

Från:
Skickat:
Till:
Ämne:

Hur skulle en teknisk lösning för en registerbaserad e-krona kunna se ut?

Svar: Detta är enkelt, använd en kraftfull central databas med transaktionshantering och bygg ett api med tjänster (t.ex. REST) som kan skalas upp kraftigt för hög tillgänglighet.

Hur skulle en teknisk lösning för en värdebaserad e-krona kunna se ut?

Svar: Man skulle kunna använda en variant av blockkedjeteknik för detta. Vill man ha en centraliserad lösning istället för decentraliserad (public ledger) som bitcoin är så kan man byta ut metoden som bestämmer den rätta versionen av historiken i huvudboken. Bitcoin använder sig av "proof of work" men det skulle kunna bytas ut mot t.ex. digitala signaturer. Man kan tänka sig en central enhet (riksbanken) som signerar block istället för att ett kostsamt *nonce* beräknas och används för blockverifiering, man sparar elektricitet, hårdvara, omorganiseringar i liggaren, bekräftelsetider och propagering i nätet snabbas upp. Hela systemet skulle fungera mycket bättre än bitcoin med den stora skillnaden att man måste lita på en central enhet som har full kontroll och därmed möjligheten/rätten att censurera transaktioner. En variant kan vara att använda sig av en grupp av centrala enheter t.ex. 10 noder som alla får var sin digitala signatur, sedan kan man t.ex. kräva att minst 7 signaturer av 10 behövs för att signera ett block som godkänt i kedjan. Detta ger feltolerans om någon nod skulle falera eller hamna i "orätta händer". Vill man ha en lösning där ingen central spelare finns med i bilden så kan man titta närmare på algorand-lösningen av MIT prof. Silvio Micali. Det är en algoritm som löser "Byzantine Agreement" med hjälp av kryptografisk "Sortation" och enligt uppgift ska kunna skala upp och hantera miljontals transaktioner per sekund trots att det handlar om en "public ledger". <https://people.csail.mit.edu/nickolai/papers/gilad-algorand.pdf>

Vilka utmaningar och möjligheter ser ni med respektive e-kronalösning?

Svar: De som i dagsläget använder kontanter kommer förmodligen inte att gå över till e-kronor om de inte blir mer eller mindre tvingade till det, d.v.s. om kontanter försvinner och ersätts av e-kronor.

Fördelar registerbaserad e-krona:

- * Enkel lösning med välbeprövad teknik.
- * Full kontroll på utestående penningmängd (d.v.s. antalet e-kronor registrerade i databasen) och dess ägare.
- * Snabba transaktioner (ej begränsad av en "public ledger" som måste replikeras över internet)
- * Positiva pengar (som ej är skapade genom utlåning/skuld, fractional reserve banking)
- * Inga pengar kan gå förlorade och tappas bort
- * Större möjligheter att komma åt skattefusk och penningtvätt
- * Stöldrisk/rånrisk liten

Nackdelar registerbaserad e-krona:

- * Ingen anonymitet då databasen innehåller alla ägares personnummer/kontonummer och deras respektive saldo.
- * Fiat = Ingen fysisk bakomliggande vara (t.ex. guld, silver).
- * Oändligt antal e-kronor kan skapas.
- * Ersätter ej kontanter eftersom anonymiteten försvinner
- * Databasen blir en "Single Point of Failure" som måste hanteras med spegling, backuper, olika fysiska serverhallar osv. för att hålla hög tillgänglighet.

- * Kan utsättas för ddos-attacker och bli otillgänglig eller stundtals mindre tillgänglig.
- * Trovärdighetsrisk/inflationsrisk (Befolkningen kan tappa förtroende för valutan om riksbanken plötsligt beslutar att utöka penningmängden avsevärt)
- * Övervakningssamhälle? Staten kan konfiskera medborgarnas tillgångar/pengar, risken finns även om den är liten.

Fördelar värdebaserad e-krona:

- * Kan lagras offline på ett minne/lagringsmedia.
- * Stor anonymitet
- * Kan ersätta kontanter i många avseenden
- * Kan fortsätta fungera även om delar av nätet slås ut
- * Kan konstrueras med begränsning av total penningmängd = inflationssskyddad.
- * Positiva pengar (som ej är skapade genom utlåning/skuld, fractional reserve banking)

Nackdelar värdebaserad e-krona:

- * Pengar kan tappas bort eller gå förlorade om lagringsmedia havererar.
- * Krångligt att ta reda på saldot på ett offline minneskort.
- * Fiat = Ingen fysisk bakomliggande vara (t.ex. guld, silver).
- * Större möjlighet att gömma tillgångar och utföra svarta affärer.
- * Stöldrisk/Rånrisk för bäraren av lagringsmedia med "offline"-pengar på.

Hur ser er vision för en e-krona ut, finns andra lösningar än register- och värdebaserad som ni bedömer är bättre lämpade?

Svar: Jag skulle föredra en e-krona med koppling till någon underliggande vara t.ex. guld eller silver med någon lämplig konverterings-ratio (t.ex. 1 gram 99,9% silver = 5 st e-kronor) där riksbanken står som garant för den fysiska förvaringen. Jag tänker mig en lösning liknande den tidigare omåttligt populära e-gold <https://en.wikipedia.org/wiki/E-gold> med den skillnaden att riksbanken är garanten bakom allt, d.v.s. både förvaring och utfärdande av korrekt antal e-kronor i förhållande till fysiskt metallinnehav. Man kan även tänka sig en lösning utan fysisk koppling till ädla metaller (fiat) men inte skapad genom kredit/skuld som dagens SEK, då blir det extra viktigt med en mycket restriktiv policy vad gäller att utöka penningmängden (inflationsmål 0%) samt att valutan måste göras gällande som lagligt betalningsmedel för skatteinbetalning för att få högt förtroende och stor efterfrågan/spridning.

Vad saknas i vårt koncept?

Svar: Kopplingen av e-kronor till nuvarande SEK. Hur ska detta hanteras? Ska det finnas två parallella valutor där en är skapad genom skuld (fractional reserve banking) och en som inte är det?. Ska båda gälla som giltigt betalningsmedel för skatteinbetalning?

Jörgen Bilander
Creang AB