# Introduction to Credit Networks

## Security, Privacy, and Applications

Aniket Kate
Purdue University
aniket@purdue.edu

## ABSTRACT

Credit networks model transitive *IOweYou* (IOU) credit between their users. With their flexible-yet-scalable design and robustness against intrusion, we are observing a rapid increase in their popularity as a backbone of real-world permission-less payment settlement networks (e.g., Ripple and Stellar) as well as several other weak-identity systems requiring Sybil-tolerant communication. In payment scenarios, due to their unique capability to unite emerging crypto-currencies and user-defined currencies with the traditional fiat currency and banking systems, several existing and new payment enterprises are entering in this space. Nevertheless, this enthusiasm in the market significantly exceeds our understanding of security, privacy, and reliability of these inherently distributed systems. Currently employed ad hoc strategies to fix apparent flaws have made those systems vulnerable to bigger problems once they become lucrative targets for malicious players.

In this tutorial, we first define the concept of IOU credit networks, and describe some of the important credit network applications. We then describe and analyze recent and ongoing projects to improve the credit-network security, privacy and reliability. We end our discussion with interesting open problems and systems challenges in the field. This introductory tutorial is accessible to the standard CCS audience with graduate-level security knowledge.

## Keywords

I Owe You; Credit networks; Sybil tolerance; Trust networks; Ripple; Stellar; Blockchain

## 1. INTRODUCTION

Credit networks [3–5] model credit (or trust) among users in a network through a directed, weighted graph, where the value of each edge shows the amount of IOU credit that a user is willing to extend to another. As the loss of credit incurred by the honest users in a credit network is *independent* of the number of malicious users and is instead *bounded* [3] by the credit they have extended to a misbehaving user, credit networks constitute the core of a variety of Sybil-tolerant applications, such as trustworthy online marketplaces [16], spam filtering [11], and social networks [12]. Some of the emerging payment networks, such as Ripple [1] and Stellar [2], also rely on credit networks to represent and process the settlement transactions between users. Thanks to their scalability, speed, and cost-effectiveness for cross-currency transactions across the globe, several banks [6, 9, 10, 17, 18] have now started to use Ripple as a backbone for online transactions.



*CCS'16 October 24-28, 2016, Vienna, Austria*



ACM ISBN 978-1-4503-4139-4/16/10.

DOI: http://dx.doi.org/10.1145/2976749.2976755

## 2. PRIVACY ISSUES

Credit Networks, such as Ripple [1] and Stellar [2], similarly to cryptocurrencies, opted for a blockchain-based consensus to demonstrate reliability and consistancy of transactions through transparency. However, this public ledger leaves credit networks highly susceptible to the privacy attacks. In particular, pseudonymity employed in Ripple is not effective as transactions still remain linkable to each other, and they are susceptible to deanonymization attacks. Our recent work [14] demonstrates that users accounts as well as their transactions are easily linkable in Ripple. This is clearly conflicting with the users' desire to hide their credit links and their transactions [8], and thus developing a privacy-preserving transaction scheme is one of the key challenges with the credit networks today.

### 2.1 Private Credit Network Transactions

In this direction, Moreno-Sanchez et al. [13] formalize the integrity and privacy requirements of credit network transactions, and develop PrivPay, a centralized privacy-preserving architecture for credit networks, based on trusted hardware and data-oblivious computations. PrivPay provides formal privacy guarantees and is found to efficient enough to support the current Ripple transactions; however, the usage of trusted hardware can make its employment in real life quite problematic.

Nevertheless, a *centralized* cryptographic solution that does not rely on trusted hardware seems far-fetched; it is unclear how one could possibly read the network information required to perform transactions without breaking the privacy of the other users. Our ongoing work [7] moves from the observation that the user's credit links alone determine her available credit in the network and the amount of credit loss she can incur due to misbehaving users. Therefore, unlike Bitcoin and other cryptocurrencies, credit networks are an ideal target for a distributed architecture where each user maintains her own credit links locally and checks that her inflow and outflow of credit do not change without explicit consent. The work explores this approach, designing a distributed architecture Whispers that provides strong privacy guarantees, offers better scalability and reliability, enforces the correctness of transactions. Whispers, without requiring a blockchain (i.e., ledger and proof-of-work), guarantees integrity and privacy of link values and transactions using a novel combination of secret-sharing-based multi-party computation and digital signature chains.

Although above approaches provide best possible privacy and integrity guarantees, they are inherently incompatible with the existing real-world networks such as Ripple and Stellar. Given the effective attacks such as [14], it is important to develop privacy-preserving solutions that are compatible with Ripple and Stellar in their current form.

## 3. CONCURRENCY ISSUES

In credit networks, transactions over disjoints sets of links can be easily carried out concurrently. If, however, two or more transactions require more credit than available at a *shared* link, it is important to allow one transaction go through and abort the others, notifying the users in the involved paths. Most credit networks fail to consider this concurrency (or serialization) issue. To perform this serialization among distributed transactions, Ripple (and similarly Stellar) employ a tailored Ripple Protocol Consensus Algorithm (RPCA). RPCA should allow all non-faulty Ripple parties to agree on the same set and order of transactions to be applied to the public ledger in a decentralized manner. However, its safety and liveness properties have not yet being analyzed at all.

