Transitive Network

Tokenless IOweYou Based Credit Network

Adithya Bhat(🔊)[1] Pedro Moreno-Sanchez[2] Aniket Kate[1]

[1] Purdue University, [2] TU Wien

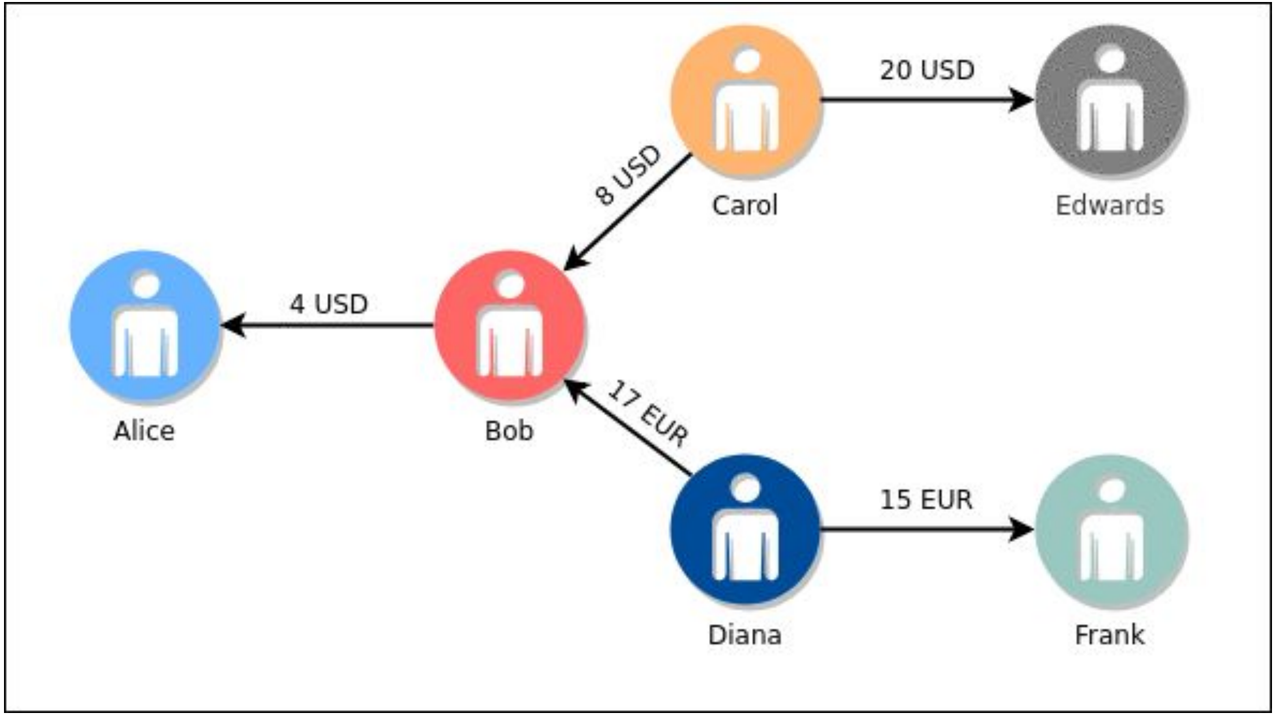
Website: https://transitive.network

Github: https://github.com/pedrorechez/transitivenetwork

Credit Networks

- ➔ Links represent Trust/Counterparty risks
- ➔ Can support multiple currencies and transactions over several hops
- ➔ Local Information is sufficient and global information is not necessary [SlientWhispers, NDSS 2017]

Example


20 USD
8 USD
Carol
Edwards
4 USD
Alice
Bob
17 EUR
15 EUR
Diana
Frank

Token-Based Credit Networks

- Prominent blockchain based instantiations are Ripple and Stellar
- Ripple and Stellar are Token based on XRP/XLM!
- Ripple is currently ~~#2~~ #3 in terms of market cap
- Stellar and Ripple share almost similar protocols

Ripple Credit Networks

- Uses a distributed ledger to record transfer of tokens and link updates
- A new account **must maintain reserve XRPs** to create accounts, links, offers, etc
  - It is necessary to buy XRP to use the credit network
- Suggested use of XRP is to stop DoS attack
- Number of Reserve XRP required for a transaction is decided centrally

