CAD AND BLOCKCHAIN TECHNOLOGY INTEGRATION MODEL FOR THE PURPOSE OF DATA PROTECTION

Irena Tasić
The College of academic studies „Dositej“, Belgrade, Serbia, irena.tasic67@gmail.com
Saša Đorđević
“Habitat” d.o.o., Vranje, Serbia, habitatvr@mts.rs
Vukašin Tasić
Singidunum University, Beograd, Serbia, tasicvuki@gmail.com

Abstract: Distributed and interactive environments, such as computer aided design (CAD), including building information modeling (BIM) and geographic information systems (GIS) in construction and architecture as well as product data management and/or product lifecycle management (PDM/PLM) in mechanical engineering. In any case, it is necessary to preserve the integrity of data in these computer applications, which builds user confidence in CAD and BIM data. Blockchain technology is increasingly being used to address data integrity in interactive CAD environments. Blockchain is built from blocks that are linearly connected, in chronological order, which creates a permanent and immutable digital ledger of all transactions on the network. The use of smart contracts, self-executing contracts with terms of agreement between buyers and sellers written directly into computer code, has further expanded the potential uses of blockchain. The first smart contracts were implemented on the Ethereum blockchain in 2015, and have since become a key feature of blockchain technology. Blockchain technology, like everything else we use, has its advantages and disadvantages. The essential advantages of blockchain are: data integrity, reliability, traceability, decentralization, persistence, anonymity. Disadvantages such as data transparency and the slowness of data archiving in blockchain should not be a reason to abandon the implementation of blockchain in wider use.
Keywords: blockchain, Cad, BIM, Ethereum, cryptographic keys, data integrity

MODEL INTEGRACIJE CAD-a I BLOCKCHAIN TEHNOLOGIJE U CILJU ZAŠTITE PODATAKA

Irena Tasić
Visoka škola akademskih studija “Dositej” Beograd, Srbija, irena.tasic67@gmail.com
Saša Đorđević
“Habitat” d.o.o., Vranje, Serbia, habitatvr@mts.rs
Vukašin Tasić
Singidunum Univerzitet, Beograd,Serbia, tasicvuki@gmail.com

Rezime: Distribuirana i interaktivna okruženja, kao što je dizajniranje računarom (CAD), uključuje informaciono modeliranje zgrada (BIM) i geografske informacione sisteme (GIS) u građevinarstvu i arhitekturi kao i upravljanje podacima o proizvodima i/ili upravljanje životnim cikluskom proizvoda (PDM/PLM) u mašinstvu. U svakom slučaju neophodno je sačuvati integritet podataka u ovim kompjuterskim aplikacijama čime se gradi poverenje korisnika u CAD i BIM podatke. U rešavanju integriteta podataka u interaktivnim CAD okruženjima sve više se koristi *blockchain* tehnologija. *Blockchain* je izgrađen iz blokova koji su linearno povezani, hronološkim redosledom, što stvara trajnu i nepromenljivu digitalnu knjigu svih transakcija na mreži. Upotreba pametnih ugovora, samo izvršnih ugovora sa uslovima sporazuma između kupaca i prodavaca koji su direktno upisani u kompjuterskom kodu, dodatno je proširila potencijalnu upotrebu *blockchain*-a. Prvi pametni ugovori su implementirani na Ethereum *blockchain*-u 2015. godine, i od tada su postal ključna karakteristika *blockchain* tehnologije. *Blockchain* tehnologija, kao uostalom i sve drugo što koristimo, ima svoje prednosti i nedostatke. Bitne prednosti *blockchain*-a su: integritet podataka, pouzdanost, sledivost, decentralizacija, postojanost, anonimnost. Nedostatak kao što je transparentnost podataka i sporost arhiviranja podataka u *blockchain*-u ne bi trebali da predstavljaju razlog zbog koga bi se odustalo od implementacije *blockchain*-a u široj upotrebi.
Ključne reči : *blockchain*, CAD, BIM, Ethereum, kriptografski ključevi, integritet podataka

1. UVOD

Savremeno tržište diktira korišćenje novih tehnologija. Sve veći zahtevi tržišta kao što su ekološki prihvatljivi proizvodi, pametne zgrade, dinamički globalni lanci nabavke, zahtevi za smanjenjem troškova i mobilnost radne snage promenili su doskorašnje korake u ciklusu nekog proizvoda. Sada se svaki zadatak obavlja kao timski rad kako bi se proizvod isporučio na vreme.

