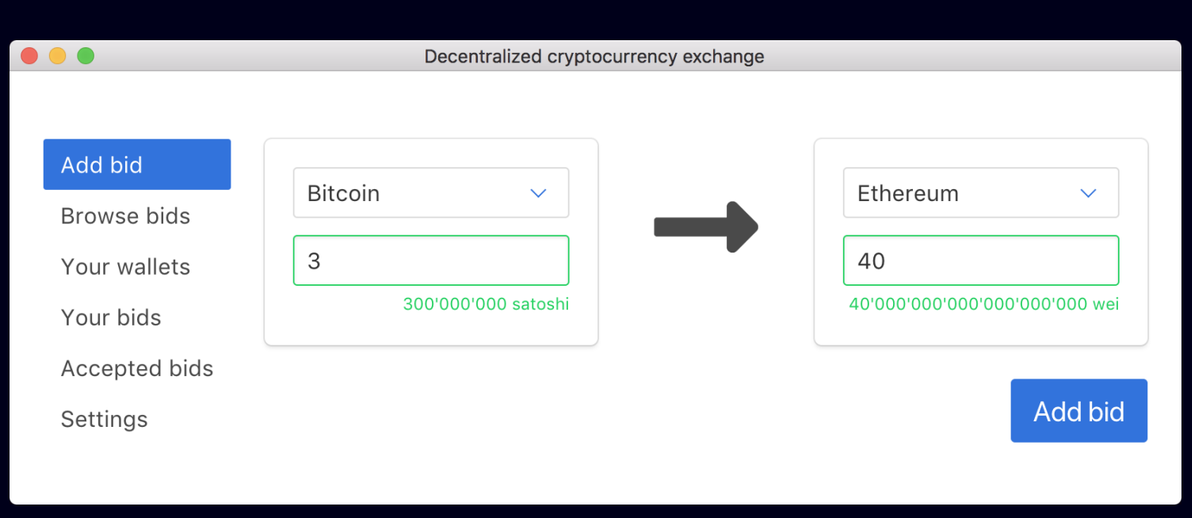
Decentraliserad växling av kryptovalutor

Inledning

Kryptovalutor ökar snabbt i popularitet. Numera finns det över 1 500 kryptovalutor [1] och deras totala börsvärde överstiger 400 miljarder amerikanska dollar [2]. Detta stora antal kryptovalutor innebär att efterfrågan att kunna växla mellan dem också ökar. Växling mellan olika kryptovalutor sker ofta genom centraliserade växlingskontor. Detta ger vissa fördelar men även ett antal nackdelar eftersom monetär säkerhet och anonymitet inte kan garanteras.

Ett alternativ till centraliserade växlingskontor är att systemet för att genomföra växlingar är decentraliserat. Syftet med detta kandidatarbete är att sätta upp ett antal krav som en sådan decentraliserad växlingstjänst bör uppfylla för att därefter utveckla en prototyp som uppfyller dessa krav.

Det finns tre huvudproblem som behöver lösas för att en prototyp ska vara välfungerande. Det första problemet är att en växling ska kunna genomföras på ett decentraliserat men samtidigt säkert sätt. Det andra problemet är att det ska gå att lagra information som gör att användarna kan hitta varandra på ett decentraliserat sätt. Det tredje problemet är att det ska gå att upprätta en kommunikationskanal mellan två användare så att de kan genomföra en växling. Prototypen begränsas till Bitcoin, Ethereum och Ethereum Classic men den testas både på testnätverk och på riktiga nätverk.



Resultat

[Resultat för byten?]

Vi bedömer att de krav som specificerats för användargränssnittet har uppfyllts.

Intresserad? Här finns koden till prototypen:

Metod

Prototypen är uppdelad i två delar: ett användargränssnitt och ett program som sköter kommunikationen med andra decentraliserade system. Användargränssnittet ska vara snabbt, stabilt och användarvänligt men samtidigt ha en stor mängd användbara funktioner. Denna del implementeras som en webbapplikation och körs som en Electronapplikation. Större delen av användargränssnittet är implementerat i det funktionella programmeringsspråket Elm.

Den del som sköter kommunikationen med andra decentraliserade system är i sin tur uppdelad i de tre delar som beskrivs som huvudproblem i inledningen. För att genomföra en växling används så kallade atomiska växlingar (engelska: atomic swaps). Detta genomförs genom en typ av smarta kontrakt som kallas hashade tidslåsta kontrakt (engelska: hashed timelock contracts). Dessa kontrakt gör att säkerhet kan garanteras. De kontrakt som skapas i prototypen kommer att bedömas utifrån hur lång tid ett byte tar, hur mycket det kostar samt hur många par av kryptovalutor som går att växla mellan.

För att lagra information som gör att användarna kan hitta varandra och för att därefter upprätta kommunikationskanaler mellan dem används databasen OrbitDB. Det är en decentraliserad databas som bygger på ett antal andra decentraliserade tekniker. Databasen kan spara strängar och JSON-dokument, vilket är vad som behövs. Kommunikationen med själva blockkedjorna sker med Geth och Bitcoin core för Ethereum respektive Bitcoin.

Diskussion

Huvudsyftet med projektet är att bygga ett system som kan utföra decentraliserade växlingar. Detta har uppfyllts. Prototypen som demonstrerar detta har vissa säkerhetsproblem och stöder endast ett begränsat antal kryptovalutor. Däremot var syftet inte att bygga ett perfekt system. Målet var endast att visa att detta koncept är möjligt att använda och andra forskare kommer att ha möjligheten att vidare utforska området och uppnå målet att utveckla ett system som kan användas i produktionsmiljö.

Huvudproblemet med prototypens användargränssnittet är portabilitet. Samtidigt har den decentraliserade databasen större problem eftersom den är byggd med hjälp av experimentell teknologi. Dessa problem skulle kunna lösas genom byta ut de tekniker som de baseras på. Att arbeta med experimentella teknologier skapar oundvikligen problem. Däremot har vi gjort allt vi kunde för att genomföra detta projekt och med denna grund är det fullt möjligt att med mer tid bygga någonting ännu bättre.

1. CoinMarketCap. Cryptocurrency Market Capitalizations, https://coinmarketcap.com/ (hämtat 2018-04-30)
2. CoinMarketCap. Historical Snapshot - March 25, 2018, https://coinmarketcap.com/historical/20180325/ (hämtat 2018-03-26)