SofiWay e-krona description

Summary

ChromaWay AB and Sofitto NV suggest a register based system with the option of adding value based functionality, under the working name SofiWay. Sofitto offers the last mile solution and middleware using smart cards and phones for streamlined payments. The system runs on ChromaWay's Postchain consortium database system which is a hybrid between a private blockchain and a relational database. Sofitto technology is blockchain agnostic, and ChromaWay has a strong commitment to open-source software and integrating with a vibrant technology ecosystem. The system maximises flexibility and resilience in a rapidly changing technology landscape, while minimising the risks associated with vendor lock-in. ChromaWay and Sofitto are already cooperating to implement an integrated ATM, app and banking card solution for a European bank, backed by the Postchain blockchain. Swedish company Fidesmo's products are compatible with this software, providing an avenue to explore novel hardware form factors and wearables.

Introduction

ChromaWay AB is a blockchain startup founded in 2014 and based in Stockholm. ChromaWay has a history in payments, having worked with LHV bank to develop an award-winning blockchain-backed system for exchanging euros peer to peer. ChromaWay is currently working with Lantmäteriet to augment the current system of land registration with blockchain technology as well as with customers in other parts of the world.

Sofitto NV is a FinTech startup, established in January 2016. Sofitto aims to merge Blockchain technology into conventional banking card products through the development of the 'Sofitto card'.[1] The Sofitto card enables an autonomous store of value directly on the card, which disrupts the traditional card and remittance system. With only marginal infrastructure expenses and transaction costs, this new banking card will significantly lower the barrier to enter into banking services, while at the same time reduce maintenance costs pertinent to conventional financial networks. See footnote for demo materials.

Key people

The CTO of ChromaWay Alex Mizrahi did one of the first implementation of blockchain in the world, and created and lead the open source colored coins project from 2012. MSc in applied mathematics from Donetsk National University, graduating with honors. Author of several academic papers about blockchain.

ChromaWay has a strong technology team and network. Co-founder Dr Iddo Bentov from Technion University is active in research about zero-knowledge proofs. Dr Christopher Jämthagen has a PhD focused on Software Security and Blockchain. Kalle Rosenbaum is writing a book about bitcoin for Manning Publications and is an author of bitcoin protocol improvements. The ChromaWay advisory board includes Charlie Lee, founder of Litecoin, and Richard Brown, CTO of R3CEV.

[1] Demo of P2P cryptocurrency payments using a Card and Mobile app and ATM withdrawals: https://youtu.be/zRMVbf-8N9U
P2P transfers using ATM for customers who don't use smartphones: https://youtu.be/gsy1dHOc3sw
Example of card to card ad-hoc network in case of a disaster or missing connection: https://vimeo.com/155629363

After obtaining a PhD in Electrical Engineering from the KULeuven - IMEC, Belgium, Sofitto's CEO Dr Alexander Vasylchenko was working for leading R&D centers in Europe with involvement in top-notch industrial projects for global technology companies. Since 2012 Alexander has been at the technical forefront in a number of blockchain startups such as Megion R&D GmbH, Mycelium, Grid Singularity. In 2016, Alexander founded Sofitto NV a FinTech startup merging Blockchain technology into conventional banking card products.

Approach

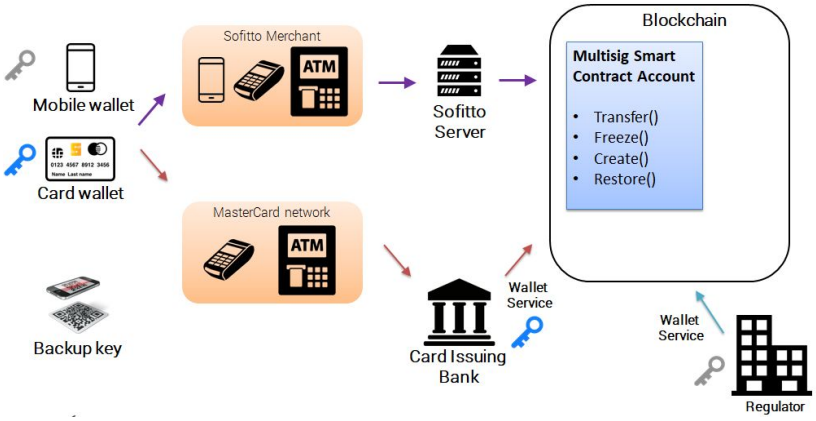
We propose making a register-based money (ledger) base system, because it offers a higher degree of flexibility and a broader spectrum of possible uses. Value-based systems can be developed on top of register-based, but the reverse is not possible. Thus committing to a register-based design does not preclude value-based systems closer to cash, but instead allows them to be adapted to the needs of society more easily, as the ledger can be used as a compatibility layer during upgrades.

