UNIVERSITE BRETAGNE LOIRE / MATHSTIC

UNIVERSITÉ DE RENNES 1

# THESE DE DOCTORAT DE

L'UNIVERSITE DE RENNES 1
COMUE UNIVERSITE BRETAGNE LOIRE

ECOLE DOCTORALE N° 601
*Mathématiques et Sciences et Technologies de l'Information et de la Communication*
Spécialité : Informatique

Par
## « Florian DOLD »

## « The GNU Taler System »

« Practical and Provably Secure Electronic Payments »

**Thèse présentée et soutenue à « Rennes », le « 25.02.2019 »**
**Unité de recherche : Inria**
**Thèse N° : 195897**

**Rapporteurs avant soutenance** :

| | |
|---|---|
| Philip ROGAWAY | Professeur à l'University of California, Davis |
| Sarah MEIKLEJOHN | Professeure à l'University College London |

**Composition du Jury :**

| | | |
|---|---|---|
| Président : | Alan SCHMITT | Chercheur à l'Inria Rennes |
| Examinateurs : | Philip ROGAWAY | Professeur à l'University of California, Davis |
| | Sarah MEIKLEJOHN | Professeure à l'University College London |
| | Alex PENTLAND | Professeur à Massachusetts Institute of Technology |
| Dir. de thèse : | Christian GROTHOFF | Professeur à Bern University of Applied Sciences |
| Co-dir. de thèse : | Jean-Louis LANET | Directeur de recherche, Inria |

**Titre :** Le système GNU Taler : Paiements électroniques pratiques et sécurisés.

**Mots clés :** *Monnaie électronique, Cryptographie, Sécurité, Systèmes distribués, Applications pratiques*

**Résumé :**

Les nouveaux protocoles de réseautage et cryptographiques peuvent considérablement améliorer les systèmes de paiement électroniques en ligne. Le présent mémoire porte sur la conception, la mise en œuvre et l'analyse sécuritaire du GNU Taler, un système de paiement respectueux de la vie privée conçu pour être pratique pour l'utilisation en ligne comme méthode de (micro-)paiement, et en même temps socialement et moralement responsable.

La base technique du GNU Taler peut être dû à l'e cash de David Chaum. Notre travail va au-delà de l'e-cash de Chaum avec un changement efficace, et la nouvelle notion de transparence des revenus garantissant que les marchands ne peuvent recevoir de manière fiable un paiement d'un payeur non fiable que lorsque leurs revenus du paiement est visible aux autorités fiscales.

La transparence des revenus est obtenue grâce à l'introduction d'un protocole d'actualisation donnant lieu à un changement anonyme pour un jeton partiellement dépensé sans avoir besoin de l'introduction d'une évasion fiscale échappatoire. De plus, nous démontrons la sécurité prouvable de la transparence anonyme de nos revenus e-cash, qui concerne en plus l'anonymat habituel et les propriétés infalsifiables de l'e-cash, ainsi que la conservation formelle des fonds et la transparence des revenus.

Notre mise en œuvre du GNU Taler est utilisable par des utilisateurs non experts et s'intègre à l'architecture du web moderne. Notre plateforme de paiement aborde une série de questions pratiques telles que la prodigue des conseils aux clients, le mode de remboursement, l'intégration avec les banques et les chèques "know-your-customer (KYC)", ainsi que les exigences de sécurité et de fiabilité de la plateforme web. Sur une seule machine, nous réalisons des taux d'opérations qui rivalisent avec ceux des processeurs de cartes de crédit commerciaux globaux.

Pendant que les crypto-monnaies basées sur la preuve de travail à l'instar de Bitcoin doivent encore être mises à l'échelle pour servir de substituant aux systèmes de paiement établis, d'autres systèmes plus efficaces basés sur les blockchains avec des algorithmes de consensus plus classiques pourraient avoir des applications prometteurs dans le secteur financier. Nous faisons dans la conception, la mise en œuvre et l'analyse de la Byzantine Set Union Consensus, un protocole de Byzantine consensus qui s'accorde sur un (Super-)ensemble d'éléments à la fois, au lieu d'accepter en séquence les éléments individuels sur un ensemble. Byzantine Set consensus peut être utilisé comme composante de base pour des chaînes de blocs de permissions, où (à l'instar du style Nakamoto consensus) des blocs entiers d'opérations sont convenus à la fois d'augmenter le taux d'opération.

**Title:** The GNU Taler System: Practical and Provably Secure Electronic Payments

**Keywords:** *Electronic Cash, Cryptography, Security, Distributed Systems, Practical Applications*

**Abstract:**

We describe the design and implementation of GNU Taler, an electronic payment system based on an extension of Chaumian online e-cash with efficient change. In addition to anonymity for customers, it provides the novel notion of income transparency, which guarantees that merchants can reliably receive a payment from an untrusted payer only when their income from the payment is visible to tax authorities.

Income transparency is achieved by the introduction of a refresh protocol, which gives anonymous change for a partially spent coin without introducing a tax evasion loophole. In addition to income transparency, the refresh protocol can be used to implement Camenisch-style atomic swaps, and to preserve anonymity in the presence of protocol aborts and crash faults with data loss by participants.

Furthermore, we show the provable security of our income-transparent anonymous e-cash, which, in addition to the usual anonymity and unforgeability properties of e-cash, also formally models conservation of funds and income transparency.

Our implementation of GNU Taler is usable by non-expert users and integrates with the modern Web architecture. Our payment platform addresses a range of practical issues, such as tipping customers, providing refunds, integrating with banks and know-your-customer (KYC) checks, as well as Web platform security and reliability requirements.

On a single machine, we achieve transaction rates that rival those of global, commercial credit card processors.

We increase the robustness of the exchange—the component that keeps bank money in escrow in exchange for e-cash—by adding an auditor component, which verifies the correct operation of the system and allows to detect a compromise or misbehavior of the exchange early.

Just like bank accounts have reason to exist besides bank notes, e-cash only serves as part of a whole payment system stack. Distributed ledgers have recently gained immense popularity as potential replacement for parts of the traditional financial industry. While cryptocurrencies based on proof-of-work such as Bitcoin have yet to scale to be useful as a replacement for established payment systems,
other more efficient systems based on blockchains with more classical consensus
algorithms might still have promising applications in the financial industry.

We design, implement and analyze the performance of Byzantine Set Union Consensus (BSC), a Byzantine consensus protocol that agrees on a (super-)set of elements at once, instead of sequentially agreeing on the individual elements of a set. While BSC is interesting in itself, it can also be used as a building block for permissioned blockchains, where—just like in Nakamoto-style consensus—whole blocks of transactions are agreed upon at once, increasing the transaction rate.