Friendship Bracelet: A Blockchain With No Threat Model

Alexandra Schofield
Cornell University
Ithaca, NY 14850
xanda@cs.cornell.edu

Ethan Cecchetti
Cornell University
Ithaca, NY 14850
ethan@cs.cornell.edu

ABSTRACT

Blockchains, or distributed decentralized ledgers of transactions, have been popularized over the past decade as a means of generating VC funding, popular science articles, and status as an Internet celebrity. However, existing algorithms suffer from unnecessary complexity due to goals like fault tolerance and consensus. In this work, we propose Friendship Bracelet, a surprising new altchain paradigm built on a foundation of mutual trust. We demonstrate that Friendship Bracelet achieves fast and transparent computation and verification of blocks.

1. INTRODUCTION

Blockchain, blockchain blockchain. Blockchain blockchain blockchain blockchain blockchain. Blockchain blockchain, blockchain blockchain blockchain blockchain blockchain. Blockchain blockchain blockchain: blockchain blockchain? Blockchain blockchain blockchain? Blockchain blockchain?

2. STRUCTURE

Friendship Bracelet simplifies many of the elements of blockchains made needlessly complex by trust issues with respect to other users. Instead of issuing blocks of transactions, FB issues *rows* of KNOTS, or Known Non-Obfuscated Transactions. Each KNOT contains an unencoded, conditionless string containing the contents you want on the ledger. No proof is attached to each KNOT or row. It therefore becomes possible to directly transmit the contents of the transaction in plaintext to other decentralized nodes. This also allows the transmission of individual knots within a row, such that transactions may be logged immediately before a row is completed. The lack of need for proofs also eliminates the need for farming, saving potentially millions of dollars in computing resources spent for other blockchains.

3. TRUST

Friendship Bracelet is built on trust. In this regard, it differs from other blockchains with significant overhead allocated

Figure 1: An example state of Friendship Bracelet [1]. Note that rows may be left incomplete when transmitted.

to warding off possible threats. For instance, where other systems might encrypt transactions, making them more difficult to verify, Friendship Bracelet leaves them unencrypted and easy to verify. Friends can transmit bracelets to each other without worrying about consensus, as friends never disagree or deceive each other. Double spending is also not a concern in Friendship Bracelet; friends always pay each other back eventually.

4. HANDLING THREATS

As Friendship Bracelet is designed to be a high-performance blockchain protocol, it eschews many of the complex and expensive operations that blockchains like Bitcoin use to mitigate potential attacks. Many of these attacks are, however, unrealistic.

Instead we focus solely on the correctness and performance in the model where all participants are friends. As such, Friendship Bracelet needs no thread model. After all, friends don't let friends make bracelets with adversaries.

5. ACKNOWLEDGMENTS

6. REFERENCES

[1] M. Stewart. Friendship bracelets, all grown up. *Martha Stewart Living*, 2013.