Taler for e-Krona

Introduction

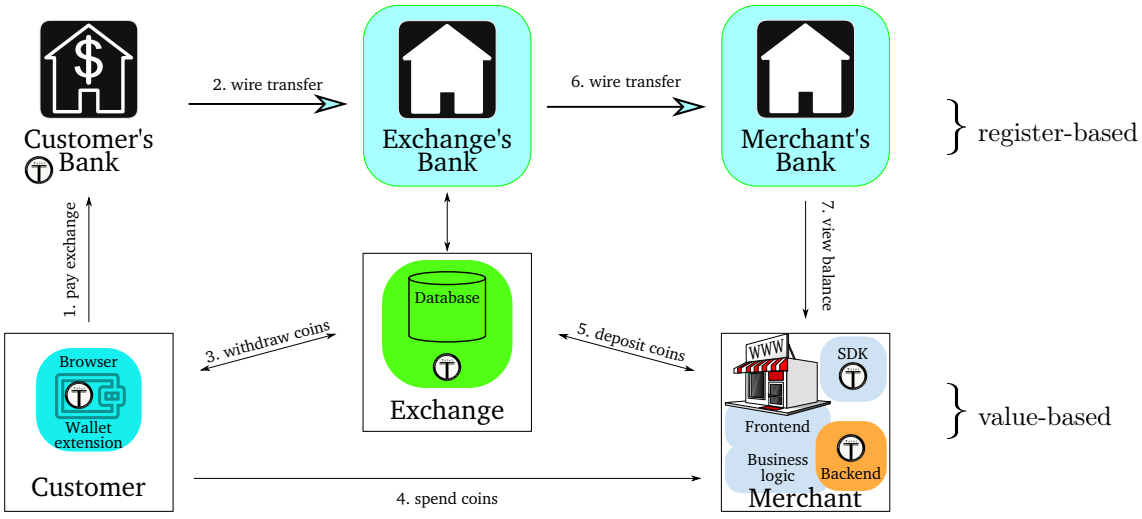
Taler Systems is developing an online payment system called Taler, that could easily fit the requirements of the e-Krona project.

Taler is an open source system based on a consumer wallet, merchant backend and a central exchange for payment processing. It provides instant one-click payments, implements privacy-by-design and assures receiver transparency for tax purposes using modern cryptography. It is fast and efficient, and can hence also cover micro-payments (payments of 1 cent) economically.

The USPs of Taler are:

- All operations provide cryptographically secured, with mathematical proofs for courts and auditors
- Customer payments are privacy-preserving, like cash
- Merchants are identifiable in each payment they receive
- Payments are in existing currencies
- Payment fraud is eliminated, short of catastrophic failure in cryptographic primitives
- Linear scalability ensures Taler handles transaction volumes of widely used systems
- Suitable for micro-payments due to very low transaction costs
- Ease of use (one-click, instant, no authentication during payment, again like cash)
- Open standard protocol without patents, with free reference implementation

The Taler architecture includes a register-based system of bank accounts for customers and merchants with an escrow-account for the exchange. The exchange signs electronic coins into existence, customers use them to sign contracts and merchants deposit them in return for a credit to the register. The exchange collects cryptographic proofs that it operates correctly, which are then checked by an auditor (auditor not shown):



What would a solution for a register-based e-Krona look like?

Taler's focus is on a cryptographic protocol for a value-based transaction system. However, Taler requires integration with some register-based accounting system, equivalent to traditional bank accounts. For this, it would be possible to use a permissioned block chain. Taler aggregates many small transactions from different customers to the same merchant, thereby reducing the transaction rate in the register-based solution.

What would a solution for a value-based e-Krona look like?

Taler issues electronic coins based on deposits into an escrow account. Citizens could use their wallets to withdraw e-Krona from their traditional bank accounts, or they could be provided e-Krona directly (for example via social security) if they lack a bank account. Electronic coins are blindly signed by the issuing exchange, which is obliged to exchange e-Krona back into Krona when they are deposited by merchants. An auditor supervises the operation of the exchange.

Our vision is thus very close to the electronic cash system "DigiCash" proposed by David Chaum in the 1990s, except that Taler's design and implementation supports key features such as giving change, providing refunds, securely handling aborts and various other practical issues previous technical solutions lacked.

What is your vision for an e-Krona?

We imagine a realistic e-Krona solution based on the Taler system to be effectively a hybrid solution, with a register-based component and a value based component, in order to fulfill the maximum requirements outlined in "The Riksbank's e-Krona project" report.

The e-Krona Taler wallet can exist on smartphones, in browsers, on smartcards or secure USB sticks. It is filled via wire-transfer to the Taler exchange's escrow account, where the subject identifies the Taler wallet eligible to withdraw the e-Krona. Regulators could limit the amount an entity is entitled to exchange from Krona into e-Krona, like ATM limits. When withdrawing electronic coins, they are blindly signed by the Taler exchange and stored in the consumer's wallet, which is value-based. The consumer can then spend its coins at merchants using cryptographic signatures over electronic contracts. Merchants must immediately deposit the coins at the exchange, which performs an online check for double-spending. The exchange will then credit the merchant's register-based accounts.

Thus, the Taler system combines value-based and register-based accounting, providing anti-money laundering capabilities by making income transparent, identifying the users of the system (upon withdrawal and deposit), but also providing privacy for citizens by not requiring identification of the buyer for ordinary transactions. Thus, Taler is a hybrid system combining the advantages of value-based and register-based solutions.

Specifically, Taler addresses the following requirements outlined in the report:

Specified in Swedish Krona Taler is designed to work for all currencies for which a register-based accounting system exists.

