije	Kriptografi koriste matematiku kako bi definirali primitive, protokole i željena sigurnosna svojstva na formalan način i dokazali da su sigurni s pomoću široko prihvaćenih pretpostavki o težini izračuna specifičnih matematičkih zadataka. - Narayanan et al, Princeton bitcoin book

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
digital signature	an electronic string of symbols or code denoting identity	Specifically, cryptographic digital signatures enable a user to sign a digital asset or transaction proving the ownership of that asset. -Antanopulous, Mastering blockchain A digital signature is supposed to be the digital analog to a handwritten signature on paper. We desire two properties from digital signatures that correspond well to the handwritten signature analogy. Firstly, only you can make your signature, but anyone who sees it can verify that it's valid. Secondly, we want the signature to be tied to a particular document so that the signature cannot be used to indicate your agreement or endorsement of a different document. -Narayanan et al, Princeton bitcoin book Digital signatures ensure that transactions originated from senders (signed with private keys) and not imposters. -IBM, Blockchain basics		digitalni potpis	elektronički niz znakova ili kôd koji označava identitet	Konkretno, kriptografski digitalni potpisi omogućuju korisniku da potpiše digitalnu imovinu ili transakciju i dokaže vlasništvo nad njome. -Antanopulous, Mastering blockchain Digitalni potpis trebao bi biti istovjetan ručno napisanom potpisu na papiru. Dva svojstva su poželjna za uspostavu analogije između digitalnog i analognog potpisa. Kao prvo, samo potpisnik bi trebao moći na nešto staviti potpis, no bilo tko tko ga vidi mora moći potvrditi da je valjan. Kao drugo, digitalni potpis treba biti vezan uz određeni dokument kako ne bi bilo moguće isti potpis iskoristiti za suglasnost s nekim drugim dokumentom. -Narayanan et al, Princeton bitcoin book Digitalni potpisi osiguravaju da su transakcije započele od pošiljatelja (potpisane privatnim ključem), a ne od prevaranta. -IBM, Blockchain basics

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
distributed consensus	agreement between all nodes in a peer-to-peer system	Consensus is the collaborative process that the members of a blockchain business network use to agree that a transaction is valid and to keep the ledger consistently synchronized. -IBM, Blockchain basics The implications of having a distributed consensus protocol reach far beyond this traditional application. If we had such a protocol, we could use it to build a massive, distributed key-value store, that maps arbitrary keys, or names, to arbitrary values. -Narayanan et al. Princeton bitcoin book		distribuirani konsenzus	suglasnost svih čvorova unutar *peer-to-peer* mreže	Konsenzus je proces suradnje kojeg članovi poslovne mreže ulančanih blokova koriste kako bi se složili da je transakcija važeća te kako bi glavnu knjigu održali konzistentno sinkroniziranom. -IBM, Blockchain basics Implikacije korištenja protokola distribuiranog konsenzusa sežu dalje od tradicionalnih primjena. Kada bismo imali takav protokol, mogli bismo ga iskoristiti da izgradimo golemo, distribuirano spremište ključnih vrijednosti, koje povezuje arbitrarne ključeve ili imena s arbitrarnim vrijednostima. -Narayanan et al. Pricneton bitcoin book
distributed ledger	a shared principal book	A distributed ledger is a type of database, or system of record, that is shared, replicated, and synchronized among the members of a network. The distributed ledger records the transactions, such as the exchange of assets or data, among the participants in the network. This shared ledger eliminates the time and expense of reconciling disparate ledgers. -IBM, Blockchain basics		distribuirana glavna knjiga	dijeljena glavna knjiga	Distribuirana glavna knjiga oblik je baze podataka, ili sistema zapisivanja, koji je dijeljen, umnožen i sinkroniziran između članova mreže. Distribuirana glavna knjiga bilježi transakcije, kao što su razmjena imovine ili podataka, među korisnicima mreže. Ova dijeljena glavna knjiga eliminira vrijeme i trošak uspoređivanja dvije različite glavne knjige. -IBM, Blockchain basics

