

Elektrotechnická asociace spouští první průmyslový blockchain v České republice

Digitalizace reálně prostupuje výrobou, službami i našimi životy. Nejcenějšími statky v průmyslu již nejsou suroviny ani stroje, ale data, know-how, algoritmy a digitální modely. S nimi přichází i blockchain jako technologie počínající éry digitálního vlastnictví. Víze této éry vedla Elektrotechnickou asociaci České republiky (EIA) ke spuštění projektu EIA blockchain.

EIA blockchain je určen pro zájemce z oblasti firem v průmyslu a ve službách. Jde pravděpodobně o první blockchain vyvinutý a spuštěný na území České republiky, avšak svým účelem, jako důvěryhodná platforma pro průmyslové podniky, které na něm mohou vytvářet své vlastní aplikace, je unikátní i celosvětově.

EIA blockchain byl vyvinut a spuštěn ve spolupráci s firmou IBM CZ, Fakultou elektrotechnickou ČVUT v Praze a za přispění členů Elektrotechnické asociace České republiky.

Co je blockchain

Blockchain je často charakterizován jako databáze pro registraci digitálního vlastnictví. Je to však databáze, která se od klasických databází podstatně liší. Charakterizují ji tři vlastnosti:

- decentralizace,
- sekvenční ukládání,
- neprůhlednost (opacita).

Blockchain je decentralizovaný tím, že existuje v mnoha identických kopiích na počítačích nazývaných blockchainové nody, které spolu komunikují v blockchainové síti.

Obsah blockchainu nelze zpětně měnit, je k němu možné pouze přidat další data, tzv. bloky. Plní se tedy pouze sekvenčním ukládáním a uchovává nezměnitelnou historii.

Nejpodstatnější odlišnost od běžné databáze spočívá v tom, co je v blockchainu jako v databázi uloženo. Nejsou to čitelná data, pouze jejich otisky – hashe datových souborů. Obsah blockchainu je tedy neprůhledný. K jeho neprůhlednosti přispívá i šifrování a několikanásobné zabezpečení.

Na technologii blockchainu je postavena kryptoměna bitcoin, která je dnes asi nejznámějším příkladem digitálního vlastnictví a prokazuje spolehlivost blockchainu jako prostředku jeho úschovy. Za deset let existence bitcoinu nedošlo k prolomení blockchainu, na kterém je založen. Přitom jde o síť anonymní a veřejnou a k jejímu napadení existuje silná motivace. Jestliže byly bitcoiny odcizeny, bylo to vždy neopatrností uživatele, který dostatečně nezabezpečil přístup ke své aplikaci. Blockchain však nejsou jen bitcoiny.

Co je EIA blockchain

EIA blockchain nemá s bitcoinem nic společného. Jeho síť nodů je sice veřejná a otevřená, ale neanonymní. Svůj node si do sítě nemůže připojit každý, ale pouze důvěryhodná právnická osoba, jejíž kredibilitu garantuje Elektrotechnická asociace. Oproti bitcoinu s těžebními farmami a jejich obrovskými náklady umožňuje tento koncept jednoduchou a levnou realizaci transakcí při zachování identické bezpečnosti. Tím otvírá možnost využití blockchainu v běžném životě firmy. Provoz na síti, její ochranu a stabilitu technicky zajišťuje firma, kterou EIA pro tento účel založila a již plně vlastní: EIA Blockchain Services, a. s. Jejím úkolem je technická údržba sítě a péče o to, aby síť zůstala transparentní a heterogenní. Není tedy žádným centrálním správcem sítě, takového správce blockchain z principu nemá. Jednou spuštěný blockchain žije vlastním životem a např. i upgrade softwaru je pouze zvláštním typem transakce, kterou musí všechny nody odsouhlasit. Technicky je EIA blockchain založen na průmyslové verzi blockchainu Hyperledger a využívá jeho open source verze vyvinuté a podporované firmou IBM.

Digitální vlastnictví se zde, jako v každé realizaci blockchainu, prokazuje uloženým hashem. Co bude předmětem tohoto vlastnictví, záleží na aplikaci, která je nad blockchainem postavena. Když se rozhodnete ke zřízení nodu EIA blockchain, dostanete již v instalačním balíčku základní aplikaci Blockchain Notarius[®]. Ta je určena k prokázání vlastnictví obsahu datového souboru. A protože datový soubor může být odkazem na jakékoliv další vlastnictví (obsahuje např. smlouvu), má Blockchain Notarius neuvěřitelně široké možnosti využití.

Proč zřídíme EIA blockchain

Blockchain je budoucností průmyslu, obchodu a bankovníctví. Umožňuje levně a spolehlivě ověřovat pravost souborů, např. certifikátů nebo diplomů. Umožňuje uzavírat nezpochybnitelné smlouvy, sledovat pohyb zboží, odhalovat padělků. Obrovské využití se očekává v průmyslu, při komunikaci mezi stroji, je to jedna z technologií pro prů-

mysl 4.0. Chceme umožnit členům EIA i dalším firmám v průmyslu i ve službách, aby byli na startu této technologie a měli možnost od začátku ji využívat a stavět na ní svá řešení. Proto kolem EIA blockchainu zřídíme i webovou platformu, kterou bude možné použít k vývoji a provozu blockchainových obchodních i technických projektů. Chceme umožnit firmám blockchain nejen používat, ale také na něm vydělávat.