Key Operations in Ripple

- ➔ Create Wallet / Add Node
- ➔ Create Link
- ➔ Create Offer
- ➔ Path-Based Payment

Transitive Network

- **Token-less** Credit Network built on top of Ethereum
- Transitive Network also allows:
  - Atomic multi-path (upto 4) payments
  - Nodes can be contracts that can be used to setup custom rules
  - Setting up challenge contracts for path based payments (Eg. find me a payment with fees upto 20 USD and I will reward you with 0.1 ETH)

Data Structures

```
struct Node {
        address addr;
        // Node Structure
}
```

```
struct Link {
        Node from;
        Node to;
        uint32 upperLimit;
        uint8 ripplingFlags;
        uint32 currentVal;
        uint32 feesFrom;
        uint32 feesTo;
        uint8 currencyID;
}
```

```
struct Offer {
        uint8 inputCurrencyID;
        uint32 inputAmount;
        uint8 outputCurrencyID;
        uint32 outputAmount;
        address provider;
}
```

Events

- ➔ New Node Registration
- ➔ New Link Setup
- ➔ Update Link
- ➔ New Order
- ➔ Cancel Order
- ➔ Payment

Public Functions

- Add Node
- Create Link
- Update Link
- Add Offer
- Cancel Offer
- Pay

Demo

Optimizations

- Keys for mappings are always ripemd160 hashes to minimize storage costs
- Pack two bools in a single ***uint8*** to save storage and retrieval gas costs
- Represent conversion rates as integers p/q
  - Example: If the conversion rate for USD/EUR is 0.667, it is represented as 3:2
  - This enables arbitrary (upto 2^{-32}) precision in conversion rates.
  - For example, a users pays 2 USD they get 1 EUR. However, if they pay 3 USD, they get 2 EUR.

Gas Costs

Function	Gas Cost
Add Node	43466
Create Link	117879
Update Link	37224
Create Offer	73971
Cancel Offer	36541
Pay	100799

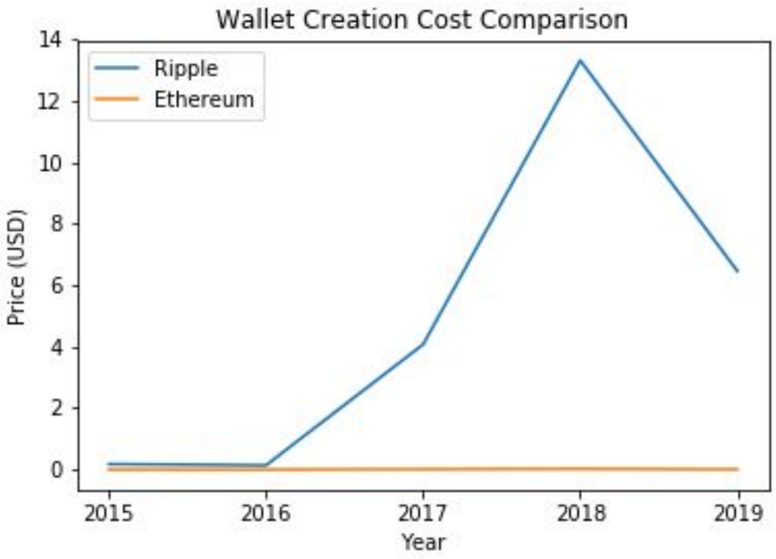
Early Results

Function in Ripple	Equivalent Function in Transitive Network	USD Cost in Ripple[1]	USD Cost in Ethereum[1]
Create Wallet	addNode	6.228	0.0108
Create Link	createLink	1.558	0.0294
Update Link	updateLink	0.0009	0.0093
Create Offer	addOffer	1.558	0.0185
Path Based Payment	creditNetPay	0.0009	0.0252

