Milan Feltovic

Potenciálne využitie Blockchain technológie na modernizáciu policajných operácií: zabezpečenie bezpečnosti, transparentnosti a efektivity

Anotácia: Tento článok skúma transformačný potenciál blockchainovej technológie v policajných operáciách, zameriavajúc sa na zlepšenie bezpečnosti, transparentnosti a efektivity. Blockchain, ktorý bol spočiatku uznávaný pre svoju úlohu v kryptomenách, teraz využíva svoje vlastnosti nezmeniteľnosti a distribuovaného záznamu na revolučné zlepšenie správy dát v rámci orgánov činných v trestnom konaní. Technológia zaručuje bezpečné, auditovateľné a nezmeniteľné zaznamenávanie všetkých transakcií a dát súvisiacich s policajnými operáciami, od záznamov vyšetrovaní po správu dôkazov, pričom zaručuje prístup len oprávneným osobám.

Kľúčové oblasti skúmania zahŕňajú zlepšenie bezpečnosti a transparentnosti prostredníctvom nezmeniteľných a distribuovaných záznamov blockchainu, zabezpečenie integrity dát a správy dôkazov poskytovaním nezmeniteľného záznamu všetkých transakcií a dát a zlepšenie interoperability medzi rôznymi policajnými oddeleniami a agentúrami. Integrácia pokročilých technológií, ako sú tzv. Zero-Knowledge Proofs a *Layer 2* riešenia, ďalej posilňujú ochranu súkromia a rýchlosť operácií, čo prispieva k efektívnejšiemu a spoľahlivejšiemu informačnému systému polície.

Praktické implementácie v policajných zložkách po celom svete, napríklad iniciatíva Polície v Dillí na sledovanie dôkazov pomocou blockchainu a spolupráca Dubajskej polície s Cardano Blockchain na bezpečné zdieľanie dát, demonštrujú významné zlepšenia v transparentnosti, integrite a bezpečnosti procesov. Článok končí riešením pretrvávajúcich výziev škálovateľnosti, interoperability a ochrany súkromia, zdôrazňujúc potrebu ďalšieho vývoja a štandardizácie na plné využitie výhod blockchainu pri modernizácii policajných operácií.

Vyhodnotením týchto aspektov článok zdôrazňuje kľúčovú úlohu blockchainu v digitálnej transformácii orgánov činných v trestnom konaní, podporujúc väčšiu dôveru verejnosti a spoluprácu medzi policajnými zložkami na národnej aj medzinárodnej úrovni.

Kľúčové slová: Interoperabilita, škálovateľnosť, Zero-Knowledge dôkazy, inteligentné zmluvy, Layer 2 riešenia, blockchainové mosty, formálna verifikácia

Úvod

Blockchainová technológia, známa najmä svojím využitím v kryptomenách, nachádza nové uplatnenie v policajnom prostredí, kde prináša revolučné zlepšenia v oblasti bezpečnosti, transparentnosti a efektivity. Vďaka svojej základnej charakteristike –nezmeniteľnosti a distribuovanému záznamu – môže blockchain poskytnúť policajným zložkám efektívny nástroj na zlepšenie uchovávania a spracovania dát zaisťujúc ich ochranu, auditovateľnosť a odolnosť voči manipulácii. Implementácia blockchainu umožňuje zaznamenávať všetky transakcie a dáta spojené s policajnými operáciami, od záznamov o vyšetrovaniach po správu dôkazov, pričom zaručuje ich dostupnosť pre oprávnené osoby bez rizika neoprávneného zásahu.

Z hľadiska interoperability môže blockchain slúžiť ako spojovací most medzi rôznymi policajnými oddeleniami a agentúrami, umožňujúc bezproblémovú výmenu informácií a spoluprácu. S pridaním pokročilých technológií, napr. tzv. Zero-Knowledge[1] dôkazov či škálovacích riešení môže byť zabezpečená ochrana súkromia a zvýšená rýchlosť operácií, čo prispieva k vytvoreniu efektívnejšieho a spoľahlivejšieho informačnému systému polície. Tieto výhody predstavujú zásadný posun k modernizácii a digitalizácii policajných operácií v súčasnom digitálnom veku.

Tento článok o využití blockchainovej technológie v policajnom prostredí sa zameriava na zodpovedanie troch hlavných otázkok:

[1] ROSIC, Ameer. *Zero Knowledge Proofs*. blockgeeks.com. [online]. 2023. [cit. 22. júla 2024]. Dostupné na internete: https://blockgeeks.com/guides/zero-knowledge-proofs/.

1. **Ako môže blockchain zlepšiť bezpečnosť a transparentnosť v policajných operáciách?** Článok skúma, ako základné vlastnosti blockchainu, ako sú nezmeniteľnosť a distribuované záznamy, prispievajú k ochrane a transparentnosti spracovania citlivých policajných dát.
2. **Akým spôsobom môže blockchain zabezpečiť integritu dát a správu dôkazov v policajnom prostredí?** Článok analyzuje, ako implementácia blockchainu umožňuje nezmeniteľné zaznamenávanie všetkých transakcií a dát, čo zaručuje ich dostupnosť len pre oprávnené osoby a ochranu pred neoprávneným zásahom.
3. **Ako môže blockchain zvýšiť interoperabilitu medzi rôznymi policajnými zložkami a agentúrami?** Článok preskúma, ako blockchain môže slúžiť ako most pre spojenie rôznych policajných zložiek na zvýšenie efektivity a spolupráce a akú úlohu v tom plnia pokročilé technológie, ako sú Zero-Knowledge dôkazy a škálovateľné riešenia.

Metódy

Blockchainová technológia[2], ktorá sa často spája s finančným sektorom a kryptomenami, sa postupne začína uplatňovať aj v policajnom prostredí. Jej implementácia prichádza s významným potenciálom pre zlepšenie správy dát, zvýšenie bezpečnosti a efektivitu operácií, najmä vďaka jej schopnosti zabezpečiť dôvernosť a integritu policajných záznamov. Jej nasadenie v policajných systémoch sa stáva čoraz relevatnejším, keďže poskytuje riešenia pre niektoré z najakútnejších problémov súčasných bezpečnostných síl – ako sú zabezpečenie dôvernosti, integrita dát a zlepšenie medziagentúrnej spolupráce.

Jadro blockchainovej technológie spočíva v jej schopnosti udržiavať distribuovaný, decentralizovaný a nezmeniteľný záznam transakcií. Táto inherentná vlastnosť umožňuje policajným oddeleniam viesť nezmeniteľné a transparentné evidencie, čo je zásadné pre právne a vyšetrovacie procesy. Každý záznam uložený na blockchaine je chránený proti manipulácii, čo zvyšuje dôveru v autenticitu policajných záznamov a dôkazov.

Výhody nasadenia blockchainu v policajnom prostredí siahajú od zvýšenej transparentnosti a zabezpečenia až po zlepšenie spolupráce medzi rôznymi orgánmi činnými v trestnom konaní. Transparentnosť poskytovaná blockchainovou technológiou umožňuje účinný audit a kontrolu operácií, zatiaľ čo jej schopnosť zabezpečiť dáta môže pomôcť chrániť citlivé informácie a zároveň uľahčuje zdieľanie dát medzi jurisdikciami bez obáv z ich zneužitia alebo straty.

Na druhej strane interoperabilita medzi rôznymi blockchainovými platformami môže podporiť bezproblémový prenos informácií medzi policajnými zložkami a agentúrami, čo je často komplikované kvôli nekompatibilným systémom a protokolom. Blockchain by tu mohol slúžiť ako jednotný formát pre zdieľanie dát, čím by sa zjednodušila komunikácia. ako aj spolupráca.

Zavedenie blockchainu však vyžaduje aj dôkladné zváženie technických, právnych a operatívnych výziev vrátane otázok súkromia, škálovateľnosti a integrácie s existujúcimi IT systémami. Tento úvod do problematiky teda nastavuje scénu pre hlbšiu diskusiu
o konkrétnych technológiách, ktoré môžu tieto výzvy riešiť, a skúma, ako môžu byť tieto technológie prispôsobené na splnenie špecifických potrieb policajných orgánov.

Blockchain v prostredí polície

Blockchainová technológia pôvodne vytvorená pre kryptomeny ako Bitcoin predstavuje významný nástroj pre policajné prostredie. Jej schopnosť zabezpečiť nezmeniteľnosť, transparentnosť a bezpečnosť dát otvára nové možnosti pre správu dôkazov, sledovanie vyšetrovaní a zabezpečenie informácií. V policajnom prostredí, kde sú dôvera a integrita na

[2] NAKAMOTO, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. bitcoin.org. [online]. 2008. [cit. 22. júla 2024]. Dostupné na internete: https://bitcoin.org/en/bitcoin-paper.

prvom mieste, môže blockchain poskytnúť platformu, ktorá zaručuje, že každý záznam je trvalý a nezmeniteľný. Táto technológia umožňuje automatické zaznamenávanie každej transakcie alebo úpravy v dátach, čo policajným zložkám umožňuje viesť presné a transparentné záznamy. Implementácia blockchainu do policajných operácií môže zároveň zvýšiť verejnú dôveru v ich činnosť a zlepšiť medziagentúrnu spoluprácu.

