BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2023
http://excel.fit.vutbr.cz

Decentralizovaná aplikace pro Question/Answer sekci využívající blockchain

Jakub Čuhanič*

Abstrakt

Tato práce se zaměřuje na vytvoření decentralizované mobilní aplikace, která nabízí Q&A sekci. Přínos aplikace je v její transparentnosti a vlastnostech vyplývajících z blockchainu. Hlavními z nich jsou zamezení cenzury a spamu za použití technologie blockchainu a smart kontraktů. Výsledná aplikace se může využít kdekoliv, kde potřebují Q&A prostor, především ve veřejnoprávních médiích nebo na internetu. Díky propojení se systémem pro správu identit by se mělo dosáhnout stavu, ve kterém nebudou moci být uživatelé a jejich otázky moderátory relací manipolováni ani cenzurováni.

*xcuhan00@fit.vut.cz, *Faculty of Information Technology, Brno University of Technology*

1. Úvod

Poprvé jsme nuceni si po 21 stoletích vybírat informace a kontrolovat, zda jsou pravdivé a objektivní. Není možné, že nám média ukazují jen část pravdy, tu část, kterou chtějí? Na internetu a v televizních a rozhlasových relacích jsou populární Q&A sekce. Jsme schopni zjistit, zda otázky, které jsou položeny skrze různé aplikace, byly nějak zmanipulovány nebo cenzurovány?

2. Cíl práce

Smyslem této práce je vytvořit koncept i implementaci decentralizované mobilní aplikace, ve které bude uživatel pokládat jednotlivé otázky a hlasovat. Aplikace poskytne přínos v tom, že díky použité technologii blockchainu nedovolí žádné straně cenzurovat otázky. Druhou, neméně cennou předností aplikace bude zamezení spamu v relacích za pomocí systému pro správu identit.

3. Existující řešení

Decentralizované řešení aplikace nabízející Q&A sekci se mi po vlastním průzkumu nepovedlo dohledat. Níže představím dvě aplikace, které mi byly svým vzhledem, nikoliv však centralizací, částečnou inspirací při tvorbě mé vlastní.

Slido

Jedná se o nejpopulárnější řešení pro interaktivní Q&A sekce využívající se především při přednáškách. Tato webová aplikace nabízí jednoduché zobrazení otázek přednášejícím i uživatelům s možností pokládat a hlasovat pro otázky. Nevýhodou řešení je možnost cenzury otázek a spamu. [1]

Mentimeter

Mentimeter je jedna z řady webových aplikací umožňující vytvoření Q&A sekce v prezentacích. Aplikace poskytuje základní možnosti zobrazení, pokládání otázek a hlasování, nicméně nevýhody jsou stejné jako u předchozího příkladu. [2]

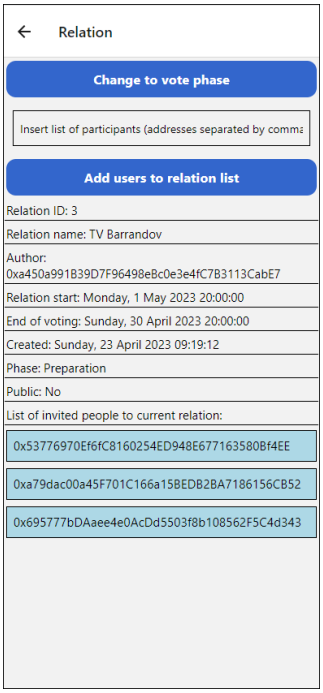
4. Použité technologie a jejich význam

Při vývoji smart kontraktu jsem se rozhodl použít jazyk Solidity. Pro testování funkčnosti aplikace byla použita testovací síť Etherea Sepolia, která slouží obdobně jako hlavní síť Etherea. Blockchain použitý při práci představuje databázi pro uchování všech dat s garancí jejich integrity a dostupnosti. Na blockchainu se také uchovávají smart kontrakty, které v případě Etherea jsou pomocí EVM [3] (Ethereum Virtual Machine) spouštěny. Samotná aplikace je vytvořena pomocí frameworku React Native [4] umožňující tvorbu aplikací pomocí jednotného kódu pro více cílových

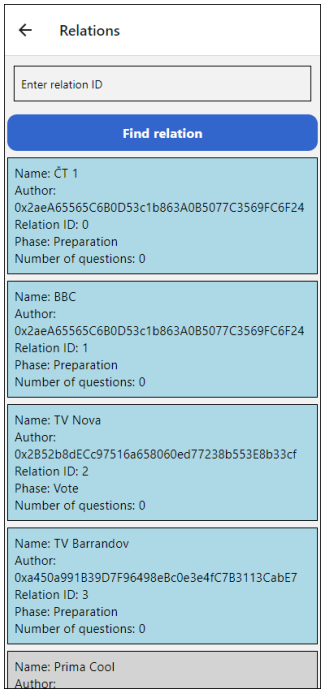
platforem. Dále jsem použil platformu Expo [5] podporující zobrazení aplikací v mobilní i ve webové formě. Webovou aplikaci jsem chtěl přidat jako rozšíření k samotné práci. Ke konci bych zmínil použití frameworku Truffle [6], který umožňuje migraci smart kontraktů na sítě Etherea a testovací blockchain Ganache, na kterém lze lokálně testovat vytvořené smart kontrakty. Nakonec k integraci s uživateli pro mobilní zařízení jsem využil Metamask SDK [7] a krypto peněženku Metamask [8].