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
distributed ledger technology, DLT	family of technologies and application using a shared principal book	DLT refers to a novel and fast-evolving approach to recording and sharing data across multiple data stores (or ledgers). This technology allows for transactions and data to be recorded, shared, and synchronized across a distributed network of different network participants. -World Bank, DLT and blockchain fintech notes		tehnologija distribuirane glavne knjige, DLT	obitelj tehnologija i primjena koje koriste dijeljenu glavnu knjigu	DLT se odnosi na nov i brzo-evoluirajući pristup bilježenju i dijeljenju podataka kroz više spremišta podatka (ili glavnih knjiga). Ova tehnologija omogućava da se transakcije bilježe, dijele i sinkroniziraju kroz distribuirane mreže različitih učesnika. -World Bank, DLT and blockchain fintech notes
double spending, double spending attack	the act of using the same monetary unit or coin in two separate transactions	If the ledger is truly append-only, we can use it to defend against double-spending by requiring all transactions to be written the ledger before they are accepted. That way, it will be publicly visible if coins were previously sent to a different owner. -Narayanan et al, Princeton bitcoin book		dvostruka transakcija, dupla transkacija	korištenje iste obračunske jedinice ili istog novčića u dva plaćanja	Ako se u glavnu knjigu zaista mogu samo dodavati podaci, onda ju je moguće koristiti za zaštitu od dvostrukih transakcija postavljanjem zahtjeva da se sve transakcije upišu u glavnu knjigu prije no što budu prihvaćene. Na taj način javno je vidljivo ako ga je isti vlasnik ranije potrošio. -Narayanan et al, Princeton bitcoin book
fork	temporary state of a blockchain network in which two blocks occupy the same height on the chain	Forks occur as temporary inconsistencies between versions of the blockchain, which are resolved by eventual reconvergence as more blocks are added to one of the forks. -Antanopulous, Mastering bitcoin		račvanje	privremeno stanje mreže ulančanih blokova u kojem se dva bloka nalaze na istoj visini lanca	Račvanja se događaju kao privremene neusklađenosti između verzija ulančanih blokova, koje se rješavaju ponovnim usklađivanjem tako da se novi blokovi dodaju jednoj inačici.-Antanopulous, Mastering bitcoin
hash value	encrypted transaction data	Each transaction in a set that makes up a block is fed to a program that creates an encrypted code known as the hash value. -Economist, The great chain of being sure about things		hash vrijednost	kriptirani podaci o transakcijama	Svaka transakcija u setu koji čini blok prolazi kroz program koji stvara kriptiranu vrijednost poznatu kao hash vrijednost. -Economist, The great chain of being sure about things

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
Merkle tree	hash value of all previous hashed values	Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree, with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. -Nakamoto, Bitcoin whitepaper		Merkleovo stablo	hash vrijednost svih prijašnjih hash vrijednosti	Kad se na zapis nove transakcije neke valute nadoveže dovoljno blokova, potrošenu transakciju može se obrisati kako bi se uštedjelo na diskovnom prostoru. Da bi se to izvelo bez kvarenja hash vrijednosti bloka, transakcije se sažimaju s pomoću Merkleovog stabla. Stari blokovi mogu se sažeti rezanjem grana na stablu. -Nakamoto, Bitcoin whitepaper
mining	using a computer's processor power to calculate new blocks	The steady addition of a constant amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended. -Nakamoto, Bitcoin Whitepaper Across the network, miners grind through trillions and trillions of possibilities looking for the answer. When a miner finally comes up with a solution other nodes quickly check it (that's the one-way street again: solving is hard but checking is easy), and each node that confirms the solution updates the blockchain accordingly. -Economist, The great chain of being sure about things		rudarenje	korištenje procesorske snage računala za izračunavanje novih blokova	Stalni rast količine novčića usporediv je s rudarima zlata koji troše svoje resurse kako bi dodali zlato u promet. U slučaju kriptovaluta, troši se vrijeme procesorskog rada i struja. -Nakamoto, Bitcoin Whitepaper U mreži rudari obrađuju trilijune i trilijune mogućih kombinacija tražeći odgovor. Kada rudar napokon dođe do izračuna, druga čvorišna računala brzo provode provjeru (to je vrlo jasna situacija, izračunavanje je zahtjevno, ali je provjera jednostavna), i svako čvorišno računalo koje potvrdi rješenje u skladu s time ažurira ulančani blok. -Economist, The great chain of being sure about things