Ovi radni timovi koriste savremene tehnologije a najčešće se to odražava kroz rad u oblaku (tzv. "*cloud*") gde se svetlo baca na deljenje resursa i razmenu podataka. Uporedo sa tim, i proizvođači softvera prebacuju svoje prizvode sa računarskih radnih stanica na resurse računarstva u oblaku, omogućavajući tako globalan distribuiran timski rad.

Upotreba računarstva u oblaku u kompjuterskom projektovanju (CAD) još uvek nije dovoljno zrela da bi prevladala nad desktop računarstvom. Interaktivna CAD okruženja kao što je informaciono modeliranje zgrada (BIM) i upravljanje podacima o proizvodu/upravljanje životnim ciklusom proizvoda (PDM/PLM) već su prihvatili prednost računarstva u oblaku, što nas dovodi do ključnog problema današnjice – do problema bezbednosti informacija. Ovaj problem bi se mogao prevazići korišćenjem novih tehnologija kao što je *blockchain*.

Poznato je da je tehnologija vezana za CAD, kompjuterski potpomognuta proizvodnja (CAM), bila decenijama vezana za ograničeno korišćenje CAD fajlova za generisanje koda za mašinsku obradu i tek od nedavno je pojačana brzom ekspanzijom tehnologije 3D štampanja. Kako je veliki broj digitalnih modela spremnih za 3D štampu dostupan u skladištima u oblaku, postoji rizik od kršenja eventualnog vlasništva (intlektualne svojine - IP) omogućavanjem jeftine proizvodnje falsifikovanih proizvoda ili jednostavnom izmenom ovih datoteka. Otvoreni problem bi se mogao rešiti integracijom *blockchain*-a u lance nabavke, pod uslovom da je tehnologija dostupna i pristupačna (Kurpjuweit et al., 2021).

Prva integrisana BIM i *blockchain* aplikacija još uvek je u razvoju u španskom projektu tehnološkog istraživanja i razvoja DELFOS. *Blockchain* je tehnologija koja omogućava razmenu informacija i transakcija između dva ili više učesnika kroz potpuno sigurno i nepovratno kodiranje. Ovaj prenos ne zahteva centralizovanog posrednika za identifikaciju i sertifikaciju informacija, ali se distribuira između nezavisnih učesnika *blockchain* mreže (čvorova) koji se registruju i potvrđuju bez potrebe za poverenjem među njima. Svaki učesnik ima tačnu kopiju informacija, što omogućava obavljanje transakcija kojima se može trgovati i koje se ne mogu lažirati. Ova sledivost može se proširiti na bilo koju promenu koja je napravljena na modelu projekta. Iz tog razloga, *blockchain* garantuje sigurno i kontrolisano okruženje za saradnju oko BIM-a. S obzirom da je *blockchain* arhitektura dizajnirana kao distribuirana baza podataka, nijedna od uključenih strana ne bi bila u povoljnijoj poziciji u odnosu na drugu jer *blockchain* garantuje princip neutralnosti na svaku promenu napravljenu na modelu. *Blockchain* deluje kao izvor poverenja u kome su učesnici sistema sigurni prilikom razmene informacija. Uz *blockchain* možemo ostaviti nepromenljiv zapis svih promena napravljenih na svakom BIM objektu. Sve ove promene biće automatski povezane sa autorom. Dakle, informacije bi se reflektovale i memorisale u svim sistemima i serverima sa pristupom, izbegavajući problem pri idetifikaciji autora. Samim tim, autorstvo i prava nad svakim delom samog modela odmah su razgraničeni (Valero, 2018).

Francuska start-up tehnološka kompanija, Lutecium, počela je da razvija *blockchain* softver baziran na BIMChain, koji je imao za cilj da ubrza BIM za građevinsku industriju (Cousins, 2018; Gueguen, 2018). Njihovo rešenje, bazirano na Ethereum platformi, integriše BIM ekosistem pomoću namenskih dodataka za Revit ili ArchiCAD. Projekat je podržan od strane Autodeska i francuske radne grupe *Plan Transition Numériquedans le Bâtiment*. Rana beta verzija softvera pokrenuta je početkom 2019. godine. Njihova težnja bila je da stvore interaktivni proces koji će da premosti raskorak između 3D CAD modela i pravno obavezujućih formalnih procesa zasnovanih na papiru koji se odnose na upravljanje projektima, održavanje i kontrolu zgrada i osiguranje i plaćanje. Cilj je da se povežu validni dokazi doprinosa 3D CAD modela sa oblikom pametnog ugovora, čineći BIM podatke ugovornim.