Co je originálního na EIA blockchain

V první řadě je to způsob, kterým síť budujeme. Většinu profesionálních blockchainových projektů v zahraničí iniciují a financují velké korporace (např. MAERSK), které svým partnerům jen nabízejí jeho využití. Podobně staví blockchainy banky nebo fintech firmy.

EIA blockchain nemá takového centrálního zřizovatele. Jde o dobrovolné sdružení majitelů nodů, kterými jsou důvěryhodné subjekty – přednostně právnické osoby. Seznam nodů a jejich majitelů je veřejný a externí uživatel si, např. k ověření platnosti listiny, může vybrat toho, kterému důvěřuje. Tento koncept má své důvody. Chtěli jsme, aby se v oblasti digitálního vlastnictví stal EIA blockchain skutečně nezávislou, transparentní a bezpečnou autoritou.

Projekt EIA blockchainu vznikl na půdě Elektrotechnické asociace původně jako nástroj pro podporu obchodu. Členové asociace často realizují své projekty v zemích, kde je obtížné shodnout se na autoritě potřebné k potvrzení smlouvy, certifikátu, technické zprávy nebo předávacího protokolu. EIA blockchain má předpoklady být za takovou autoritu uznán kdekoli ve světě. Není centrální autoritou, kterou někdo ovládá, která může být korumpována, vydírána či jinak napadena. Autorita je zde „sdílena“ mnoha nezávislými důvěryhodnými subjekty a ani selhání části z nich nezpůsobí selhání jejího rozhodnutí. Předpokládáme, že průmyslové firmy u nás i v zahraničí tyto principy znají, a budou tedy akceptovat EIA blockchain jako důvěryhodnou autoritu potvrzující např. pravost uvedených dokumentů. Navíc motivujeme majitele nodů k tomu, aby nabídli svým obchodním partnerům v zahraničí podporu při zřízení vlastního nodu EIA blockchain. Podíl na sdílené autoritě zvýší její důvěryhodnost i pro zahraniční uživatele. Také EIA se snaží o maximální rozšíření EIA blockchainu prostřednictvím partnerských a jiných profesních asociací v zahraničí.

EIA blockchain se rovněž liší tím, že nevznikl pro jedno konkrétní využití, ale je otevřený pro jakýkoliv typ aplikace. Blockchain Notarius je jen základem, který má sloužit pro běžné použití ve firmě. EIA blockchain je však připraven nést mnoho dalších specializovaných aplikací, obchodních, technických,

ta na věky uloženy v mnoha kopiích na všech nodech. Tento proces se na EIA blockchainu nazývá registrace souboru. Je to tedy připojení bloku, který obsahuje hash souboru a jeho metadata, k blockchainu na všech nodech sítě, které pak mají identické kopie nového obsahu.

hou však vytvářet účty pro další klienty. Je věcí majitele nodu, za jakých podmínek přístup poskytne.

Na rozdíl od registrace je služba ověření v aplikaci Blockchain Notarius veřejná a bezplatná. Není třeba žádné jméno a heslo, stačí otevřít web kteréhokoliv nodu EIA blockchain a zjistit, zda byl soubor registrován. Seznam webových adres nodů je (resp. bude) na webu EIA Blockchain Services i na webu blockchainotarius.cz. Na kterémkoliv z nich může kdokoli soubor ověřit.

Pro ilustraci uvedme ještě dvě zajímavé možnosti, které Blockchain Notarius poskytuje.

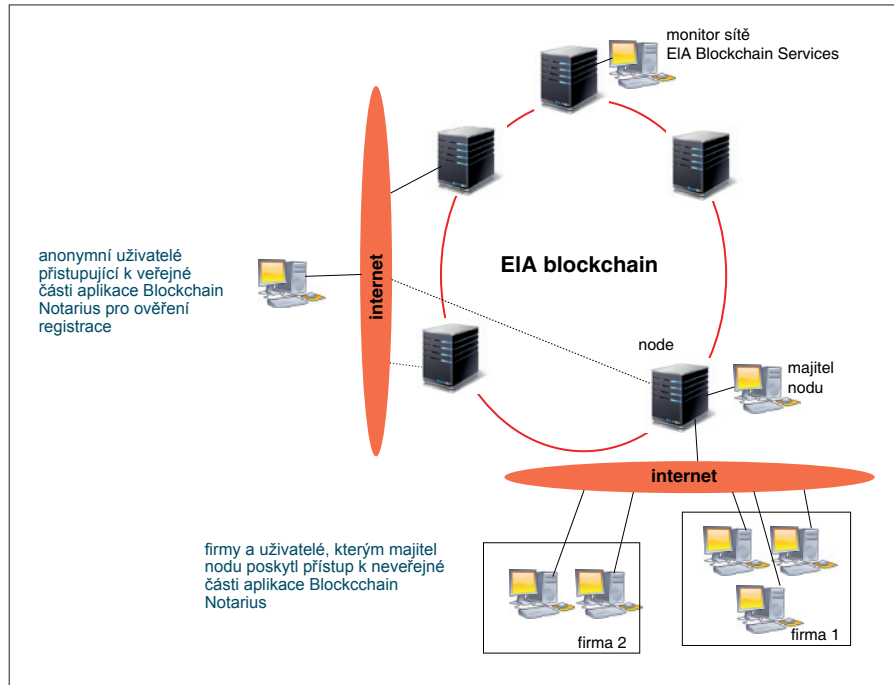
K registraci není nutné soubor do aplikace vkládat (ani v tom případě se soubor nikam neukládá ani neodesílá, aplikace z něj pouze vypočte hash). Blockchain Notarius však nabízí i možnost registrovat soubor jen ručním vložením hashe vypočteného jiným způsobem. Lze tedy registrovat soubor, jehož obsah kromě autora nikdo neviděl, a pomocí anonymního přihlášení je možné zakrýt i samotného autora. Tato možnost byla zamýšlena pro maximální utajení citlivých smluv a dokumentů, mohou ji však využít kreativci, designéři a jiní autoři k ochraně díla (textu, digitální fotografie, klipartu, zvukového souboru, filmového klipu) před udělením copyrightu.