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
mining pool	an association of blockchain miners	Once the purview of hobbyists, bitcoin mining is now dominated by large “pools”, in which small miners share their efforts and rewards, and the operators of big data centres, many based in areas of China, such as Inner Mongolia, where electricity is cheap. -Economist, The great chain of being sure about things		rudarsko udruženje	skup rudara ulančanih blokova	Nekad hobi, a danas rudarenjem bitcoina dominiraju velika rudarska udruženja u kojima rudari dijele trud i nagrade s operatorima velikih podatkovnih centara, kojih je mnogo u Kini, na primjer u središnjoj Mongoliji, gdje je struja jeftina. -Economist, The great chain of being sure about things
node	a computer connected to a blockchain network	every computer connected to the Bitcoin network using a client that performs the task of validating and relaying transactions -Swan, blockchain blueprint for a new economy		čvor	računalo spojeno na mrežu ulančanih blokova	Svako računalo povezano na bitcoin mrežu koje koristi klijentski softver koji izvodi zadatak potvrđivanja i prosljeđivanja transakcija. -Swan, blockchain blueprint for a new economy
nonce	a number string used to calculate a block	For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. -Nakamoto, bitcoin whitepaper The header then becomes part of a cryptographic puzzle solved by manipulating a number called a nonce. -Economist, The great chain of being sure about things		jednokratni niz	niz brojeva s pomoću kojih se izračunava blok	U mrežu za dodjeljivanje vremenskih oznaka uvodi se dokaz o radu ponavljanjem izračuna koristeći jednokratni niz u bloku dok se ne pronađe rješenje u kojem hash vrijednost bloka ima potreban broj bitova vrijednosti nula. -Nakamoto, bitcoin whitepaper Zaglavlje postaje dio kriptografske zagonetke koju se rješava manipuliranjem broja koji se naziva jednokratnim nizom. -Economist, The great chain of being sure about things

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
peer-to-peer	type of network utilizing computers on the same level, without hierarchy	A blockchain network for business is a collectively owned peer-to-peer network that is operated by a group of identifiable and verifiable participants. Participants may be individuals or institutions, such as a business, university, or hospital, for example. -IBM, Blockchain basics In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. -Nakamoto, Bitcoin Whitepaper		*peer-to-peer,* distribuirana mreža	vrsta mreže koja koristi ravnopravna računala, bez hierarhije	Mreža ulančanih blokova za poslovanje je mreža ravnopravnih računala u zajedničkom vlasništvu koju održava skupina korisnika čiji je identitet i provjerenost moguće ustvrditi. Korisnici mogu biti pojedinci ili institucije, kao što su na primjer privatna društva, sveučilišta ili bolnice. -IBM, Blockchain basics U ovom tekstu, predlažemo rješenje za dvostruke transakcije s pomoću distribuiranog servera koji izdaje vremenske žigove ravnopravnim računalima kako bi stvorio matematički dokaz o kronološkom redoslijedu transakcija. -Nakamoto, Bitcoin Whitepaper
permissioned blockchain	private blockchain network	Permissioned networks, on the other hand, are usually private and are limited to participants within a given business network. On permissioned blockchains, participants are allowed to view only the transactions relevant to them. Hyperledger is a collaborative effort, hosted by the Linux Foundation, to support the development of permissioned blockchains for business. -IBM, Blockchain basics	Syn: closed blockchain, private blockchain	zatvoreni sustav ulančanih blokova	privatna mreža ulančanih blokova	Zatvoreni sustavi ulančanih blokova, s druge strane, najčešće su privatni i sudjelovanje u njima je ograničeno na određenu poslovnu mrežu. U zatvorenim sustavima ulančanih blokova sudionici smiju pristupati samo transakcijama povezanima s njima. Hyperledger je suradnički projekt koji podržava Linux Foundation, čiji je cilj razvoj zatvorenih sustava ulančanih blokova namijenjenih poslovanju. -IBM, Blockchain basics