Among the academic solutions, Privpay [13] relies on the centralized hardware module to decide the order, while Whispers [7] employ the blocking solution with randomized delays such that some transactions are not delayed infinitely. In the tutorial, we also describe our effort to formally define the serialization requirement of the asynchronous credit network transaction, and design blocking as well as wait-free solutions for this purpose.

Finally, we explore the use of the developed techniques in the emerging Interledger Protocol [19], a technology to bridge the wide range of blockchain-based systems together, and the lightning network [15], designed to enable scalable payments in Bitcoin.

## 4. COMPARISON WITH CRYPTOCURRENCIES

The tutorial also compares credit network-based Ripple and Stellar networks with the contemporary Bitcoin and Ethereum like cryptocurrency systems. Cryptocurrencies are limited to transactions where both transacting parties agree on a common currency. Credit networks, instead, inherently enable cross-currency transactions in any user specified currency as long as they have a credit path of enough value. Thus, they are considered as a salient technology towards overcoming the drawbacks of traditional banking systems [10].

## 5. INTENDED AUDIENCE

The tutorial only expects graduate-level cryptography, security, and privacy knowledge from its audience. All required security, distributed systems as well as economics concepts will be introduces before using, and we expect this introductory tutorial is accessible to the standard ACM CCS audience.

## 6. SPEAKER BIO

Prof. Aniket Kate is an assistant Professor in the the computer science department at Purdue university. He designs, implements, and analyzes privacy and transparency enhancing technologies for networked systems. His current research integrates cryptography, distributed computing, and trusted hardware.

Before joining Purdue in 2015, Prof. Kate was a junior faculty member and an independent research group leader at Saarland University in Germany, where he was heading the Cryptographic Systems Research Group. He was a postdoctoral researcher at Max Planck Institute for Software Systems (MPI-SWS), Germany for 2010 until 2012, and he received his PhD from the University of Waterloo, Canada in 2010.

## 7. REFERENCES


[1] Ripple website. https://ripple.com/.

[2] Stellar website. https://www.stellar.org/.

[3] DeFigueiredo, D., and Barr, E. T. TrustDavis: A Non-Exploitable Online Reputation System. In *7th IEEE CEC* (2005), pp. 274–283.

[4] Fugger, R. Money as IOUs in Social Trust Networks & A Proposal for a Decentralized Currency Network Protocol, 2004.

[5] Ghosh, A., Mahdian, M., Reeves, D. M., Pennock, D. M., and Fugger, R. Mechanism Design on Trust Networks. In *WINE'07*.

[6] Holley, E. Earthport launches distributed ledger hub via Ripple. http://www.bankingtech.com/420912/earthport-launches-distributed-ledger-hub-via-ripple/.

[7] Kate, A., Maffei, M., Malavolta, G., and Moreno-Sanchez, P. Silentwhispers: Enforcing security and privacy in credit networks, 2016. http://crypsys.mmci.uni-saarland.de/projects/DecentralizedPrivPay/.

[8] Liu, A. Implementing the interledger protocol in ripple. https://ripple.com/insights/implementing-the-interledger-protocol/.

[9] Liu, A. Ripple Labs Signs First Two US Banks. https://ripple.com/ripple-labs-signs-first-two-us-banks/, 2014.

[10] Liu, A. Santander: Distributed Ledger Tech Could Save Banks $20 Billion a Year. https://ripple.com/blog/santander-distributed-ledger-tech-could-save-banks-20-billion-a-year/, 2015.

[11] Mislove, A., Post, A., Druschel, P., and Gummadi, K. P. Ostra: Leveraging Trust to Thwart Unwanted Communication. In *NSDI'08*.

[12] Mohaisen, A., Hopper, N., and Kim, Y. Keep your friends close: Incorporating trust into social network-based Sybil defenses. In *INFOCOM'11*.

[13] Moreno-Sanchez, P., Kate, A., Maffei, M., and Pecina, K. Privacy preserving payments in credit networks: Enabling trust with privacy in online marketplaces. In *NDSS'15*.

[14] Moreno-Sanchez, P., Zafar, M. B., and Kate, A. Listening to whispers of ripple: Linking wallets and deanonymizing transactions in the ripple network. *PoPETS 2016*, 4 (2016), 436–453.

[15] Poon, J., and Dryja, T. The bitcoin lightning network. https://lightning.network.

[16] Post, A., Shah, V., and Mislove, A. Bazaar: Strengthening User Reputations in Online Marketplaces. In *NSDI'11*.

[17] Rizzo, P. Fidor Becomes First Bank to Use Ripple Payment Protocol. http://www.coindesk.com/fidor-becomes-first-bank-to-use-ripple-payment-protocol/.

[18] Rizzo, P. Japan's SBI Holdings Teams With Ripple to Launch New Company. http://www.coindesk.com/sbi-holdings-ripple-new-company/.

[19] Thomas, S., and Schwartz, E. A Protocol for Interledger Payments.