Druhou zajímavou možností je schválení registrace dalším účastníkem. Tato varianta byla vytvořena pro uzavírání smluv na dálku, kontrasiagnaci dokumentů a podobné příležitosti. Spočívá v tom, že když se váš vzdálený partner přesvědčí ověřením souboru smlouvy, třeba i na jiném nodu na druhém konci světa, že obsah registrované smlouvy je totožný s tím, na kterém jste se dohodli, zaregistruje k souboru smlouvy své schválení. Navěky je pak v blockchainu smlouva zaregistrována s oběma souhlasly.

EIA blockchain je tu pro byznys

Již několikrát zde bylo zdůrazněno, že EIA blockchain je budován jako platforma pro aplikace, které na ní její členové mohou vybudovat. Založila ji Elektrotechnická asociace, je však otevřena všem, kteří budou zachovávat její základní myšlenku: otevřenost a důvěryhodnost. Firma EIA Blockchain Services provozuje webové stránky www.elachain.cz, kde se zájemci dozvědí, jak si pořídit node EIA blockchain, kdo nabízí služby a vývoj aplikací a jak sami mohou EIA blockchain využívat a rozvíjet.

Otto Havle, EIA Blockchain Services, a. s.



Obr. 1. Struktura sítě EIA blockchain

i těch dnes neznámých, které přinese budoucnost. Je technickou platformou, bezpečnou a transparentní pro váš byznys.

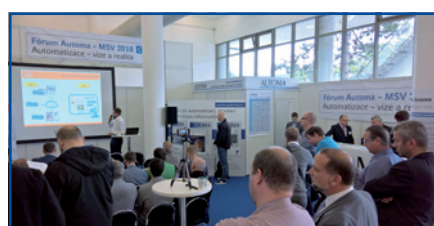
Blockchain Notarius, základní aplikace EIA blockchain

Na příkladu aplikace Blockchain Notarius lze názorně ukázat, co EIA blockchain nabízí.

Aplikace Blockchain Notarius umožňuje dvě základní operace: registraci souboru a ověření souboru. K vysvětlení, co při těchto operacích probíhá, se znovu vrátíme k principu blockchainu. Do EIA blockchainu se neukládají dokumenty, ale pouze jejich digitální otisky, tzv. hashe. Hash souboru spolu s metadaty (údaji pro snadnější orientaci nebo vyhledávání) tvoří blok, který je připraven k přidání do blockchainu. Po kontrolách oprávnění a bezpečnosti je blok rozeslán všem nodům, které jej přidají ke své kopii blockchainu a shodnost všech kopií blockchainu se znovu ověří. Tak budou hash souboru a jeho metadata

Ověření souboru spočívá v tom, že se uživatel přesvědčí, že byl soubor v blockchainu registrován. Jak, když je v blockchainu jen nic neříkající hash? Právě podle něj. Ten, kdo má soubor k dispozici, může znovu spočítat hash, prohledat blockchain a zjistit, zda obsahuje identický hash. Když jej obsahuje, je i ověřovaný soubor identický s tím, který byl registrován. Jestliže se však někdo pokusí ověřit soubor, ve kterém byl změněn jediný bit, identický hash v blockchainu nenajde a blockchain ohlásí, že ověřovaný dokument registrován nebyl.

Na obr. 1 je ukázána struktura sítě EIA blockchain s nody, na kterých je instalována aplikace Blockchain Notarius. Tu může majitel nodu (uživat sám, může k ní však umožnit přístup i uživatelům, kteří nemají vlastní node). Aplikace obsahuje administrátorskou část, ve které lze poskytnout účet, tedy uživatelské jméno a heslo, zákazníkům nebo partnerům. Ti pak mohou registrovat soubory úplně stejně jako majitel nodu, nemo-



Fórum automatizace – vize a realita

MSV 2019, Brno
7. až 11. 10. 2019, hala C