Blockchain je izgrađen iz blokova koji su linearno povezani, hronološkim redosledom, što stvara trajnu i nepromenljivu digitalnu knjigu svih transakcija na mreži. Blok je kolekcija podataka koja sadrži informacije o nizu transakcija. Svaki blok ima jedinstven kod („heš" bloka) koji ga razlikuje od drugih blokova i povezuje ga sa prethodnim blokom u lancu. Vreme između blokova (eng. *block time*) je veoma važna osobina koja se odnosi na količinu vremena potrebnog da se novi blok doda, jer određuje koliko brzo transakcije mogu biti potvrđene i novi blokovi dodati u lanac.

Upotreba pametnih ugovora, samo izvršnih ugovora sa uslovima sporazuma između kupaca i prodavaca koji su direktno upisani u kompjuterskom kodu, dodatno je proširila potencijalnu upotrebu *blockchain*-a. Koncept pametnih ugovora prvi put je predložio Nik Sabo 1994. godine (Szabo, 1996), kao potencijal korišćenja digitalne tehnologije za automatizaciju pregovora i sprovođenja ugovora, i počeo da piše o ideji samo izvršnih kompjuterskih programa koji se mogu koristiti umesto tradicionalnih ugovora. Iako tehnologija za implementaciju pametnih ugovora u to vreme nije postojala, Sabove ideje su postavile temelj za razvoj *blockchain*-a i tehnologije pametnih ugovora u

godinama koje dolaze. Prvi pametni ugovori su implementirani na Ethereum *blockchain*-u 2015. godine, i od tada su postal ključna karakteristika *blockchain* tehnologije.

2. MATERIJALI I METODE

Problem koji se obrađuje u radu zasniva se na modelu integracije CAD-a i blockchain-a a u cilju zaštite intelektualne svojine.

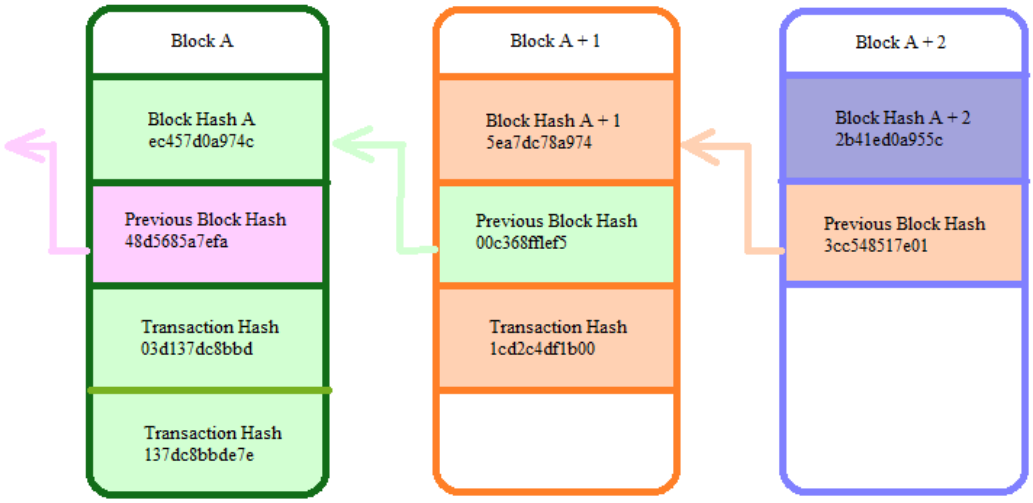
Blockchain stvara blokove informacija fiksne veličine koristeći takozvane *hash* funkcije. Ovi blokovi se zatim dodaju u nizu koji se zove *blockchain.* Svaki novi blok se nepovratno šifrira koristeći *hash* funkciju, a zatim skraćuje kako bi se dobio izlaz fiksne veličine. Lanac blokova tako sadrži šifrovanu verziju kompletne istorije promena svih blokova. *Blockchain* se oslanja na kriptografske *hash* funkcije. To su matematičke funkcije koje kreiraju izlazni niz bitova fiksne veličine. Gotovo je nemoguće pogoditi dužinu *hash*-a ako neko pokuša dešifrovati *blockchain*. *Hash* algoritam proizvodi jedinstveni izlaz i to je jednosmerna funkcija. Razvoj Ethereum-a poklapa se sa razvojem SHA3 standarda, a proces standardizacije napravio je promenu u dodatku finalnog *hash* algoritma. Ethereum *blockchain* koristi SHA3_256 koji nije standardni SHA3 već varijanta koja se često pominje kao "Keccak-256" (Ethereum, 2023).