1. Škálovateľnosť riešenia

Jednou z najväčších výziev, ktorým čelí blockchain technológia, je škálovateľnosť. To znamená schopnosť systému efektívne riešiť zvyšujúce sa množstvo transakcií a dát bez významného poklesu výkonnosti. V policajnom prostredí, kde môže byť zaznamenané obrovské množstvo dát z rôznych zdrojov, je kriticky dôležité, aby blockchainová platforma bola schopná spracovať a uchovať tieto dáta rýchlo a bezpečne. Nasledovné technológie sú nevyhnutné pre zabezpečenie, aby blockchainové systémy používané v policajných operáciách boli dostatočne rýchle, bezpečné a schopné riešiť náročné úlohy spojené s moderným vyšetrovaním a správou dát:

Sharding[3] je proces rozdeľovania celkovej databázy blockchainu na menšie segmenty, známe ako „shardy“. Každý shard obsahuje nezávislú časť dát, čím sa umožňuje paralelné spracovanie transakcií. Toto výrazne zvyšuje celkovú škálovateľnosť a výkon siete tým, že rozkladá záťaž na viaceré uzly, ktoré môžu operovať simultánne.

V policajnom blockchain systéme by sharding mohol pomôcť rýchlejšie spracovávať dáta z rôznych zdrojov, ako sú záznamy z kamerových systémov, databázy biometrických údajov alebo evidencie volaní, čím zefektívňuje vyšetrovanie a sledovanie prípadov.

Layer 2 Solutions[4] sú navrhnuté tak, aby poskytli alternatívne metódy pre transakcie a interakcie mimo hlavný blockchain (Layer 1)[5], čo znižuje záťaž a zlepšuje rýchlosť transakcií. Medzi najznámejšie patria:

- **Lightning Network**[6] je protokol druhej vrstvy navrhnutý pre blockchainy ako Bitcoin. Umožňuje rýchle a takmer bezpoplatkové transakcie tým, že transakcie prebiehajú mimo hlavný blockchain a na hlavný reťazec sa zaznamenávajú iba konečné saldá. Môže byť použitý pre rýchle a efektívne mikroplatby medzi rôznymi policajnými a bezpečnostnými agentúrami, čo zvyšuje operatívnu spoluprácu a efektivitu.

- **Rollups**[7] sú tiež riešenia druhej vrstvy, ktoré spracovávajú a ukladajú transakčné dáta mimo hlavný blockchain, ale zároveň zabezpečujú ich integritu pomocou smart kontraktov. Existujú dva hlavné typy Rollups: Optimistic Rollups a Zero-knowledge Rollups, pričom oba poskytujú rôzne úrovne bezpečnosti a efektivity. Rollups môžu zvýšiť schopnosť blockchainu spracovávať veľké množstvo transakcií, čo je

[3] MEARIAN, L. *Sharding*. computerworld.com. [online]. 2019. [cit. 22. júla 2024]. Dostupné na internete: https://www.computerworld.com/article/1716485/sharding-what-it-is-and-why-so-many-blockchain-protocols-rely-on-it.html.

[4] ANON. *Layer 2*. ethereum.org. [online]. 2024. [cit. 23. júla 2024]. Dostupné na internete: https://ethereum.org/en/layer-2/.

[5] ANON. *Layer 1 vs. Layer 2*. academy.binance.com. [online]. 2022. [cit. 23. júla 2024]. Dostupné na internete: https://academy.binance.com/en/articles/blockchain-layer-1-vs-layer-2-scaling-solutions.

[6] NETWORK LIGHTNING. *Lightning Network*. lightning.network. [online]. 2024. [cit. 23. júla 2024]. Dostupné na internete: https://lightning.network/.

[7] LEDGER. *Blockchain Rollups*. www.ledger.com. [online]. 2023. [cit. 24. júla 2024]. Dostupné na internete: https://www.ledger.com/academy/what-are-blockchain-rollups.

užitočné pri spracovaní veľkého objemu dôkazov alebo pri monitorovaní rozsiahlych policajných operácií.

2. Interoperabilita

Interoperabilita v kontexte blockchain technológie odkazuje na schopnosť rôznych blockchainových systémov a protokolov vzájomne komunikovať a spolupracovať. Táto schopnosť je zásadná pre policajné systémy, kde rôzne zložky a oddelenia často potrebujú zdieľať informácie a koordinovať operácie naprieč rôznymi platformami. Efektívna interoperabilita umožňuje, aby sa dáta a aktíva bezpečne a plynule presúvali medzi rôznymi blockchainmi bez kompromisu o ich bezpečnosť alebo integritu. Nasledovné technológie predstavujú pokročilé riešenia, ktoré môžu v policajnom prostredí zvýšiť interoperabilitu, zlepšiť bezpečnosť a zjednodušiť procesy zdieľania informácií.

Integráciou týchto technológií môžu policajné zložky výrazne zlepšiť svoje operácie a posilniť spoluprácu na národnej aj medzinárodnej úrovni.

Blockchain Bridges (Blockchainové mosty)[8] sú technológie, ktoré umožňujú prenos dát a hodnôt medzi dvoma rôznymi blockchainmi, ktoré by inak neboli priamo kompatibilné. Tieto premostenia fungujú ako mediátory, ktoré zabezpečujú, že transakcie a informácie môžu byť prenášané medzi rôznymi sieťami bez nutnosti opustiť ich pôvodné blockchainové prostredie.

V policajnom prostredí môžu blockchainové mosty zohrávať kľúčovú úlohu pri zdieľaní informácií o páchateľoch, dôkazoch alebo pri medzinárodnej spolupráci medzi orgánmi činnými v trestnom konaní. Tým, že umožňujú bezpečný a kontrolovaný prenos dát medzi rôznymi blockchainovými systémami, môžu orgány z rôznych krajín efektívne spolupracovať, aj keď používajú odlišné technológie alebo majú rozdielne právne požiadavky na ochranu dát.

Blockchainové mosty pomáhajú zabezpečiť súlad s právnymi predpismi v rôznych štátoch tým, že umožňujú implementáciu prispôsobených pravidiel prístupu a overovania pri prenose dát. Napríklad pri **prispôsobení právnym normám** môžu byť do blockchainového mosta integrované špecifické právne požiadavky každej jurisdikcie, ako sú zákony o ochrane osobných údajov, pravidlá pre uchovávanie dôkazov či predpisy týkajúce sa kybernetickej bezpečnosti. **Kontrola prístupu** umožňuje nastaviť detailné oprávnenia, aby k citlivým informáciám mali prístup iba oprávnené osoby podľa legislatívy danej krajiny. **Auditovateľnosť a transparentnosť** sú zabezpečené tým, že všetky prenosy dát sú zaznamenané a sledovateľné, čo orgánom umožňuje preukázať, že postupovali v súlade s právnymi predpismi, čo uľahčuje riešenie prípadných sporov alebo vyšetrovaní. **Šifrovanie a bezpečnosť** zaručujú, že prenášané dáta môžu byť šifrované podľa bezpečnostných štandardov požadovaných v jednotlivých krajinách, čím sa zabezpečuje ich ochrana počas prenosu.

Týmto spôsobom blockchainové mosty nielen zlepšujú technickú interoperabilitu medzi rôznymi systémami, ale takisto orgánom činným v trestnom konaní umožňujú spolupracovať spôsobom, ktorý je v súlade s právnymi a regulačnými požiadavkami každej zúčastnenej jurisdikcie. To napomáha efektívnejšej medzinárodnej policajnej spolupráci a zvyšuje dôveru medzi partnermi z rôznych krajín.

Polkadot[9] je multichainová škálovateľná platforma, ktorá umožňuje interoperabilitu medzi viacerými blockchainmi. Polkadot sa skladá z hlavného blokového reťazca známeho ako

[8] STEVENS, R. *What Are Blockchain Bridges*. www.coindesk.com. [online]. 2022. [cit. 24. júla 2024]. Dostupné na internete: https://www.coindesk.com/learn/what-are-blockchain-bridges-and-how-do-they-work/.

[9] POLKADOT. *Polkadot's technology*. polkadot.network. [online]. 2024. [cit. 24. júla 2024]. Dostupné na internete: https://polkadot.network/.

Relay Chain a množstva paralelných reťazcov známych ako parachains. Táto unikátna architektúra umožňuje blockchainom, ktoré fungujú na platforme Polkadot, zdieľať bezpečnosť, zatiaľ čo stále môžu operovať nezávisle. Polkadot môže poskytnúť policajným organizáciám platformu, kde môžu rôzne databázy a systémy komunikovať a spolupracovať v reálnom čase, zjednodušujúc komplexné operácie, ako sú cezhraničné vyšetrovania alebo sledovanie medzinárodného organizovaného zločinu.

