PhD subject: Security of a local exchange trading system based on device-to-device communication

Expected starting date: October 2024

Research unit: IRISA – UMR CNRS 6074
Team: INZU
Web site: http://www-inzu.irisa.fr
Address: Université Bretagne Sud, campus de Tohannic, F-56000 Vannes

PhD supervisors: Prof. F. Guidec, Prof. M. Omar
Contact: Frederic.Guidec@univ-ubs.fr

Overview of the PhD project

Traditional trading systems based on the blockchain technology can hardly be used to support a local economy (such as a local exchange trading system), not only because of the cost of cryptocurrency mining, but also because such systems require complete and continuous network connectivity in order to maintain the consensus on the state of the blockchain between all users. In [1], Lavoie and Tschudin propose the implementation of lighter systems, entirely decentralized, and based on trust and reputation within a community of participants. With such decentralized systems, transactions between community members do not necessarily require Internet access, servers, or systematic consensus. They can therefore rely exclusively on D2D (device-to-device) communications between mobile devices such as smartphones and tablets, using existing technologies such as Bluetooth and NFC.

However, the model outlined in [1] presents new problems in terms of cybersecurity. The totally decentralized approach, and the desire to be able to operate without any access to the Internet, result in the impossibility of resorting to any central authority capable of confirming the identity of a user, validating the transactions carried out between users, ensuring the non-repudiation of these transactions, maintaining their history, preventing replay attacks, etc. Indeed, although [5] describes a distributed ledger model that can be implemented in the form of a CRDT (Conflict-Free Replicated Datatype), no detail is given about how this CRDT can be deployed on mobile terminals, nor about the security problems posed by this model.

The thesis subject proposed here aims to explore these problems from the perspective of cybersecurity, proposing one or more solutions for each of them. Several major scientific challenges should thus be addressed:

• Credit-centric transaction paradigm: the main objective is to develop a new transaction model based on the exchange of digital credit cybersécuritéunits. This approach requires establishing a layer of trust around the notion of credit, which itself must be expressed in digital form, be digitally signed, and be exchanged directly between mobile devices via D2D technologies such as Bluetooth, NFC, or QR-Codes.

• Deferred credit transactions: the focus will be on formulating cryptographic protocols to support deferred credit transactions, ensuring that the validity of each transaction can be verified in a deferred manner, with very low connectivity requirements.

• Dynamic allocation and compensation: a central aspect is to explore mechanisms for the allocation and the cancellation of credits. The objective is to create a secure framework supporting the exchange of credits in a transitive manner (i.e., each unit of credit should be transferrable from one user to another) by guaranteeing the authenticity and the validity of each transaction, and preventing both replay and repudiation.

• Testimony and security: to reinforce the authenticity of transactions, we will consider the integration of witness mechanisms (via the use of third parties who may digitally sign a transaction to confirm that it was indeed carried out between two users) within the credit-based framework. Security measures will of course have to be taken to mitigate the risks posed by malicious participants and false witnesses.

• Decentralized management of certificates and cryptographic keys: verifying the identity of users, ensuring the authenticity and security of transactions require the use of cryptographic keys, which in this case must be shared and exchanged in a completely decentralized manner within the community of users. We will notably examine the possibilities offered by the concept of “web of trust”, which makes it possible to share certificates and public keys in a distributed manner between users, without requiring the use of a centralized certification authority.

• Efficient data models: digital credit units, certificates and encryption keys must be implemented using lightweight distributed data models adapted to D2D transactions between mobile devices. We will focus on distributed data structures such as CRDTs (Conflict-Free Replicated Datatypes), which make it possible to maintain multiple replicas of the same data structure over a network of communicating nodes, while maintaining overall consistency between these replicas [4]. The use of CRDTs in distributed systems involving D2D transmissions has already been investigated by members of the INZU team [2, 3]. However the security of CRDT-based systems has only been addressed recently in the literature [6, 7], so this question will need further investigation.

The research methodology will include an exhaustive review of the literature, particularly in the field of CRDTs and their security, trust models (including the Web of Trust), etc. It will further involve the creation of models to simulate real-world scenarios, the design of algorithms for credit transactions, and validation through simulation and operational implementations. The quality criteria for the results will include publication in renowned conferences and journals.

Required skills

This thesis work will involve the development of demonstrators running on smartphones or tablets. Experience with Java development is therefore required, and experience with Android application development would be a plus. A good command of the fundamental mechanisms of cybersecurity (encryption, authentication, signature, etc.) would also be very valuable.

Bibliography

1. Erick Lavoie and Christian Tschudin. *Local crypto-tokens for local economics*. In Proceedings of the 3rd International Workshop on Distributed Infrastructure for the Common Good (DICG '22). Association for Computing Machinery, New York, NY, USA, 43–48.. 2022. https://doi.org/10.1145/3565383.3566113

2. F. Guidec, Y. Mahéo, C. Noûs. *CRDT-based Collaborative Editing in OppNets: a Practical Experiment*, International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM), 2023. https://hal.science/hal-04249567

3. F. Guidec, Y. Mahéo, C. Noûs. *Supporting conflict-free replicated data types in opportunistic networks*. Peer-to-Peer Networking and Applications, 2022. https://dx.doi.org/10.1007/s12083-022-01404-6

4. M. Shapiro et al. Conflict-free Replicated Data Types. In 13th International Conference on Stabilization, Safety, and Security of Distributed Systems (SSS'2011), LNCS, Volume 6976, pp. 386-400, October 2011. http://dx.doi.org/10.1007/978-3-642-24550-3_29

5. Erick Lavoie. GOC-Ledger: State-based conflict-free replicated ledger from grow-only counters. May 2023. https://arxiv.org/abs/2305.16976

6. Kristof Jannes, Bert Lagaisse, and Wouter Joosen. Secure replication for client-centric data stores. In *3rd International Workshop on Distributed Infrastructure for the Common Good*, DICG 2022, pages 31--36. ACM, November 2022. https://doi.org/10.1145/3565383.3566111

7. Manuel Barbosa, Bernardo Ferreira, João Marques, Bernardo Portela, and Nuno Preguiça. Secure conflict-free replicated data types. In *International Conference on Distributed Computing and Networking 2021*, ICDCN 2021, pages 6--15. ACM, January 2021. http://dx.doi.org/10.1145/3427796.3427831