

## Abstrakt:

V tejto bakalárskej práci si kladieme za cieľ navrhnuť a implementovať peer-to-peer variantu služby pre komentovanie internetových zdrojov. Z funkčného hľadiska sa jedná o implementáciu diskusného fóra v P2P prostredí. Pokúšame sa o dosiahnutie čo najviac decentralizovaného riešenia pri splnení podmienok: ukladanie obsahu v distribuovanej hašovacej tabuľke, zavedenie konceptu identity užívateľa a ochrana tejto identity pred odcudzením. Pri analýze dochádzame k záveru, že v prostredí kde užívatelia neustanovujú väzby a generovaný obsah je broadcastového typu je nutná globálne dôverovaná autorita. Tá pomocou mechanizmu prenosu dôvery umožní ľubovoľnému užívateľovi overiť autenticitu obsahu vytvoreného iným užívateľom systému. Zavádzame teda PKI s certifikačnou autoritou (CA). Záväzok maximálnej decentralizácie naplníme viacerými opatreniami na úrovni dizajnu aplikácie. Umožňujeme beh viacerých inštancií CA, minimalizujeme moc CA monitorovať činnosť užívateľov, cenzurovať ich obsah apod. Zároveň vytvárame priestor pre budúce zavedenie reputácie užívateľov. Užívateľské rozhranie aplikácie integrujeme do webového prehliadača, čím sa nám darí odtieniť užívateľa od zložitosti P2P modelu.