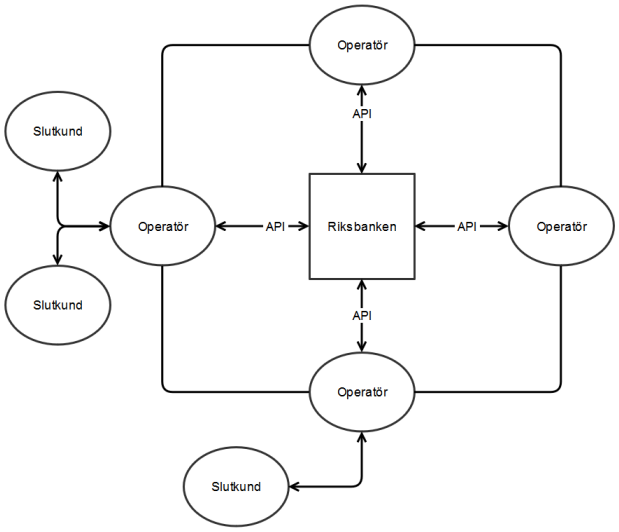
## Teknisk lösning för e-krona

Detta förslag för e-krona består av en distribuerad blockkedja där utvalda, och av Riksbanken godkända, operatörer utgör ryggraden i själva lösningen. Riksbanken ansvarar för protokollet, dess logik och egenskaper. Operatörerna ansvarar för exekvering och verifiering av transaktioner. Lösningen bygger på kryptoteknik men ska inte jämföras med de kryptovalutor som idag är populära.

Lösningen är uppdelad i två delar varav den ena, registerdelen håller ägande-registrerade adresser som ingår i ett "e-konto" som operatörerna rapporterar till Riksbanken. Riksbanken för register över samtliga adresser samt ansvarar för distribuering av dessa till operatörer.

Den andra delen består av en värdebaserad, hos Riksbanken ej ägande-registrerad del som bygger på anonyma adresser som utgör en "e-plånbok". De anonyma adresserna kan av Riksbanken begränsas till storlek och antal transaktioner per tidsenhet.




Figur 1. Övergripande arkitektur

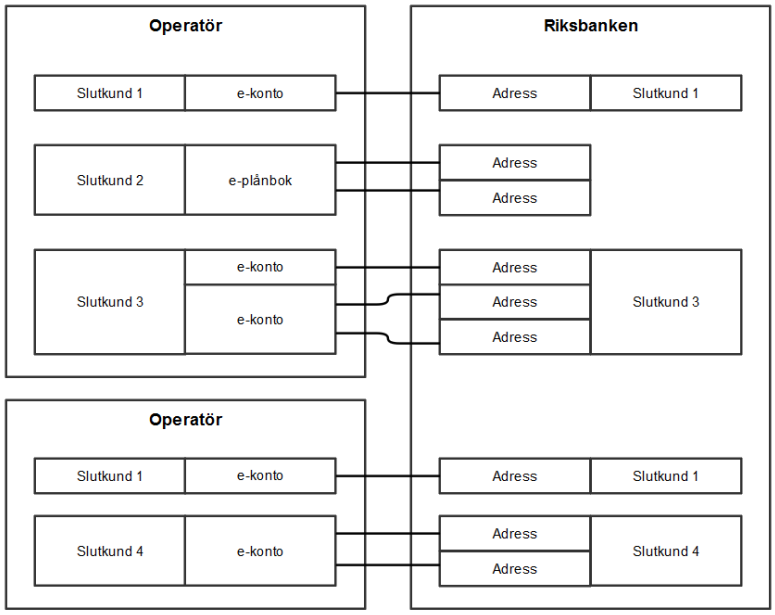
Operatörerna agerar mellanhand och tillåts i utbyte att driva kedjan, ta emot och verifiera transaktioner från slutkunder. De kan även tillhandahålla tjänster och produkter baserade på e-kronan samt erbjuda sparande i e-krona. Då samtliga operatörer validerar kedjan har systemet ingen så kallad single-point-of-failure. Dock är Riksbanken som ägare av protokollet ansvarig för att protokollet inte utnyttjas felaktigt.