- Blockchain allows the system to be decentralized, which allows higher resilience against cyberattacks, higher availability and higher trust among members of the system.
- Blockchain allows easy interoperation between members of the system. This will enable private companies to build new innovative products which can seamlessly integrate into the overall system.
- Blockchains are a globally growing phenomenon. A blockchain-based ledger might be easier to integrate with other blockchains to enable features like automatic currency exchange and so on.
- Non blockchain-based Electronic Cash Systems such as Proton, Chipknip and Quick were not very successful due to complexity and bad usability and have been decommissioned.

We propose a core blockchain-based ledger to have only a minimum number of primitives, such as account and transfer. Accounts should only contain enough information to allow regulatory oversight. Different kinds of financial operations and behaviours can be modelled using flexible authorization policies. In this case actual implementation of said operations can be moved to client systems, and thus they can evolve independently of the main ledger. The system has two main roles; a) Citizens are empowered to keep their money and transact independently of private financial institutions, and b) Private companies have the opportunity to develop innovative financial solutions while maintaining interoperability with existing systems and using trusted government currency.

Architecture overview

The e-krona ledger will be maintained using Postchain, with nodes run by a consortium of banks and financial organisations as appropriate. The key point of difference between Postchain and other private blockchains is that the transactions and data storage functionality is implemented using the traditional set of database tools, allowing for greater data complexity,



easier deployment, and more secure integration with existing systems. Postchain is the blockchain backend of the system, recording all e-krona accounts and transactions information. We estimate that the peak transaction volume of the e-krona network would be 1000tx/s at the very most.[2] This is extrapolated from recent available statistics about card, cash, and swish payments in Sweden. Postchain is more than capable of handling this volume.

Register- and value-based accounts can be implemented as multisignature (1 out of 2) blockchain smart-contract accounts. Key1 will be stored on the account issuer side (bank or other authorised payment institution) and can be used to fulfill all register-based properties requirements. Key2 will be stored on the user's device and used for value-based functionality (autonomous store of value, offline transactions) and to set account properties - limits, personal security blocks, etc.

Possibilities and considerations

- Only the central bank can issue new money.
- Accounts are registered by financial institutions (or the central bank itself). Names of physical people won't be mentioned in the ledger for privacy reasons, the only thing which is known publicly is the identity of the institution which registered an account on a user's behalf.
- Institutions are responsible for complying with AML/KYC requirements, and maintain a list which links account IDs to person names.
- Accounts might also be opened for companies, devices, smart contracts and so on.
- Some limited form of smart contracts (such as escrow contracts, for example) will be available on the main ledger.
- It will be possible for financial institutions to create and maintain subledgers.
- Value-based systems can be developed on top of the ledger system as a special kind of authorization policy. Thus value-based systems can be seamlessly integrated with register-based ones. There could even be more than one value-based system. The common ledger allows different systems to interoperate.

User experience

Flexible authorization policies allow for different kinds of interactions for different situations:

- Computer or mobile (software) wallet
- Hardware wallet, such as a smart card/bank card
- Hybrid wallet which combines a smartphone app with a bank card
- Externally managed account

The system will allow for multi-factor authentication. For example, if a person keeps a large amount of money on her account, she might require that spending is only possible if authorized by both her payment card (hardware wallet) and her bank, which latter would do in-person authentication.

Hardware will be based on Sofitto technology, such as an EMV compatible blockchain wallet card applet. It can be used in conventional banking cards with contact and contactless (NFC) interfaces. The technology allows the use of any NFC smartphone as a PoS terminal to acquire Sofitto card payments without additional hardware devices, useful for small payments.

[2] A throughput capacity of 100 payments per second is appropriate for a national level domestic payments system, according to the Emerald Performance Testing Technical Paper from Royal Bank of Scotland