Cosmos[10] je projekt zameraný na riešenie problémov škálovateľnosti a interoperability v blockchain ekosystéme. Ako „Internet blockchains“, Cosmos umožňuje rôznym blockchainom pracovať spolu prostredníctvom protokolu IBC (Inter-Blockchain Communication). Cosmos sa zameriava na vytvorenie ekosystému, v ktorom si každý blockchain môže zachovať svoju nezávislosť, ale zároveň efektívne komunikovať a spolupracovať s inými sieťami. Cosmos môže slúžiť ako základ pre vytvorenie decentralizovanej siete policajných záznamov, kde rôzne oddelenia a agentúry môžu bezpečne a transparentne zdieľať dôležité informácie bez obáv z izolácie dát alebo nedostatku kompatibility medzi systémami.

3. Zvýšenie ochrany súkromia

Ochrana súkromia je základným aspektom pri zavádzaní technologických inovácií v policajných operáciách, najmä pokiaľ ide o manipuláciu a spracovanie citlivých údajov.

Nasledovné technológie poskytujú robustné riešenia na zlepšenie ochrany súkromia v policajných aplikáciách, ktoré závisia od spracovania a zdieľania citlivých a osobných údajov. Zero-Knowledge dôkazy zabezpečujú, že môžete dokázať pravdivosť dát bez odhalenia samotných údajov, zatiaľ čo homomorfné šifrovanie umožňuje spracovávať dáta bez ich dešifrovania, čím znižuje riziko úniku alebo zneužitia informácií. Tieto technológie sú preto zásadné pre zvyšovanie dôvery verejnosti a integritu policajných operácií v digitálnej dobe.

Zero-Knowledge dôkazy (ZKP) sú pokročilé kryptografické metódy, ktoré umožňujú jednej strane (dokazovateľovi) preukázať druhej strane (overovateľovi), že určité tvrdenie je pravdivé, bez toho, aby odhalila akékoľvek ďalšie informácie okrem samotnej pravdivosti tvrdenia. Táto technológia je mimoriadne cenná v situáciách, kde je potrebné overiť autenticitu alebo pravdivosť údajov bez kompromitovania ich dôvernosti.

V policajnom prostredí môžu byť **Zero-Knowledge dôkazy (ZKP)** využité v rôznych oblastiach na zvýšenie ochrany súkromia a bezpečnosti. **Pri overovaní totožnosti bez odhalenia osobných údajov** je často potrebné potvrdiť, či osoba spĺňa určité kritériá, napríklad, či má vek nad 18 rokov alebo platný vodičský preukaz, bez prístupu k jej úplným osobným údajom. ZKP umožňujú jednotlivcom preukázať tieto skutočnosti bez odhalenia mena, dátumu narodenia či iných citlivých informácií, čo je obzvlášť užitočné pri ochrane súkromia občanov počas bežných kontrol.

Pri bezpečnej výmene informácií medzi orgánmi môže byť potrebné overiť, či určitý podozrivý figuruje v databázach iných krajín, bez odhalenia ďalších informácií o osobe. ZKP umožňujú overiť prítomnosť osoby v databáze bez odhalenia akýchkoľvek ďalších údajov o nej, čím sa zabezpečuje efektívna spolupráca pri rešpektovaní zákonov o ochrane osobných údajov jednotlivých krajín.

Pri overovaní autenticity digitálnych dôkazov je kľúčové preukázať, že dôkazy neboli pozmenené od ich získania. ZKP umožňujú preukázať integritu digitálnych súborov bez

[10] COSMOS.. *Build on the Interchain*. [online]. 2024. [cit. 24. júla 2024]. Dostupné na internete: https://cosmos.network/.

odhalenia ich obsahu, čo je dôležité v prípadoch, kde obsah môže byť citlivý alebo nevhodný na verejné zverejnenie.

Ochrana identity svedkov a informátorov je ďalším príkladom, kde môžu byť ZKP použité. Umožňujú overiť dôveryhodnosť svedkov alebo informátorov bez odhalenia ich totožnosti. Napríklad svedok môže preukázať, že bol prítomný na mieste činu alebo že má prístup k určitým informáciám, bez toho, aby odhalil svoju identitu alebo zdroj informácií.

Prínosy implementácie Zero-Knowledge dôkazy zahŕňajú predovšetkým ochranu súkromia, keďže umožňujú policajným orgánom získavať potrebné overenia bez zhromažďovania nadmerných osobných údajov, čím sa znižuje riziko úniku alebo zneužitia citlivých informácií. Takisto minimalizáciou množstva zdieľaných údajov zvyšujú bezpečnosť, čo znižuje povrch pre potenciálne kybernetické útoky. Týmto spôsobom pomáhajú dodržiavať legislatívu o ochrane údajov, ako je GDPR, keďže spracovanie osobných údajov je obmedzené na nevyhnutné minimum. Navyše umožňujú efektívnu medzinárodnú spoluprácu tým, že zabezpečujú bezpečné overovanie informácií medzi rôznymi jurisdikciami bez porušenia miestnych zákonov o ochrane súkromia.

Výzvy a obmedzenia implementácie Zero-Knowledge dôkazov zahŕňajú ich technickú náročnosť, keďže vyžadujú pokročilé kryptografické znalosti a môžu byť zložité na integráciu do existujúcich systémov. Navyše sú často výpočtovo intenzívne, čo môže spomaliť rýchlosť operácií, najmä pri spracovaní veľkých objemov dát. Neexistencia jednotných štandardov môže tiež komplikovať interoperabilitu medzi rôznymi systémami a organizáciami, čo sťažuje širšie nasadenie tejto technológie.

Praktický príkladom využitia Zero-Knowledge dôkazov je situácia, keď policajné oddelenie potrebuje overiť, či osoba má platné bezpečnostné previerky na prístup do citlivej oblasti, bez odhalenia detailov týchto previerok. Pomocou ZKP môže byť potvrdené, že osoba spĺňa požadované kritériá, bez zverejnenia akýchkoľvek ďalších informácií o jej previerkach. Podobne pri overovaní biometrických údajov, ako sú odtlačky prstov alebo rozpoznávanie tváre, ZKP umožňujú potvrdiť zhodu s databázou hľadaných osôb bez odhalenia samotných biometrických dát alebo identít jednotlivcov, ktorí nie sú hľadaní. Tým sa zachováva súkromie občanov a zároveň sa zabezpečuje efektívnosť policajných operácií.

Homomorphic Encryption (Homomorfné šifrovanie)[11] je pokročilá kryptografická technika, ktorá umožňuje vykonávanie výpočtov na zašifrovaných dátach bez potreby ich dešifrovania. To znamená, že dáta môžu byť spracovávané a analyzované, zatiaľ čo zostávajú v zašifrovanej forme, čím sa výrazne znižuje riziko ich neoprávneného prístupu alebo úniku.

Konkrétne využitia v policajnom prostredí:

Pri analýze citlivých údajov môžu policajné zložky vykonávať štatistické analýzy na dátach, ako sú záznamy o trestných činoch, bez toho, aby odhalili individuálne údaje. Napríklad, môžu identifikovať trendy v kriminalite alebo určiť hotspoty bez prístupu k osobným údajom jednotlivcov. Homomorfné šifrovanie takisto umožňuje tréning strojových modelov na citlivých dátach bez ich dešifrovania, čo je užitočné pri prediktívnom modelovaní a identifikácii potenciálnych hrozieb v rámci prediktívneho policajného výskumu.

Pri bezpečnom vyhľadávaní v databázach môžu policajti prehľadávať zašifrované záznamy bez toho, aby odhalili obsah svojich dotazov alebo samotné údaje v databáze. Napríklad, overenie prítomnosti osoby v zozname hľadaných osôb sa dá vykonať bez odhalenia identity iných osôb v databáze. Homomorfné šifrovanie zabezpečuje aj **ochranu údajov pri využívaní cloudových služieb**, takže poskytovateľ cloudovej platformy nemá prístup k obsahu dát, zatiaľ

[11] LIU, B. *Homomorphic encryption*. blockworks.co. [online]. 2024. [cit. 24. júla 2024]. Dostupné na internete: https://blockworks.co/news/what-is-fully-homomorphic-encryption.

čo policajné zložky môžu vykonávať potrebné operácie a analýzy. **Pri medziagentúrnej spolupráci** umožňuje táto technológia zdieľanie a analýzu dát medzi rôznymi policajnými a bezpečnostnými agentúrami bez odhalenia citlivých informácií, čo je užitočné napríklad pri spoločných vyšetrovaniach na identifikáciu spoločných bodov záujmu.