Som ägare av protokollet kan också Riksbanken styra över generering av nya e-kronor, ränta för registrerade eller ej registrerade adresser, om adresser ska frysas eller begränsas samt möjligheten till "sedelbyte" där Riksbanken går ut med att adresser skapade innan visst datum kommer nollställas.

## Registerbaserad kärna

Varje e-krona på ett e-konto innebär en direkt fordran på Riksbanken. Varje e-konto är direkt knuten till en privatperson, företag eller annan juridisk person. Transaktionerna mellan dessa adresser bokförs i kedjan som drivs och verifieras av operatörer. En transaktion är i detta sammanhang en överföring av e-kronor mellan två adresser.

Operatörerna kan vara affärsbanker, försäkringsbolag eller andra av Riksbanken godkända aktörer. För att skapa en adress ska en slutkund vända sig till en av dessa operatörer som i sin tur erhåller adresser av Riksbanken.




Figur 2. Konto- och adress-exempel

- Slutkund kan ha konto hos en eller flera operatörer.
- Varje e-konto är direkt bundet till en eller flera adresser

Det är endast via en operatör som slutkunder kan lagra de registrerade e-kronorna. Operatören erbjuder tjänsten till slutkund och har ansvaret för kundkännedom. Konton hos dessa operatörer kan liknas vid vanliga bankkonton och här kan operatörerna erbjuda inlåning, utlåning och kringliggande tjänster. Ett konto hos en operatör kan spänna över flera e-krona-adresser hos Riksbanken.

Genom att ha flera adresser hos Riksbanken länkade till samma konto blir det svårt för operatörer att dra slutsatser om varandras slutkunder. Detta är således en tjänst som operatörer kan men inte behöver erbjuda sina kunder.

### Värdebaserat lager

E-plånböcker kan anonymt skapas upp på kedjan. E-kronor kan sedan överföras från andra e-plånböcker eller e-konton till den nya e-plånboken. E-kronor överförda på detta sätt innebär fortfarande en fordran på Riksbanken som dock inte känner till vem som är fordringshavaren. Enda sättet att obestridligt bevisa sitt ägande av adressen är att göra en överföring till ett e-konto. Fram tills att e-kronan flyttats tillbaka till ett e-konto är denna del av lösningen således helt värdebaserad. Denna tekniska lösning tillåter adresser att spendera utan uppkoppling, antingen via överförandet av e-plånboken eller via transaktioner från eller till andra adresser som verifieras på kedjan först när uppkoppling finns. På något av dessa sätt kan således tredje-part erbjuda betaltjänster där värdet lagras på kort, så som SL-kort, eller i en app. Detta till exempel för turister som saknar möjlighet att identifiera sig elektroniskt eller på platser där uppkoppling saknas.

### Tekniska egenskaper

Eftersom blockkedjan är sluten till ett begränsat antal operatörer som i stor utsträckning litar på varandra tillåts en mindre strikt konsensusalgoritm som möjliggör hög transaktionsprestanda. Dagens kryptovalutasystem är i många fall anonyma där noderna inte litar på varandra, detta begränsar ofta hastighet och förlänger valideringstid samt gör det svårare att skala upp transaktionsmängd.

Protokollet och koden som bestämmer kedjans egenskaper, tillåts bara förändras av Riksbanken. Vid förändring av protokollet ska samtliga operatörer uppdatera sin mjukvara för att kunna fortsätta verifiera transaktioner. Vidare möjliggör det också operatörerna emellan att komma överens om icke betrodda personer och exempelvis inte verifiera transaktioner där adresser eller konton är frysta.

Förslaget ovan kan till exempel byggas med Distributed Ledger Technolgy liknande open source projekten Tendermint eller Quorum.

Visigon har tagit fram en prototyp-lösning för nordisk värdepappershandel i samarbete med Uppsala och Linköpings universitet. Visigon samarbetar gärna med Riksbanken kring att ta fram en prototyp-lösning för e-kronan.