5. Popis aplikace

Hlavním výstupem práce jsou 2 aplikace, jedna pro moderátory relací, kterým umožňuje vytvořit a spravovat relace a druhá pro uživatele pro pokládání jejich dotazů a hlasování. Díky poskytnutí smart kontraktu od vedoucího práce, který slouží ke správě identit, jsem vytvořil navíc ještě 3. aplikaci, která simuluje ověření identit uživatelů. Představte si, jako kdybyste šli na pobočku České pošty, kde vám zaměstnanec na přepážce po předložení vašich osobních údajů ověří vaši identitu a propojí ji s blockchainovou adresou. Přidání uživatelů do mých 2 aplikací je tedy závislé na této 3. aplikaci, ve které musí být adresa uživatelů ověřena, aby byli schopni interakce.



Obrázek 1. Zobrazení konkrétní relace z aplikace pro moderátora



Obrázek 2. Zobrazení relací v aplikaci pro účastníky relace

Aplikace pro moderátora

Moderátor si může vytvořit vlastní relaci, kde zadává, zda je veřejná nebo soukromá, její název, začátek a čas, do kdy může její publikum zasílat dotazy. V soukromé relaci musí navíc přidat seznam pozvaných účastníků, kterým je dovoleno pokládat otázky a hlasovat. Relace je při vytvoření v přípravném stavu a ve chvíli, kdy chce spustit hlasování, změní stav relace pomocí tlačítka. V této chvíli již nelze v soukromé relaci přidávat další účastníky a publikum dostává možnost začít pokládat otázky a hlasovat.

Aplikace pro účastníky relace

Publiku je umožněno vyhledávat jednotlivé relace a případně vyhledat tu konkrétní podle jejího ID, které získají od moderátora. Šedé označení relace značí, že již skončila. Po rozkliknutí relace lze číst ootázky ostatních. Uživatel aplikace může v relaci položit svůj dotaz nebo hlasovat pro otázky druhých, aby se zvýšila šance, že budou moderátorem zodpovězeny.

Aplikace pro poskytovatele identity

Jako nadstavba je třetí aplikace pro správu identit. Její rozhraní nabízí autorovi smart kontraktu přidání entit označených jako Identity provider. Těm je v aplikaci umožněno přidat ověřené uživatele na základě identity, kterou poskytnou.

6. Závěr

Při implementaci aplikace a integraci peněženky Metamask s dalšími knihovnami jsem zjistil jejich nekonzistentí chování. Díky tomu, že pro uživatele bude lepší pro rychlou interakci použít webovou aplikaci než stahovat mobilní a díky chování Metamask SDK jsem se rozhodl vytvořit aplikaci jako webovou. Ta funguje a zobrazuje se díky React Native prakticky stejně jako její mobilní verze. Aplikace slouží jako rozhraní, skrze které uživatel dokáže měnit stav blockchainu pomocí vyvolaných transakcí ze smart kontraktů, které má blockchain v sobě uložen.

V mé práci se podařilo vytvořit smart kontrakt umožňující správu relací a zaintegrovat ho tak do funkčních aplikací. V průběhu jsem zjistil, že webová aplikace bude lepší než mobilní a proto jsem se rozhodl mírně se odchýlit od zadání. Sekundárním cílem práce je poukázat na možnosti blockchainu a uvědomění si schopností této technologie.

Poděkování

Nakonec bych chtěl velice poděkovat vedoucímu práce Ing. Ivanu Homoliakovi, Ph.D. za jeho cenné rady při psaní bakalářské práce a poskytnutí smart kontraktů k jejímu rozšíření.

Reference

[1] Slido. Slido - audience interaction made easy. https://www.slido.com/.

[2] Mentimeter. Interactive presentation software - mentimeter. https://www.mentimeter.com/.

[3] Ethereum virtual machine (evm) — ethereum.org. https://ethereum.org/en/developers/docs/evm/.

[4] React Native. React native · learn once, write anywhere. https://reactnative.dev/.

[5] Expo. Expo. https://expo.dev/.

[6] Truffle. Truffle - truffle suite. https://trufflesuite.com/truffle/.

[7] Metamask. Sdk — metamask. https://metamask.io/sdk/.

[8] Metamask. The crypto wallet for defi, web3 dapps and nfts — metamask. https://metamask.io/.