Kako je više dostupnih resursa i zainteresovanih strana uključeno tokom životnog ciklusa proizvoda, razmena i upravljanje informacijama u vezi sa proizvodima postaju izazovan zadatak, koji značajno utiče na proces zaštite intelektualne svojine, kao i na razlikovanje uloga među zainteresovanim stranama (Papakostas et al., 2019).

Blockchain sigurnost se oslanja na enkripciju, zasnovanu na javnim i privatnim ključevima. Ključevi su dugački, nasumično generisani nizovi brojeva. Javni ključ predstavlja korisnika na *blockchain*-u, a privatni ključ, koji mora biti zaštićen, koristi se za digitalno potpisivanje transakcije, osiguravajući sledivost i integritet podataka.

Slika 1. pokazuje kako svaki blok u *blockchain*-u sadrži i kriptografski *hash* prethodnog bloka, koji se ne može promeniti. Svaki sledeći blok jača proveru prethodnog bloka i sigurnost *blockchain*-a. Dodavanjem novih blokova povećava se pouzdanost *blockchain*-a.

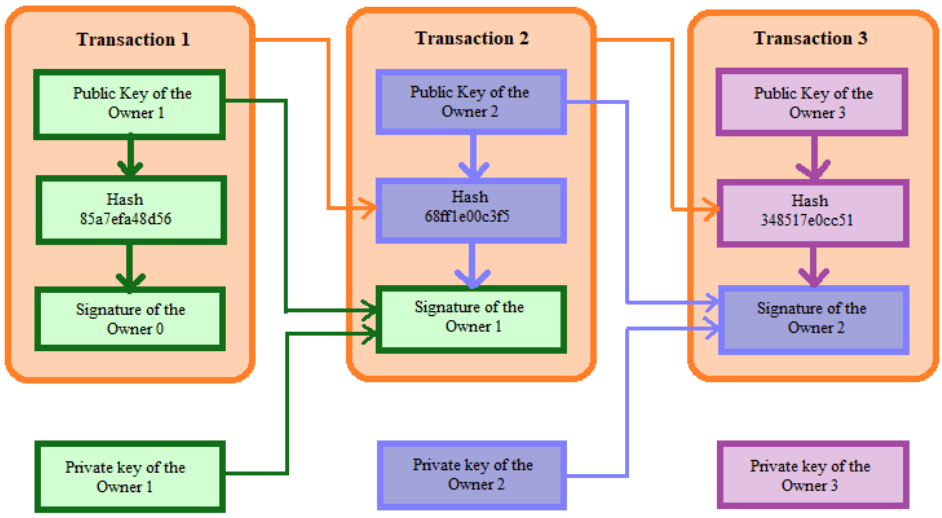
Slika 1: Redosled hash vrednosti u blockchain-u



Na *blockchain*-u upisujemo javne podatke, kao što su ID proizvoda, korisnički priručnici, smernice za odlaganje i recikliranje i podatke o transakcijama, kao što su CAD datoteke, tehničke i materijalne specifikacije, mehanička svojstva, uputstva za sastavljanje, nalozi za traženje, potpisi i ključevi za kriptografiju (Papakostas et al., 2019).