Homomorfné šifrovanie poskytuje **maximálnu ochranu súkromia**, pretože dáta zostávajú chránené počas celého životného cyklu – od uloženia až po spracovanie, čím sa minimalizuje riziko úniku citlivých informácií. **Znižuje tiež riziko interných hrozieb**, pretože ani zamestnanci organizácie nemajú prístup k dešifrovaným dátam, čo bráni zneužitiu informácií zvnútra. Okrem toho táto technológia **pomáha dodržiavať zákony o ochrane osobných údajov a súkromia**, ako je napríklad GDPR, čím sa zabezpečuje súlad s legislatívnymi požiadavkami.

Homomorfné šifrovanie je výrazne **náročné na výpočtový výkon** v porovnaní s tradičnými metódami šifrovania, čo môže spomaliť operácie a vyžadovať výkonnejší hardvér alebo optimalizované algoritmy. Jeho implementácia je komplexná a vyžaduje špecializované znalosti v kryptografii, čo môže sťažiť integráciu do existujúcich systémov bez narušenia ich funkčnosti. Homomorfné šifrovanie navyše **nepodporuje efektívne všetky typy výpočtov**, čo môže viesť k potrebným kompromisom medzi úrovňou šifrovania a výkonom.

Homomorfné šifrovanie môže byť využité **pri finančných vyšetrovaniach**, kde umožňuje analyzovať údaje od rôznych bánk bez toho, aby boli odhalené citlivé informácie o klientoch, a tým pomáha odhaliť nezrovnalosti či podvody. **Pri biometrickom overovaní** môže polícia porovnávať biometrické údaje, ako sú odtlačky prstov alebo skeny dúhovky s databázou hľadaných osôb bez odhalenia samotných biometrických údajov, čím sa chráni súkromie občanov. **V prediktívnych policajných modeloch** zase umožňuje analýzu veľkého množstva dát na predpovedanie kriminality v určitých oblastiach bez priameho prístupu k surovým údajom, čo znižuje riziko narušenia súkromia.

Riešenie výziev spojených s homomorfným šifrovaním zahŕňa **optimalizáciu algoritmov**, kde výskum napreduje k efektívnejším metódam s nižšími nárokmi na výpočtový výkon. **Použitie hybridných systémov**, ktoré kombinujú homomorfné šifrovanie s inými kryptografickými technikami, môže dosiahnuť rovnováhu medzi bezpečnosťou a výkonom. Ďalším riešením je **investícia do vzdelávania technického personálu**, čo pomôže prekonať bariéry v implementácii a údržbe týchto systémov.

Zero-Knowledge dôkazy sú vhodné na overenie konkrétnych tvrdení, ako napríklad potvrdenie veku nad 18 rokov bez toho, aby sa odhalili akékoľvek ďalšie údaje. Na druhej strane **homomorfné šifrovanie** umožňuje vykonávať komplexné výpočty priamo na zašifrovaných dátach, čo je užitočné pri analýze veľkých dátových súborov bez odhalenia ich obsahu. Zatiaľ čo Zero-Knowledge dôkazy sú ideálne pre overovanie jednotlivých faktov, homomorfné šifrovanie je lepšie pre hĺbkovú analýzu a spracovanie dát.

Homomorfné šifrovanie predstavuje dôležitý pokrok v bezpečnom spracovaní dát, umožňujúc policajným zložkám efektívne pracovať s citlivými informáciami bez kompromitovania súkromia občanov. Hoci sú s touto technológiou stále spojené technické výzvy, jej potenciál je značný. Očakáva sa, že s ďalším vývojom a optimalizáciou bude homomorfné šifrovanie v budúcnosti čoraz viac využívané v bezpečnostnom sektore.

4. Vylepšenia účinnosti

Účinnosť blockchainových systémov je kritická najmä pri aplikáciách, ktoré vyžadujú rýchle a spoľahlivé spracovanie veľkého objemu transakcií, ako je to v prípade policajných a bezpečnostných aplikácií. Tradičný mechanizmus konsenzu Proof of Work (PoW), používaný napríklad v Bitcoine, je často kritizovaný za svoju energetickú náročnosť a pomalosť. Ako alternatívu ponúkajú moderné blockchainy rôzne formy mechanizmu Proof of Stake (PoS),

ktoré sú energeticky efektívnejšie a rýchlejšie. Moderné formy PoS predstavujú značnú výhodu pre aplikácie v policajnom sektore, kde sú kľúčové rýchlosť, efektivita a bezpečnosť pri spracovaní a uchovávaní dát. Každý z týchto mechanizmov konsenzu ponúka unikátne výhody, ktoré môžu pomôcť zabezpečiť, že policajné blockchainové platformy sú spoľahlivé, dostupné a odolné voči zneužitiu.

Proof of Stake (PoS) [12] je algoritmus dosahovania konsenzu v blockchain sieti, ktorý vyžaduje, aby účastníci, známi ako validátori, držali určité množstvo mincí alebo tokenov ako "stávku". V porovnaní s PoW, PoS nemá minerov, ktorí by vykonávali energeticky náročné výpočty, ale namiesto toho sa pravdepodobnosť, že validátor bude vybraný na vytvorenie nového bloku, odvíja od veľkosti jeho stávky. V policajnom prostredí môže PoS zvýšiť rýchlosť transakcií a znižovať operatívne náklady policajných blockchainových aplikácií, čo je dôležité pre rýchle spracovanie prípadov a efektívne zdieľanie informácií.

Delegated PoS (DPoS) [13] je ďalšia vrstva vývoja PoS, kde držitelia tokenov hlasujú za „delegátov“, ktorí budú zodpovední za validáciu blokov transakcií. Tento systém je často považovaný za demokratickejší a efektívnejší, pretože znižuje počet účastníkov potrebných na dosiahnutie konsenzu, čo môže výrazne zvýšiť rýchlosť transakcií. V policajnom prostredí by DPoS mohol zabezpečiť, že len overené a dôveryhodné uzly (delegáti) by mohli spracovávať a validovať policajné dáta, čo znižuje riziko neautorizovaného prístupu a zlepšuje celkovú bezpečnosť siete.

Liquid Proof of Stake (LPoS) [14] je varianta PoS, ktorá umožňuje držiteľom tokenov delegovať svoje stávkovacie práva na iné uzly bez toho, aby museli svoje tokeny fyzicky prenášať alebo ich uzamykať. Táto flexibilita znamená, že účastníci môžu rýchlo meniť, koho autorizujú na validáciu transakcií, čo prináša dynamickosť a adaptabilitu do procesu dosahovania konsenzu.

LPoS by mohol poskytnúť policajným organizáciám schopnosť rýchlo prispôsobiť svoje siete zmenám v operačných požiadavkách alebo reagovať na vnútorné alebo vonkajšie hrozby, zvyšujúc tým bezpečnosť a reaktivitu systému.

5. Vylepšenia inteligentných zmlúv a formálna verifikácia

Smart kontrakty (inteligentné zmluvy) sú programovateľné skripty uložené na blockchaine, ktoré sa automaticky vykonávajú, keď sú splnené vopred definované podmienky. V policajnom prostredí môžu inteligentné zmluvy automatizovať a zefektívniť rôzne administratívne a operatívne procesy, pričom zabezpečujú transparentnosť a dôveryhodnosť.

V policajnej praxi možno inteligentné zmluvy implementovať na viaceré účely. Napríklad na **automatizáciu administratívnych procesov**, ako je spracovanie žiadostí o povolenia, registrácia vozidiel alebo vydávanie licencií, čím sa znižuje administratívna záťaž pre personál a minimalizuje riziko ľudských chýb. **Pri správe a sledovaní dôkazov** je kľúčové zabezpečiť ich integritu. Inteligentné zmluvy dokážu automaticky zaznamenávať každý úkon s dôkazom na blockchaine, čím vytvárajú nezmeniteľný a auditovateľný záznam v súlade

[12] NAPOLETANO, Erika a B. CURRY. *Proof-of-Stake*. www.forbes.com. [online]. 2023. [cit. 25. júla 2024]. Dostupné na internete: https://www.forbes.com/advisor/investing/cryptocurrency/proof-of-stake/.
[13] GAURAV, R. *Delegated Proof-of-Stake*. www.ledger.com. [online]. 2023. [cit. 25. júla 2024]. Dostupné na internete: https://www.ledger.com/academy/what-is-delegated-proof-of-stake-dpos.
[14] BAGATARHAN, G. *Liquid Proof Of Stake*. metatime.com. [online]. 2024. [cit. 25. júla 2024]. Dostupné na internete: https://metatime.com/en/blog/what-is-liquid-proof-of-stake-lpos-how-does-it-work.

s právnymi predpismi. Okrem toho inteligentné zmluvy môžu **riadiť prístup k citlivým informáciám** v databázach, zabezpečujúc, že k nim majú prístup len oprávnené osoby.

Pri implementácii inteligentných zmlúv je kľúčové zabezpečiť, aby boli **v súlade s platnou legislatívou** a rešpektovali ústavné princípy, ako sú zásada zdržanlivosti a práva na spravodlivý proces. Tieto zmluvy by mali slúžiť ako podporný nástroj pre príslušníkov polície a ostatné orgány činné v trestnom konaní, a nie ako náhrada ich rozhodovacej právomoci.