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
permissionless blockchain	public blockchain network	Permissionless networks are open to any participant, and transactions are verified against the pre-existing rules of the network. Any participant can view transactions on the ledger, even if participants are anonymous. Bitcoin is the most familiar example of a blockchain network that is permissionless and public. -IBM, Blockchain basics	Syn: open blockchain, public blockchain	otvoreni sustav ulančanih blokova	javna mreža ulančanih blokova	Otvoreni sustavi ulančanih blokova dostupni su bilo kome, a transakcije se potvrđuju po unaprijed određenim pravilima mreže. Bilo koji sudionik može pristupiti transakcijama u glavnoj knjizi unatoč anonimnosti sudionika. Bitcoin je najpoznatiji primjer mreže ulančanih blokova koja je otvorena i javna. -IBM, Blockchain basics
private key	a string of numbers used to verify a digital signature	Digital signatures ensure that transactions originated from senders (signed with private keys) and not imposters. -IBM, Blockchain basics		privatni ključ	niz brojeva kojim se potvrđuje digitalni potpis	Digitalni potpisi osiguravaju da su transakcije započele od pošiljatelja (potpisane privatnim ključem), a ne od prevaranta. -IBM, Blockchain basics
proof of work	an algorithm which proves a computer's processor time was expended to calculate a nonce	For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. -Nakamoto, bitcoin whitepaper		*proof of work*, dokaz o radu	algoritam koji dokazuje da je procesorsko vrijeme računala iskorišteno kako bi se izračunao jednokratni niz	U mrežu za dodjeljivanje vremenskih oznaka, uveli smo dokaz o radu ponavljanjem izračuna koristeći jednokratni niz u bloku dok se ne pronađe rješenje u kojem hash vrijednost bloka ima potreban broj bitova vrijednosti nula. Jednom kad je procesorska snaga računala iskorištena kako bi zadovoljila dokaz o radu, blok se ne može mijenjati bez ponavljanja cijelog procesa. -Nakamoto, bitcoin whitepaper

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
smart contract	automated payment system on the blockchain	Smart contracts govern interactions with the ledger, and they can allow network participants to execute certain aspects of transactions automatically. For example, a smart contract could stipulate the cost of shipping an item that changes depending on when it arrives. With the terms agreed to by both parties and written to the ledger, the appropriate funds change hands automatically when the item is received. -IBM, Blockchain basics “Smart contracts” may be the most transformative blockchain application at the moment. These automate payments and the transfer of currency or other assets as negotiated conditions are met. For example, a smart contract might send a payment to a supplier as soon as a shipment is delivered. -- Iasiti and Lakhani, Harvard Business Review, The truth about blockchain		pametni ugovor	automatizirani sustav isplate na ulančanim blokovima	Pametni ugovori upravljaju interakcijama s glavnom knjigom, mogu dopustiti korisnicima mreže da izvrše neke vrste transakcija automatski. Na primjer, pametnim ugovorom može se urediti cijena poštarine nekog paketa koja se mijenja ovisno o tome kada bi paket trebao stići. Uvjeti s kojima se slože obje stranke zapisuju se u glavnu knjigu, te se prikladna uplata izvršava automatski po isporuci paketa. -IBM, Blockchain basics "Pametni ugovori" vjerojatno su najtransformativnija primjena ulančanih blokova danas. Oni automatiziraju uplate i transfer novca ili drugih vrijednosnica u trenutku kada su zadovoljeni dogovoreni uvjeti. Na primjer, pametni ugovor može poslati novac dobavljaču u trenutku kada pošiljka pristigne. - Iasiti i Lakhani, Harvard Business Review, The truth about blockchain

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
timestamp	data relating to time appended to a other dana	The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it. -Nakamoto, Bitcoin whitepaper		vremenska oznaka	podaci o vremenu dodani drugim podacima	Rješenje koje se predlaže počinje s poslužiteljem za vremenske oznake. Poslužitelj uzima hash vrijednosti bloka, pridružuje im vremensku oznaku te objavljuje hash vrijednost javnosti, putem novina ili na Usenetu. Vremenska oznaka dokazuje da su podaci postojali u to vrijeme, jer je dio hash vrijednosti. Svaka vremenska oznaka sadržava prijašnju vremensku oznaku u svojoj hash vrijednosti, stvarajući lanac u kojem svaka dodatna vremenska oznaka potvrđuje prijašnje. -Nakamoto, Bitcoin whitepaper
transaction	transfer of assets	A transaction is an asset transfer onto or off of the ledger. -IBM, blockchain basics		transakcija	transfer vrijednosti	Transakcija je transfer vrijednosti s nekog računa zabilježenog u glavnu knjigu ili na njega. - IBM, blockchain basics
wallet	software which holds a user's cryptocurrencies	If you’re storing your bitcoins locally, you’d typically use wallet software, which is software that keeps track of all your coins, manages all the details of your keys, and makes things convenient with a nice user interface. -Narayanan et al, Princeton bitcoin book		novčanik	softver koji čuva korisnikove kriptovalute	Ako se bitcoin čuva lokalno, tipično će se koristiti softverski novčanik. To je softver koji prati sav digitalni novac u posjedu korisnika, čuva detalje njegovim kriptografskim ključevima i olakšava korištenje nudeći jednostavno korisničko sučelje. -Narayanan et al, Princeton bitcoin book