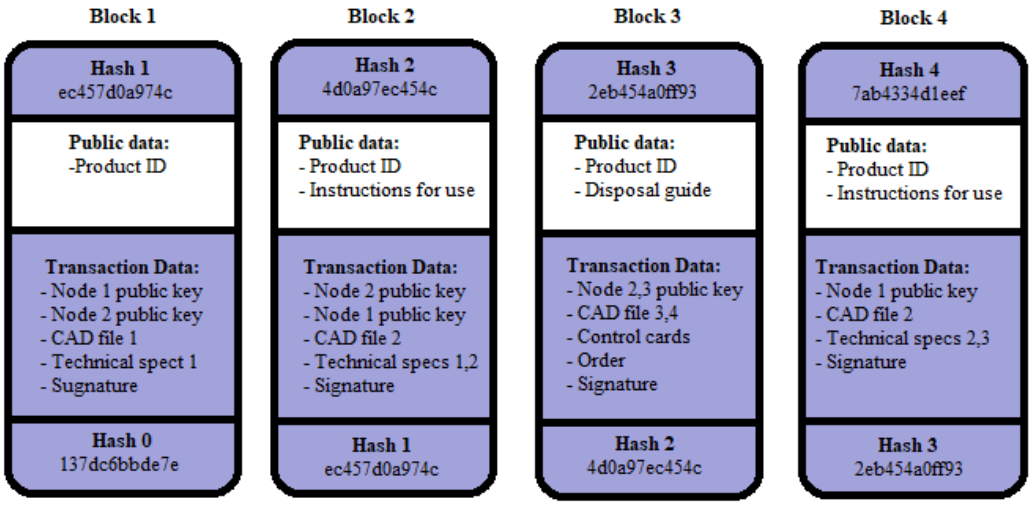
Slika 2. ilustruje procese potpisivanja i verifikacije blokova u *blockchain*-u. Proces se zasniva na kriptografiji privatnog/javnog ključa. Svaka transakcija je verifikovana javnim ključem prethodnog vlasnika bloka i potpisana njegovim privatnim ključem. *Hash* funkcija osigurava integritet podataka jer je nepovratna.

Slika 2: potpisivanje i verifikacija u blockchain-u



Uobičajena upotreba *blockchain*-a sada uključuje finansijske usluge (plaćanje, transfer novca, *benchmarking* kupaca i upravljanje životnim ciklusom pune trgovine), nabavku (sledljivost komponenti proizvoda, elektronski zapisi o usklađenosti, patenti na čekanju, podaci o kontroli kvaliteta), javni sektor (evidencija ličnih podataka kojima upravlja Vlada, uvozne/izvozne carine i porezi, regulatorne potvrde i digitalni identitet građana) i zdravstvenu zaštitu (lični zdravstveni kartoni, akreditivi pružaoca usluga i klinički podaci).
Ova lista će se verovatno proširiti a nove aplikacije se svakodnevno pojavljuju. To čini *blockchain* „rešenjem za probleme koje treba rešiti".
Na slici 3. prikazan je primer kako se *blockchain* može koristiti za omogućavanje integriteta podataka u procesu razvoja proizvoda. Svaki blok se sastoji od javnih podataka i šifrovanih podataka o transakcijama. Oba podatka se heširaju i čuvaju u šifrovanom obliku. Potpis sadrži vremensku oznaku, a svaki blok sadrži *hash* iz prethodnog bloka (Memon et al., 2020). Izmenu podataka unutra procesa može da izvrši samo vlasnik privatnog ključa i ta promena je vidljiva za ostale korisnike. Blokovi se distribuiraju unutar mreže korisnika čime se eliminiše potreba za telom za verifikaciju.

Slika 3: Blockchain osnova za razvojni proces zasnovan na CAD-u



Neke potencijalne upotrebe *blockchain*-a u građevinarstvu mogu se koristiti za:

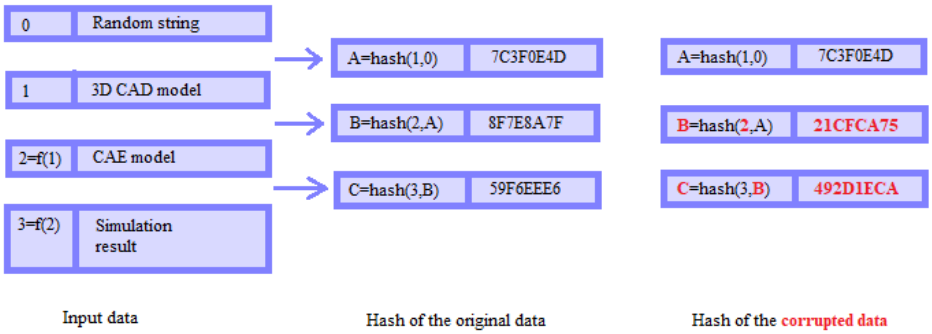
1. Čuvanje senzorskih podataka iz zgrada na pouzdan i distribuiran način, čuvanje zapisa o transakcijama vremenskim žigom, automatizovano rešavanje sporova, pametni gradovi. Predloženo je korišćenje *blockchain*-a na gradilištu kako bi se poboljšala pouzdanost građevinskih dnevnika kao i za praćenje učinka radnika i utroška materijala (Turk et al., 2017).
2. Upravljanje građevinskim inženjeringom – predložene su aplikacije koje se odnose na overavanje kako bi se eliminisao gubitak vremena za proveru autentičnosti dokumenta, aplikacije koje se odnose na transakcije kako bi se olakšala automatska nabavka i plaćanje materijala (Wang et al., 2017).
3. Potencijalna primena *blockchain*-a mogla bi da bude u fazi pripreme za izgradnju, gde je korišćenje BIM-a na maksimumu. *Blokchain* može povećati poverenje zainteresovanih strana omogućavanjem praćenja promena, utvrđivanje jasnih obaveza, pružanjem dokaza o vlasništvu nad informacijama i smanjenjem sporova oko autentičnosti informacija. Distribuirana baza podataka izbegava koncentraciju vlasništva i eliminiše zloupotrebu i korupciju informacija, čineći je pogodnom za pravne dokaze (Pradeep et al., 2019).

3. REZULTATI

Poverenje je ključna karakteristika *blockchain* tehnologije. *Blockchain* tehnologija čini svakog učesnika čuvarom svih informacija koje teku kroz životni ciklus projekta.

Slika 4. pokazuje krajnji cilj ovog rada odnosno kako se *blockchain* može implementirati u inženjersko okruženje koje se sastoji od 3D CAD modeliranja i kompjuterske simulacije (tj. statičke strukturne analize). Nasumučni niz „0“ služi kao kriptografski javni ključ i koristi se za potvrđivanje autentičnosti konačnog izlaza. CAD model „1“ se kombinuje sa slučajnim nizom „0“ i transformiše u *hesh* fiksne veličine – blok „A“, koristeći uobičajeni *hesh* algoritam. CAE model „2“ je matematički prikaz CAD modela „1“ praćen osobinama materijala, ograničenjima, silama, mrežom konačnih elemenata i opcijama izvršilaca. Kombinuje se sa heširanim potpisom bloka „A“ iz prethodnog koraka i transformiše se da u novi blok „B“. Nakon što je simulacija obavljena, rezultat simulacije „3“ se kombinuje sa heširanim potpisom bloka „B“ iz prethodnog koraka i transformiše se da bi se kreirao blok „C“.

Slika 4: Svaka promena u jednom koraku blockchain-a može se pratiti u konačnom sažetku



U slučaju da bilo koji od podataka u bilo kom koraku bude oštećen ili izmenjen od strane neovlašćenog člana tima, promene se odražavaju na blokove koji su kreirani nakon tog koraka.

4. DISKUSIJE

Ovaj rad predstavlja model integracije između CAD-a i *blockchain* tehnologije. Dalja pitanja kojima se treba pozabaviti odnosiće se na izvodljivost pisanja kodova koji mogu da rade privatne i javne mreže kao i prelazak iz CAD na BIM sisteme.

Pre korišćenja *blockchain* tehnologije u integraciji sa CAD-om neophodno je sumirati prednosti i nedostatke *blockchain*-a.

Ključne prednosti *blockchain*-a uključuju decentralizaciju, postojanost, neporicanje, anonimnost i mogućnost revizije. (Leka et el., 2019). Određeni *blockchain*, poput Ethereuma, ima i dodatne funkcije koje omogućavaju istinsku integraciju sa širom digitalnom infrastrukturom. Pametni ugovori su ugovori koji se izvršavaju unutar *blockchain*-a autonomno, bez ljudske intervencije kada dođe do određenih događaja.