Príklad: Vydávanie povolení na zadržanie

Inteligentná zmluva môže podporiť rozhodovací proces pri vydávaní povolení na zadržanie tým, že pomáha overovať splnenie formálnych náležitostí žiadosti, ako sú úplnosť dokumentácie alebo dodržanie procesných lehôt. Všetky kroky v procese žiadosti môžu byť zaznamenané na blockchaine, čo umožňuje spätnú kontrolu a zvyšuje dôveru v zákonnosť postupu.

Vylepšenia inteligentných zmlúv a ich aktualizácie, ktoré zabezpečujú ich aktuálnosť, bezpečnosť a optimalizáciu v súlade s najnovšími technologickými štandardmi a bezpečnostnými požiadavkami. Vzhľadom na dynamickú povahu digitálnych hrozieb a neustále sa meniace technologické prostredie je nevyhnutné, aby inteligentné zmluvy prechádzali pravidelnými aktualizáciami s cieľom predchádzať zraniteľnostiam a zneužitiu. V policajných systémoch môžu inteligentné zmluvy automatizovať a uľahčovať procesy, ako sú registrácia a sledovanie prípadov, správa súdnych príkazov a riadenie prístupu k dôkazom. Aktualizácie zabezpečia, že tieto procesy sú vykonávané správne s plným dodržiavaním právnych predpisov a operačných protokolov.

Formal Verification[15] (Formálna verifikácia inteligentných zmlúv) je proces matematického overenia správnosti kódu inteligentných zmlúv, ktorý zabezpečuje, že zmluvy fungujú presne podľa stanovených špecifikácií a neobsahujú chyby či zraniteľnosti. V kontexte policajných operácií je tento proces kritický z viacerých dôvodov. Po prvé, **zaisťuje bezpečnosť** tým, že zabraňuje neoprávnenému prístupu alebo manipulácii s citlivými údajmi. Po druhé, formálna verifikácia **zabezpečuje zákonnosť** implementácie inteligentných zmlúv, čím sa dodržiavajú právne predpisy a chráni základné práva a slobody. Nakoniec, tento proces **zvyšuje spoľahlivosť systémov** tým, že eliminuje chyby, ktoré by mohli viesť k nesprávnym rozhodnutiam alebo narušeniu procesov, čím sa zaisťuje hladký a efektívny priebeh policajných operácií.

Implementácia formálnej verifikácie v praxi zahŕňa niekoľko kľúčových krokov. Pred začiatkom verifikácie je nevyhnutné presne definovať požiadavky a očakávané správanie inteligentnej zmluvy v súlade s platnými právnymi normami a internými predpismi. Následne sa využívajú formálne metódy, ako sú špecializované nástroje a techniky (napr. model checking, theorem proving) na matematické overenie správnosti kódu zmluvy. Okrem toho je dôležitá spolupráca s právnymi expertmi, ktorí zabezpečujú, že zmluvy neporušujú zákony a rešpektujú procesné postupy. Pred nasadením do prevádzky by inteligentné zmluvy mali byť podrobené dôkladnému testovaniu a nezávislému auditu, aby sa overila ich funkčnosť a bezpečnosť.

Formálna verifikácia prináša **zvýšenú dôveru**, keďže orgány a verejnosť môžu mať väčšiu dôveru v systémy, ktoré prešli formálnym overením. Táto metóda tiež **minimalizuje riziko** zlyhania systémov alebo právnych následkov spôsobených nesprávnym fungovaním

[15] PETTINARI, P. *Formal Verification*. ethereum.org. [online]. 2023. [cit. 25. júla 2024]. Dostupné na internete: https://ethereum.org/en/developers/docs/smart-contracts/formal-verification/#drawbacks-of-formal-verification.

zmlúv. Okrem toho formálna verifikácia **zvyšuje efektívnosť** tým, že predchádza nákladným opravám a právnym sporom spôsobeným chybami v systéme.

Implementácia inteligentných zmlúv a formálnej verifikácie v policajnom prostredí ponúka významné výhody v oblasti efektivity a transparentnosti. Úspešné nasadenie však vyžaduje dôkladné plánovanie, spoluprácu medzi technickými a právnymi odborníkmi a dôraz na dodržiavanie legislatívnych a etických štandardov. Technológia by mala byť využitá na podporu a zefektívnenie práce policajných orgánov, pričom konečné rozhodovacie právomoci zostávajú v rukách oprávnených osôb.

Postavenie známej Fuzzy Hash technológie

Fuzzy hashing[16], známy aj ako kontextovo citlivé hashovanie alebo hashovanie po častiach citlivé na kontext (v angličtine *Context-Triggered Piecewise Hashing*), je pokročilá kryptografická metóda, ktorá umožňuje identifikovať a porovnávať podobné, nielen identické, súbory alebo dátové bloky. Táto technológia je obzvlášť užitočná v situáciách, kde existujú malé rozdiely v dátach, ktoré by tradičné hashovacie metódy nezachytili. V policajnom prostredí, kde môže dochádzať k úpravám dôkazov alebo dokumentov, môže fuzzy hashing zohrávať kľúčovú úlohu pri identifikácii a analýze týchto zmien.

Na rozdiel od tradičného hashovania, kde aj minimálna zmena vstupných dát vedie k úplne odlišnému hashovému výstupu (vlastnosť nazývaná *lavínový efekt*), fuzzy hashing zachytáva podobnosti medzi súbormi. Využíva algoritmy ako **ssdeep** alebo **sdhash**, ktoré rozdeľujú súbor na menšie bloky a generujú hashové hodnoty pre tieto bloky. Porovnaním týchto čiastkových hashov je možné určiť mieru podobnosti medzi dvoma súbormi.

Integrácia fuzzy hashovania s blockchainovou technológiou v policajnom prostredí

V kontexte blockchainu môže byť fuzzy hashing integrovaný na zlepšenie správy dôkazov a **zabezpečenie integrity dát**. Hashe vytvorené pomocou fuzzy hashovania môžu byť uložené na blockchaine, čím sa vytvorí nezmeniteľný záznam o stave súborov v konkrétnom čase. V prípade pokusu o manipuláciu s dôkazmi fuzzy hashing umožní identifikovať tieto zmeny porovnaním nových hashov s pôvodnými uloženými na blockchaine. Kombinácia blockchainu s fuzzy hashovaním tiež umožňuje **sledovať históriu zmien súborov alebo dokumentov**, pričom každá verzia súboru môže mať svoj fuzzy hash uložený na blockchaine. To poskytuje transparentný a nezmeniteľný záznam o tom, kedy a aké úpravy boli vykonané. Navyše, ukladanie fuzzy hashov na blockchain umožňuje rôznym policajným zložkám a bezpečnostným agentúram **zdieľať informácie** o dôkazoch bez potreby zdieľania samotných citlivých dát. Tým sa zabezpečí, že všetci účastníci majú prístup k overeným informáciám a môžu efektívne spolupracovať.

Praktické využitie v policajnej praxi

Fuzzy hashing sa v policajnej praxi využíva najmä pri **forenznej analýze digitálnych dôkazov**, kde pomáha identifikovať súbory alebo dokumenty, ktoré boli mierne upravené alebo poškodené. Napríklad, ak páchateľ zmení nepatrné detaily v súbore s cieľom vyhnúť sa detekcii, fuzzy hashing dokáže odhaliť vysokú mieru podobnosti s pôvodným súborom. Okrem toho sa fuzzy hashing používa na **detekciu nelegálneho obsahu**, ako je detská pornografia alebo materiály podnecujúce k terorizmu, umožňujúc identifikáciu aj mierne zmenených verzií týchto materiálov. Prispieva aj k **ochrane pred únikom citlivých dokumentov** tým, že umožňuje organizáciám monitorovať internet a darknet na prítomnosť citlivých dokumentov

[16] NOVRIANSYAH, N. *Fuzzy Hashing*. medium.com. [online]. 2024. [cit. 25. júla 2024]. Dostupné na internete: https://medium.com/cybersecurity-101/understanding-fuzzy-hashing-c299f87ae43c.

a identifikovať aj čiastočne upravené alebo úryvky dokumentov, čím umožňuje rýchlejšie reagovať na únik informácií.

Výhody fuzzy hashovania spočívajú vo zvýšenej efektivite vyšetrovania, keďže umožňuje automatizované porovnávanie veľkého množstva súborov a rýchlu identifikáciu relevantných dôkazov. Pomáha odhaliť pokusy o manipuláciu s dôkazmi alebo zámerné úpravy súborov, čím zvyšuje schopnosť detekcie manipulácie. Navyše uľahčuje zdieľanie informácií medzi rôznymi policajnými zložkami bez odhalenia citlivých dát, čo podporuje spoluprácu a koordináciu.