Payment size Taler is designed to handle micropayments as well as arbitrarily large payments between consumers, companies and authorities. Regulation may impose limits on withdrawals and maximum amounts transacted.

Direct claim on Riksbank The Taler design involves the exchange owning an escrow account (for example, with the Riksbank) to keep the funds to back the issued electronic coins. The contractual obligations of the system are supposed to entitle the holder of e-Krona to exchange them anytime into other representations of Krona.

Accessible in real-time Customers and merchants always have access to their full account histories and their balances on their local computer. Backups and cross-device synchronization will also be supported.

Payments in real-time Payments typically clear in one network RTT. The system is designed for 24/7 operations.

Offline payments For Taler transactions, either the payer or the merchant must be online and able to communicate with the exchange. Otherwise the merchant cannot be sure that the payer did not double-spend and risks being defrauded.

Anonymous payments Taler is designed for payers to remain anonymous when buying goods, unless regulation requires disclosure (i.e. for particular sensitive purchases). However, the merchant is never anonymous.

e-Krona account A register-based account is required for merchants to receive transactions. The exchange also must have an escrow account.

Riksbank functions The Riksbank would primarily hold the escrow account. It could also either (1) run the operations of the exchange and guarantee the exchange of e-Krona in Swedish Krona directly, or (2) else audit privately operated exchanges similar to its regulatory oversight of conventional banks and payment processors.

No bank account necessary Taler can enable distribution of funds (i.e. from social security) directly to wallets. Thus, citizens having a Taler wallet could be given remittances without the need for a bank account. However, merchants must have a register-based bank account to receive payments.

Interest payments Taler could theoretically support interest on e-Krona by varying the exchange rate between e-Krona and Krona. Taler can also theoretically support *negative* interest on coins held long-term in wallets.

Connection to existing payment systems With proper system integration, wire transfers, debit and credit cards or even NFC-enabled ATMs could all be used to fund the e-Krona wallet.

Taler effectively provides electronic cash and thus solves the problem of gaining access to risk-free assets. As the Riksbank supervises the e-Krona escrow funds (either directly or by auditing the private operator), the government can assure citizens that they can always exchange e-Kronas back to cash. Thus, in Taler's design, the government acts as a trust anchor.

Taler removes inefficiencies the current system creates through fraud risks inherent in register-based systems. In Taler, citizens only ever authenticate to their bank (or social services). By avoiding disclosing personally identifying information or even performing credit card-style authentication via third parties, Taler improves usability and eliminates most vectors of authentication token compromise.

What challenges and opportunities do you envisage?

Taler provides the advantages of cash while supporting taxation and limiting criminal abuse, as recipients of payments are identifiable. Furthermore, Taler transactions are faster, easier and more secure than cash or credit card transactions.

The main challenge is the integration of the Taler merchant backend into the diverse POS systems that exist today. While integrating Taler can be done with a few hundred lines of code, NFC-enabled POS systems would require at least a firmware update. Convincing vendors to upgrade their systems will thus require a major up-front investment.

Taler also requires further development to ensure that wallets are available on all relevant platforms. However, consumer systems are much less diverse and hence this effort is significantly smaller.

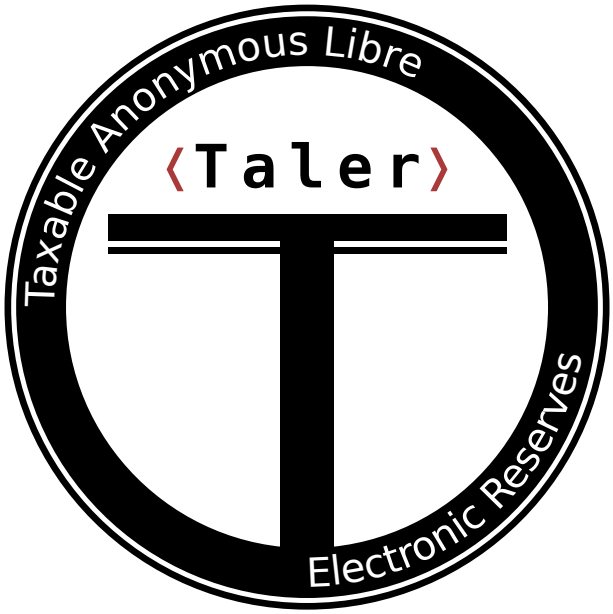
Deploying Taler at scale should have no major impact on monetary policy because the issued e-Krona would be 1:1 backed by Swedish Krona in the escrow account at the Riksbank. However, if there is a significant shift from the use of credit-cards to e-Krona, there might be a reduction in M2 from fractional reserve banking as e-Krona is debit-based while credit-cards are credit-based. Thus, instead of commercial bank money being created from debts, consumers may effectively hold e-Krona claims against the escrow account at the central bank. The resulting reduction in M2, and the loss of revenue at banks from credit-card interest payments, may require adjustments in monetary policies.

What is missing in our concept?

A key requirement for governments considering electronic payment systems is the preservation of the Commons. Cash is a Commons as all market participants have equal liberties in handling cash. If cash is replaced by proprietary solutions such as Visa's credit card system or ApplePay, these companies have exclusive control over critical infrastructure, which often leads to high fees. Worse, such payment service providers may discriminate against individuals or certain businesses and can refuse service to individuals or businesses without judicial oversight.

In contrast, Taler is implemented as Free Software distributed under the GNU General Public License, and without patent encumbrances. This ensures that any government retains sovereignty after deploying Taler, as it can liberally inspect, use and modify the software. In particular, no foreign government or company can impose their own restrictions or regulatory regime. Governments can foster competition between multiple Taler exchange operators, or run a Taler exchange as a government monopoly equivalent to a government mint for coins.

Contact



https://taler.net/