Glavni nedostaci *blockchain*-a identifikovani su u: visokoj potrošnji električne energije zbog velike potrebe za računarskom snagom koja se koristi za proces proračuna, i ravnoteža između broja čvorova i povoljnih troškova

korisnika (Golosova et al., 2018). Kvantno računarstvo moglo bi biti jedno od mogućih rešenja koje bi rešilo veliku potražnju za računarskim resursima.

5. ZAKLJUČCI

Uprkos velikom potencijalu *blockchain* tehnologije u interaktivnom CAD okruženju, prednosti ove tehnologije su još uvek u ranoj fazi usvajanja. Kako *blockchain* eliminiše svaku mogućnost prevare, samim tim povećava međusobno poverenje između projektanata, izvođača radova, dobavljača i geometara. Platne transakcije mogu se automatizovati, a podaci iz bilo kog koraka u procesu su u potpunosti sledivi i zaštićeni od neovlašćenih promena, čineći proces jakim i otpornim. Drugi sektori su već prepoznali prednost *blockchain*-a, posebno finansijske usluge i usluge lanaca nabavke.

Nedostaci kao što je transparentnost podataka i sporost čuvanja podataka u *blockchain*-u, nisu ključni faktori u odlaganju implementacije ove tehnologije. Interaktivni CAD može sebi priuštiti kašnjenje u intervalu od nekoliko minuta ili sati, i nisu mu potrebni podaci u realnom vremenu. Transparentnost bi predstavljala problem kada su ugrožena prava intelektualnog vlasništva, ali *blockchain* prati sve transakcije i svako nepoštovanje autorskih prava može se lako pratiti i identifikovati, čak i uz automatsku novčanu transakciju.

Blockchain za interaktivni CAD je još uvek dostupan samo kao dodatna tehnologija koju pružaju mali distributeri, dok vodeći provajderi CAD softvera još uvek oklevaju, što zbog nedostatka informacione pismenosti što zbog oportunističkog stava.

REFERENCE

Cousins, S. (2018). French start-up develops Blockchain solution for BIM. *Retrieved April*, *14*, 2019.

Erri Pradeep, A. S., Yiu, T. W., & Amor, R. (2019). Leveraging blockchain technology in a BIM workflow: A literature review. In *International Conference on Smart Infrastructure and Construction 2019 (ICSIC) Driving data-informed decision-making* (pp. 371-380). ICE Publishing.

Ethash [*on line*]. Dostupno na: https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/mining-algorithms/ethash/#sha3

Golosova, J., & Romanovs, A. (2018, November). The advantages and disadvantages of the blockchain technology. In *2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)* (pp. 1-6). IEEE.

Gueguen, A. (2018). BIM and Blockchain an Alliance that Makes Sense. Paris, France: Lutecium SAS [*on line*]. Dostupno na: https://bimchain.io/bim-and-blockchain-an-alliance-that-makes-sense/

Kurpjuweit, S., Schmidt, C. G., Klöckner, M., & Wagner, S. M. (2021). Blockchain in additive manufacturing and its impact on supply chains. *Journal of Business Logistics*, *42*(1), 46-70.

Leka, E., Selimi, B., &Lamani, L. (2019, September). Systematic literature review of blockchain applications: Smart contracts. In *2019 International Conference on Information Technologies (InfoTech)* (pp. 1-3). IEEE.

Memon, R. A., Li, J. P., Ahmed, J., Nazeer, M. I., Ismail, M., & Ali, K. (2020). Cloud-based vs. blockchain-based IoT: a comparative survey and way forward. *Frontiers of Information Technology & Electronic Engineering*, *21*(4), 563-586.

Papakostas, N., Newell, A., & Hargaden, V. (2019). A novel paradigm for managing the product development process utilising blockchain technology principles. *CIRP Annals*, *68*(1), 137-140.

Szabo, N. (1996). Smart contracts: building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought,(16)*, *18*(2), 28.

Turk, Ž., &Klinc, R. (2017). Potentials of blockchain technology for construction management. *Procedia engineering*, *196*, 638-645.

Valero F. (2018). BIM and Blockchain. Barcelona: Zigurat Global Institute of Technology [*on line*]. Dostupno na: https://www.e-zigurat.com/en/blog/bim-and-blockchain/

Wang, J., Wu, P., Wang, X., &Shou, W. (2017). The outlook of blockchain technology for construction engineering management.