Obmedzenia a výzvy fuzzy hashovania zahŕňajú nedostatočnú presnosť pri rozlišovaní veľmi jemných zmien, čo môže viesť k falošne pozitívnym alebo falošne negatívnym výsledkom; preto je nevyhnutné kombinovať túto techniku s ďalšími analytickými metódami. Ďalšou výzvou je výpočtová náročnosť porovnávania fuzzy hashov pri veľkých objemoch dát, čo si vyžaduje dostatočný výpočtový výkon a optimalizované algoritmy. Okrem toho neexistencia jednotných štandardov môže komplikovať interoperabilitu medzi rôznymi systémami a organizáciami, čo sťažuje širšie nasadenie tejto technológie.

Možnosti riešenia výziev zahŕňajú kombináciu fuzzy hashovania s inými technológiami, ako sú blockchain, Zero-Knowledge dôkazy a homomorfné šifrovanie, čo poskytuje komplexné riešenia pre bezpečnú správu a analýzu dát. Podpora štandardizácie algoritmov a formátov pre fuzzy hashovanie uľahčí spoluprácu medzi organizáciami a zlepší interoperabilitu systémov. Investovanie do odborného vzdelávania a školení personálu zabezpečí správnu implementáciu a efektívne využitie tejto technológie.

Fuzzy hashing v kombinácii s blockchainovou technológiou predstavuje silný nástroj na zlepšenie správy dôkazov a integrity dát v policajnom prostredí. Umožňuje nielen identifikovať a sledovať zmeny v súboroch, ale aj zabezpečiť, že tieto informácie sú uložené nezmeniteľne a transparentne. To zvyšuje dôveru v dôkazy predkladané súdom a podporuje efektívnu spoluprácu medzi rôznymi policajnými zložkami a medzinárodnými agentúrami.

Platformy

Pre policajné aplikácie, kde je nevyhnutná vyššia úroveň kontroly nad prístupom a správou dát, sú dôležité aspekty ako súkromie, bezpečnosť, škálovateľnosť a interoperabilita. Vhodné blockchainové platformy by mali poskytnúť robustné riešenia na zabezpečenie týchto kľúčových požiadaviek.

Rôzne typy blockchainových sietí - verejné, súkromné a konsorciálne - majú jedinečné charakteristiky, ktoré ovplyvňujú ich vhodnosť pre rôzne aplikácie v policajnom prostredí. Verejné blockchainy, ako sú Bitcoin alebo Ethereum, poskytujú vysoký stupeň decentralizácie a transparentnosti, čo je užitočné pre aplikácie vyžadujúce bezpečnú a auditovateľnú výmenu informácií medzi viacerými stranami. Z dôvodu potreby ochrany citlivých policajných údajov však súkromné blockchainy môžu byť preferovanejšie, pretože umožňujú kontrolovaný prístup a rýchlejšie spracovanie transakcií. Konsorciálne blockchainy, ktoré spravuje skupina dôveryhodných entít, môžu poskytovať vyvážené riešenie medzi centralizovanou kontrolou a potrebou spolupráce medzi viacerými agentúrami.

Nasledovné platformy ponúkajú rôzne vlastnosti a funkcie, ktoré vyhovujú špecifickým požiadavkám policajných aplikácií, vrátane potreby vyššej úrovne kontroly nad prístupom a správou dát, ako aj schopnosti efektívne a bezpečne spracovávať citlivé informácie. Pri výbere konkrétnej platformy by mala byť zvážená špecifická situácia a požiadavky jednotlivých policajných organizácií.

Hyperledger Fabric[17] je open-source blockchainová platforma určená na podnikové použitie, ktorá sa vyznačuje vysokou úrovňou modularizácie a prispôsobiteľnosti. Táto platforma umožňuje organizáciám navrhnúť a implementovať blockchainové systémy, ktoré presne vyhovujú ich potrebám, vrátane podpory rôznych typov inteligentných zmlúv známych ako „chaincode“, ktoré sa vykonávajú v izolovaných prostrediach na zvýšenie bezpečnosti. Hyperledger Fabric je obzvlášť užitočný pre policajné aplikácie vďaka svojej schopnosti konfigurovať privátne kanály, prostredníctvom ktorých účastníci môžu bezpečne zdieľať informácie v rámci uzavretej skupiny a používať pokročilé kontroly prístupu k citlivým údajom. Táto platforma je navrhnutá tak, aby zvládla vysoké objemy transakcií pri zachovaní vysokého výkonu, čo je kľúčové pre rýchle spracovanie policajných údajov. Okrem toho Hyperledger Fabric podporuje integráciu s existujúcimi systémami, čo zjednodušuje implementáciu v organizáciách s komplexnými IT infraštruktúrami.

Ponúka efektívnejšiu a ekologickejšiu alternatívu k metódam, ktoré sú energeticky náročné, ako je napríklad Proof of Work, vďaka čomu je ideálna pre podnikové prostredie, v ktorom sú energetické nároky a udržateľnosť dôležitými faktormi. Hyperledger Fabric je navyše podporovaná rozsiahlou komunitou vývojárov a spoločností, čo zabezpečuje jej neustály vývoj a zdokonaľovanie, čo je zárukou dlhodobej udržateľnosti a spoľahlivosti pre použitie v policajných operáciách.

Corda[18] je blockchainová platforma navrhnutá špeciálne na podnikové použitie, najmä vo finančných službách, ale jej vlastnosti sú vhodné aj pre policajné a súdne aplikácie, kde je potrebná vysoká miera dôvernosti a zabezpečenia. Corda poskytuje „point-to-point“ súkromie, vďaka čomu transakcie medzi dvoma stranami nie sú viditeľné pre ostatných účastníkov siete. Toto je zásadné pre zachovanie dôvernosti citlivých policajných informácií, ako sú osobné údaje občanov alebo detaily o vyšetrovaniach. Corda umožňuje aj presné riadenie toho, kto môže vidieť aké informácie, čím sa zabezpečuje, že údaje sú prístupné len oprávneným osobám. Vďaka svojej schopnosti spravovať komplexné pracovné toky a automatizovať procesy s pomocou inteligentných zmlúv Corda zaisťuje efektivitu a presnosť vo vykonávaní policajných operácií. Okrem toho platforma podporuje vysoký výkon a škálovateľnosť pri spracovaní transakcií, čo je kľúčové pre rýchle spracovanie veľkého objemu policajných údajov.

MultiChain[19] je platforma založená na Bitcoine, ktorá umožňuje rýchle a efektívne nasadenie privátnych blockchainov s rôznymi úrovňami prístupových práv. Je navrhnutá tak, aby poskytovala jednoduché riešenia pre vytváranie a správu privátnych blockchainov, ktoré sú ideálne na policajné použitie, kde je potrebná kontrola prístupu a zabezpečenie citlivých dát. MultiChain ponúka funkcie ako riadenie prístupu, rýchle transakcie a jednoduchú integráciu s existujúcimi systémami. Táto platforma umožňuje policajným organizáciám prispôsobiť sieť podľa špecifických požiadaviek vrátane definovania vlastných pravidiel a transakčných protokolov. MultiChain je známa aj svojou schopnosťou zvládať vysoké objemy transakcií bez kompromisov na výkone, čo je zásadné pre operácie, pri ktorých sa vyžaduje rýchle spracovanie dát.

[17] HYPERLEDGER. *Hyperledger Fabric*. www.hyperledger.org. [online]. 2024. [cit. 25. júla 2024]. Dostupné na internete: https://www.hyperledger.org/projects/fabric.
[18] CORDA. 2024. *Corda*. corda.net. [online]. 2024. [cit. 25. júla 2024]. Dostupné na internete: https://corda.net/.
[19] MULTICHAIN. *MultiChain*. multichain.com. [online]. 2024. [cit. 25. júla 2024]. Dostupné na internete: https://www.multichain.com/.

Quorum[20] je privátna blockchainová platforma, ktorá je variantom Ethereum, navrhnutá na poskytovanie riešení pre podniky, ktoré vyžadujú vysoký stupeň súkromia a bezpečnosti transakcií. Quorum je optimalizovaná pre použitie v podnikovom prostredí s dôrazom na vysoký výkon a súkromie transakcií, čo je ideálne pre citlivé policajné operácie. Platforma podporuje transakcie súkromného charakteru, čo znamená, že citlivé informácie môžu byť spracované a uchovávané bez toho, aby boli prístupné nepovolaným stranám. Quorum takisto poskytuje vysokú škálovateľnosť a nízke náklady na transakcie, čo zaisťuje efektívne spracovanie veľkého objemu policajných údajov. Okrem toho vďaka podpore pre inteligentné zmluvy a pokročilé kryptografické protokoly, Quorum zabezpečuje, že všetky policajné operácie sú vykonávané transparentne a bezpečne.

Príklady nasadenia z praxe

Nasledovné riešenia ukazujú, ako blockchain technológia môže významne zvýšiť transparentnosť, integritu a bezpečnosť procesov v rámci policajných zložiek.

Delhi Polícia v Indii[21]

Delhi Polícia spolupracuje s Delhi Forensic Science Laboratory (DFSL)[22] na využití blockchainovej technológie na zaznamenávanie a sledovanie reťazca zachovania dôkazov.

Táto iniciatíva umožní vytvárať nemenné a transparentné záznamy každého kroku v manipulácii s dôkazmi, čím sa DFSL stáva prvou takouto inštitúciou v Indii. Blockchainová technológia, známa svojou bezpečnosťou a neschopnosťou úprav, zaznamenáva informácie v reťazci blokov, pričom každý blok obsahuje šifrované údaje, ako sú forenzné záznamy a prípadové logy. Tento systém je teraz integrovaný do Inter-Operable Criminal Justice System (ICJS) v Dillí, čo zjednodušuje prenos dát medzi políciou, forenznými laboratóriami, súdnymi a trestnými inštitúciami. Každý prenos dôkazu medzi rôznymi osobami je dokumentovaný ako nový blok v blockchaine, čím sa zaručuje podrobná sledovateľnosť a ochrana súkromia počas celého vyšetrovacieho procesu.

Polícia v Firozabade, Uttar Pradesh, India

Policajný zbor vo Firozabade[23], v najľudnatejšom štáte Uttar Pradesh, spustil iniciatívu založenú na blockchainovej technológii, ktorá má sledovať verejné sťažnosti. Tento systém vyvinutý s využitím blockchain protokolu Polygon umožňuje občanom podávať sťažnosti na policajných dôstojníkov bez obáv, že by ich sťažnosti boli zamietnuté alebo zmanipulované. Platforma s názvom „police complaint on blockchain“ je dostupná vo viacerých jazykoch a poskytuje možnosť sledovať status sťažnosti, identifikovať prideleného dôstojníka a prijímať upozornenia na pokrok vo vyšetrovaní. Sťažnosti podané cez tento portál sú chránené pred zásahmi vďaka nemeniteľnosti blockchainu, čo znamená, že raz zaznamenané údaje nemožno zmazať ani upraviť. Iniciatíva je považovaná za potenciálne revolučnú v zabezpečení

[20] NELSON, M. *Consensys Quorum*. consensys.io. [online]. 2021. [cit. 25. júla 2024]. Dostupné na internete: https://consensys.io/blog/what-is-consensys-quorum.

[21] TIMES, H. *Delhi Police adopts blockchain*. [online]. 2023. [cit. 25. júla 2024]. Dostupné na internete: https://www.hindustantimes.com/cities/delhi-news/delhi-forensic-science-laboratory-implements-blockchain-technology-for-transparent-evidence-record-101692294375620.html.

[22] FORENSICSDIGEST. *The Delhi Police Initiative*. forensicsdigest.com. [online]. 2024. [cit. 25. júla 2024]. Dostupné na internete: https://forensicsdigest.com/delhi-police-embraces-blockchain-technology-for-evidence-custody/.

[23] BHARDWAJ, S. *Polygon joins hands with Firozabad police to use blockchain technology in battling crime*. www.forbesindia.com. [online]. 2022. [cit. 25. júla 2024]. Dostupné na internete: https://www.forbesindia.com/article/cryptocurrency/polygon-joins-hands-with-firozabad-police-to-use-blockchain-technology-in-battling-crime/80533/1.

spravodlivosti, keďže umožňuje transparentné a spravodlivé zaobchádzanie so sťažnosťami občanov.

Dubai Polícia, Spojené Arabské Emiráty

Dubajská polícia[24] sa spojila s platformou Cardano Blockchain, aby zlepšila bezpečnosť a integritu zdieľania údajov v trestných vyšetrovaniach, konkrétne pri zdieľaní snímok po celom svete, vrátane Interpolu. Táto iniciatíva je súčasťou širšieho úsilia Dubaja stať sa popredným centrom pre krypto technológie, čo je v súlade s úsilím Spojených arabských emirátov o začlenenie pokročilých technológií, ako je blockchain, do rôznych sektorov. Využitím blockchainu Cardano si dubajská polícia kladie za cieľ využiť nezmeniteľné a transparentné vlastnosti tejto technológie, aby zabezpečila, že raz zaznamenané dôkazy nemôžu byť pozmenené ani sfalšované, čím sa zachová autenticita dôkazov. Projekt bol oznámený na Svetovom policajnom summite v marci 2024 v Dubaji, čo odráža záväzok mesta prijať inovatívne riešenia na zlepšenie administratívnych a policajných činností. Tento krok dubajskej polície sa považuje za významný pokrok vo využívaní blockchain technológie v policajnej praxi a môže slúžiť ako príklad pre iné jurisdikcie po celom svete.

Výsledky skúmania

Článok o využití blockchainovej technológie v policajnom prostredí sa zameriava na zodpovedanie troch kľúčových otázok. Prvá otázka sa týka toho, ako môže blockchain prispieť k zvýšeniu bezpečnosti a transparentnosti v policajných operáciách.

Ukazuje sa, že unikátne vlastnosti blockchainu, ako sú nezmeniteľnosť a distribuované záznamy, poskytujú významnú ochranu pri spracovaní citlivých policajných údajov, zvyšujúc tak dôveru v autenticitu policajných záznamov a dôkazov.

Druhá otázka skúma, akým spôsobom môže blockchain zabezpečiť integritu dát a efektívnu správu dôkazov v policajnom prostredí. Zistil som, že implementácia blockchainu umožňuje nezmeniteľné zaznamenávanie všetkých policajných transakcií a dát. Tento prístup zaručuje ich dostupnosť výlučne pre oprávnené osoby a chráni ich pred neoprávneným zásahom, čím zvyšuje bezpečnosť a súkromie v policajných procesoch.

Tretia otázka sa zaoberá tým, ako môže blockchain zlepšiť interoperabilitu medzi rôznymi policajnými zložkami. Výsledky ukazujú, že implementácia blockchainu umožňuje nezmeniteľné zaznamenávanie všetkých policajných transakcií a dát. Výsledky naznačujú, že blockchain môže slúžiť ako most na prepojenie rôznych policajných zložiek, čím zvyšuje efektivitu a spoluprácu. Technológie, ako sú Zero-Knowledge dôkazy a škálovateľné riešenia, umožňujú bezpečnú a plynulú výmenu informácií medzi rôznymi platformami, čo podporuje lepšiu koordináciu a reakciu na národnej aj medzinárodnej úrovni.

Záver

Blockchainová technológia, ktorá sa pôvodne uplatnila najmä v oblasti kryptomien, postupne nachádza svoje miesto aj v policajnom prostredí, kde prináša významné zlepšenia v oblastiach ako bezpečnosť, transparentnosť a efektivita. Vďaka svojej nezmeniteľnosti a distribuovanému charakteru poskytuje blockchain policajným zložkám možnosť viesť nezmeniteľné a auditovateľné záznamy, a tým chráni citlivé údaje pred manipuláciou a zároveň umožňuje efektívnejšiu medziagentúrnu spoluprácu.

S príchodom nových technológií, napríklad kvantových počítačov, a vďaka pokroku v kryptografii sa otvárajú nové možnosti aj potenciálne výzvy pre bezpečnosť blockchainov. Kvantové počítače by mohli teoreticky ohroziť súčasné kryptografické algoritmy, ale zároveň

[24] SHARMA, S. *Dubai Police Will Use Cardano to Share Bullet Scans in Blockchain Policing Project*. www.ccn.com. [online]. 2024. [cit. 25. júla 2024]. Dostupné na internete: https://www.ccn.com/news/crypto/dubai-police-cardano-blockchain-crypto/.

ponúkajú možnosti pre kvantovú kryptografiu, ktorá by mohla zabezpečiť ešte vyššiu odolnosť voči kybernetickým útokom.

Napriek súčasným úspechom a obrovskému potenciálu blockchainu v policajnom sektore je dôležité riešiť pretrvávajúce výzvy, ako sú interoperabilita, škálovateľnosť a ochrana súkromia. Tieto oblasti si vyžadujú ďalší vývoj a štandardizáciu, aby bolo možné blockchain plne využiť na zlepšenie policajných operácií.

V posledných rokoch narastá záujem o kvantové počítače a ich potenciálny vplyv na bezpečnosť kryptografických systémov vrátane tých, ktoré sú základom pre blockchain technológie. Kvantové počítače by teoreticky mohli prelomiť mnohé súčasne používané kryptografické algoritmy, čo by mohlo ohroziť bezpečnosť blockchainov. Napriek tomu vývoj kvantovo odolných kryptografických algoritmov, známych aj ako post-kvantová kryptografia, ponúka riešenia na zmiernenie týchto hrozieb. Tieto algoritmy sú navrhnuté tak, aby odolali útokom kvantových počítačov, čím zabezpečia, že kryptografické ochrany zostanú pevné aj v ére kvantového výpočtového veku.

Zahrnutie kvantovo odolných technológií do blockchainových platform môže zabezpečiť, že tieto systémy zostanú bezpečné a spoľahlivé aj v budúcnosti. Implementácia týchto technológií by mala byť prioritou pre vývojárov a technológie vedúcich organizácií, ktoré si prajú udržať náskok v oblasti bezpečnosti a odolnosti voči rýchlo sa vyvíjajúcim technologickým hrozbám.

Policajné zložky sú na prahu veľkých zmien v spôsobe, akým policajné zložky pracujú a chránia dáta. Perspektíva, že by policajné systémy mohli využívať najnovšie technológie, už nie je len vzdialenou možnosťou, ale rýchlo sa stáva realitou. Tento vývoj by mohol viesť k vytvoreniu spoľahlivejších, efektívnejších a transparentnejších policajných systémov, čo by zvýšilo dôveru verejnosti a poskytlo lepšiu ochranu pre všetkých.

Keďže sa diskutuje o potenciálnom využití blockchainovej technológie v policajnom prostredí, je dôležité realisticky zhodnotiť nielen možnosti, ale aj prekážky, ktoré by mohli ovplyvniť jej efektívne nasadenie. Jednou z hlavných výziev je škálovateľnosť blockchainových systémov, ktorá môže byť obmedzená vzhľadom na veľký objem dát, ktoré policajné zložky spracovávajú. Rýchlosť transakcií je ďalším kritickým faktorom, pretože vysoké oneskorenie môže byť prekážkou v naliehavých policajných operáciách. Integrácia blockchainu so súčasnými IT systémami a databázami policajných zložiek okrem toho vyžaduje komplexné technické a organizačné zmeny, ktoré môžu byť časovo a finančne náročné. Preto je nevyhnutné, aby sa tieto výzvy starostlivo preverili a riešili v procese plánovania a implementácie, aby bolo možné plne využiť výhody, ktoré blockchain ponúka.

Literatúra

ANON. *Layer 2*. ethereum.org. [online]. 2024. [cit. 23. júla 2024]. Dostupné na internete: https://ethereum.org/en/layer-2/.

ANON. *Layer 1 vs. Layer 2*. academy.binance.com. [online]. 2022. [cit. 23. júla 2024]. Dostupné na internete: https://academy.binance.com/en/articles/blockchain-layer-1-vs-layer-2-scaling-solutions.

BAGATARHAN, Goknil. *Liquid Proof Of Stake*. metatime.com. [online]. 2024. [cit. 25. júla 2024]. Dostupné na internete: https://metatime.com/en/blog/what-is-liquid-proof-of-stake-lpos-how-does-it-work.

BHARDWAJ, Shashank. *Polygon joins hands with Firozabad police to use blockchain technology in battling crime*. www.forbesindia.com. [online]. 2022. [cit. 25. júla 2024]. Dostupné na internete: https://www.forbesindia.com/article/cryptocurrency/polygon-joins-hands-with-firozabad-police-to-use-blockchain-technology-in-battling-crime/80533/1.

CORDA. *Corda*. corda.net. [online]. 2024. [cit. 25. júla 2024]. Dostupné na internete: https://corda.net/.

COSMOS. *Build on the Interchain*. [online]. 2024. [cit. 24. júla 2024]. Dostupné na internete: https://cosmos.network/.

FORENSICSDIGEST. *The Delhi Police Initiative*. forensicsdigest.com. [online]. 2024. [cit. 25. júla 2024]. Dostupné na internete: https://forensicsdigest.com/delhi-police-embraces-blockchain-technology-for-evidence-custody/.

GAURAV, Roy. *Delegated Proof-of-Stake*. www.ledger.com. [online]. 2023. [cit. 25. júla 2024]. Dostupné na internete: https://www.ledger.com/academy/what-is-delegated-proof-of-stake-dpos.

HYPERLEDGER. *Hyperledger Fabric*. www.hyperledger.org. [online]. 2024. [cit. 25. júla 2024]. Dostupné na internete: https://www.hyperledger.org/projects/fabric.

LEDGER. *Blockchain Rollups*. www.ledger.com. [online]. 2023. [cit. 24. júla 2024]. Dostupné na internete: https://www.ledger.com/academy/what-are-blockchain-rollups.

LIU, Bessie. *Homomorphic encryption*. blockworks.co. [online]. 2024. [cit. 24. júla 2024]. Dostupné na internete: https://blockworks.co/news/what-is-fully-homomorphic-encryption.

MEARIAN, Lucas. *Sharding*. computerworld.com. [online]. 2019. [cit. 22. júla 2024]. Dostupné na internete: https://www.computerworld.com/article/1716485/sharding-what-it-is-and-why-so-many-blockchain-protocols-rely-on-it.html.

MULTICHAIN. *MultiChain*. multichain.com. [online]. 2024. [cit. 25. júla 2024]. Dostupné na internete: https://www.multichain.com/.

NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. bitcoin.org. [online]. 2008. [cit. 22. júla 2024]. Dostupné na internete: https://bitcoin.org/en/bitcoin-paper.

NAPOLETANO, Erika a CURRY, Benjamin. *Proof-of-Stake*. www.forbes.com. [online]. 2023. [cit. 25. júla 2024]. Dostupné na internete: https://www.forbes.com/advisor/investing/cryptocurrency/proof-of-stake/.

NELSON, Matt. *Consensys Quorum*. consensys.io. [online]. 2021. [cit. 25. júla 2024]. Dostupné na internete: https://consensys.io/blog/what-is-consensys-quorum.

NETWORK, Lightning. *Lightning Network*. lightning.network. [online]. 2024. [cit. 23. júla 2024]. Dostupné na internete: https://lightning.network/.

NOVRIANSYAH, Nova. *Fuzzy Hashing*. medium.com. [online]. 2024. [cit. 25. júla 2024]. Dostupné na internete: https://medium.com/cybersecurity-101/understanding-fuzzy-hashing-c299f87ae43c.

PETTINARI, Pablo. *Formal Verification*. ethereum.org. [online]. 2023. [cit. 25. júla 2024]. Dostupné na internete: https://ethereum.org/en/developers/docs/smart-contracts/formal-verification/#drawbacks-of-formal-verification.

POLKADOT. *Polkadot's technology*. polkadot.network. [online]. 2024. [cit. 24. júla 2024]. Dostupné na internete: https://polkadot.network/.

ROSIC, Ameer. *Zero Knowledge Proofs*. blockgeeks.com. [online]. 2023. [cit. 22. júla 2024]. Dostupné na internete: https://blockgeeks.com/guides/zero-knowledge-proofs/.

SHARMA, Shraddha. *Dubai Police Will Use Cardano to Share Bullet Scans in Blockchain Policing Project*. www.ccn.com. [online]. 2024. [cit. 25. júla 2024]. Dostupné na internete: https://www.ccn.com/news/crypto/dubai-police-cardano-blockchain-crypto/.

STEVENS, Robert. *What Are Blockchain Bridges*. www.coindesk.com. [online]. 2022. [cit. 24. júla 2024]. Dostupné na internete: https://www.coindesk.com/learn/what-are-blockchain-bridges-and-how-do-they-work/.

TIMES, Hindustan. *Delhi Police adopts blockchain*. [online]. 2023. [cit. 25. júla 2024]. Dostupné na internete: https://www.hindustantimes.com/cities/delhi-news/delhi-forensic-science-laboratory-implements-blockchain-technology-for-transparent-evidence-record-101692294375620.html.

Keywords: interoperability, scalability, Zero-Knowledge proofs, smart contracts, Layer 2 solutions, blockchain bridges, formal verification

Summary

This scientific article explores the transformative potential of blockchain technology in police operations, focusing on enhancing security, transparency, and efficiency. Initially recognized for its role in cryptocurrencies, blockchain's inherent immutability and distributed ledger features are now being utilized to revolutionize data management within law enforcement. The technology ensures secure, auditable, and tamper-resistant recording of all transactions and data related to police operations, from investigation records to evidence management, ensuring access only to authorized personnel.

The key areas examined include the enhancement of security and transparency via blockchain's immutable and distributed records, ensuring data integrity and evidence management by providing an unalterable record of all transactions and data, and improving interoperability between various police departments and agencies. The integration of advanced technologies such as Zero-Knowledge Proofs and Layer 2 solutions further strengthens privacy protection and operational speed, contributing to a more efficient and reliable police information system.

Practical implementations in police forces worldwide, such as the Delhi Police's blockchain initiative for evidence tracking and Dubai Police's collaboration with Cardano Blockchain for secure data sharing, demonstrate significant improvements in the transparency, integrity, and security of processes. The presented article concludes by addressing the ongoing challenges of scalability, interoperability, and privacy protection, emphasizing the need for further development and standardization to fully realize blockchain's benefits in modernizing police operations.

By evaluating these aspects, the article highlights blockchain's critical role in the digital transformation of law enforcement, promoting greater public trust and co-operation between police forces, both nationally and internationally.

Ing. Milan Feltovic
Žilinská univerzita
Fakulta bezpečnostného inžinierstva
e-mail: milan@feltovic.com

Recenzent: Mgr. Marek Matulík