[1] Updated on February 10, 2019

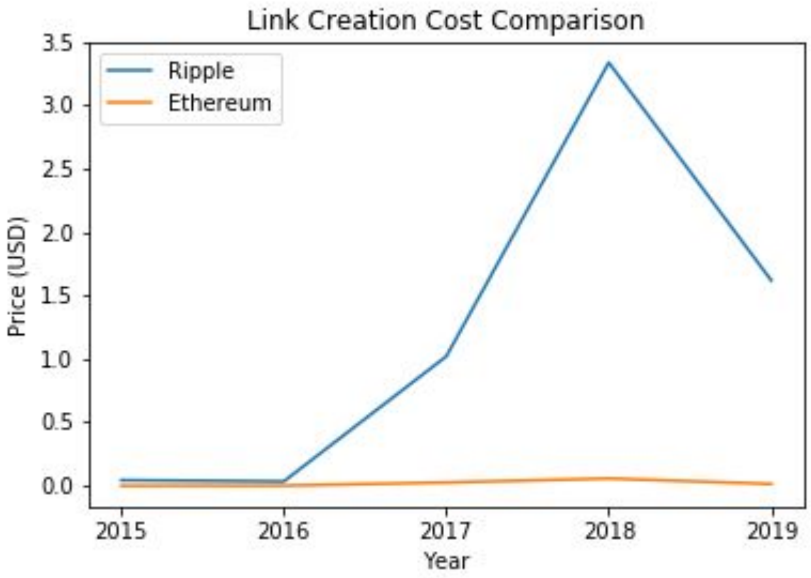
Cost Comparison
(Ripple vs Transitive Network)

Adding a Node



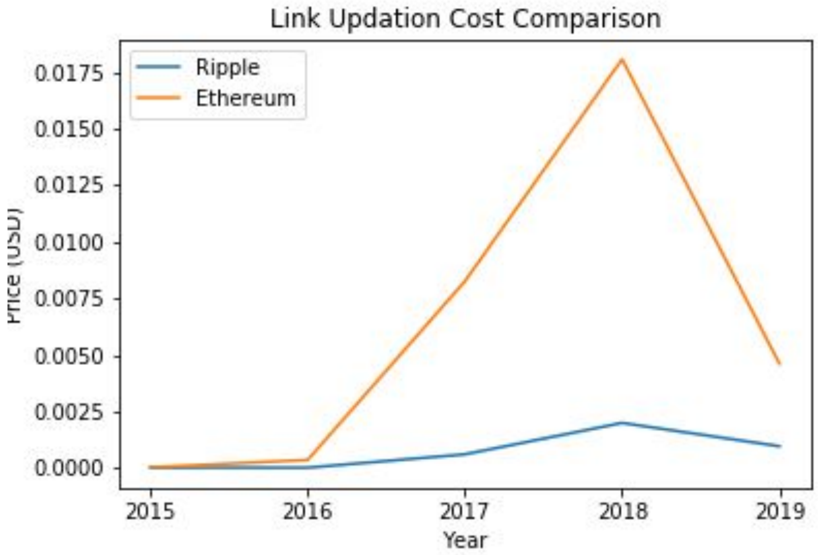
Cost Comparison (Ripple vs Transitive Network)

Link Creation



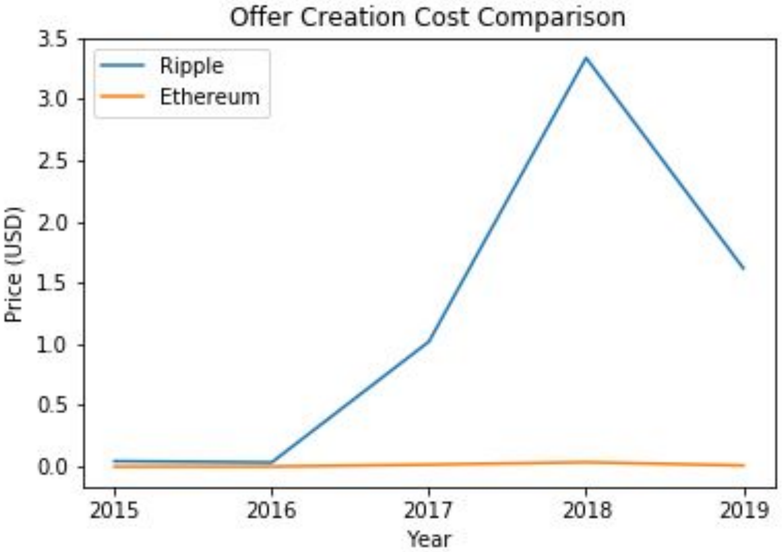
Cost Comparison
(Ripple vs Transitive Network)

Updating a Link



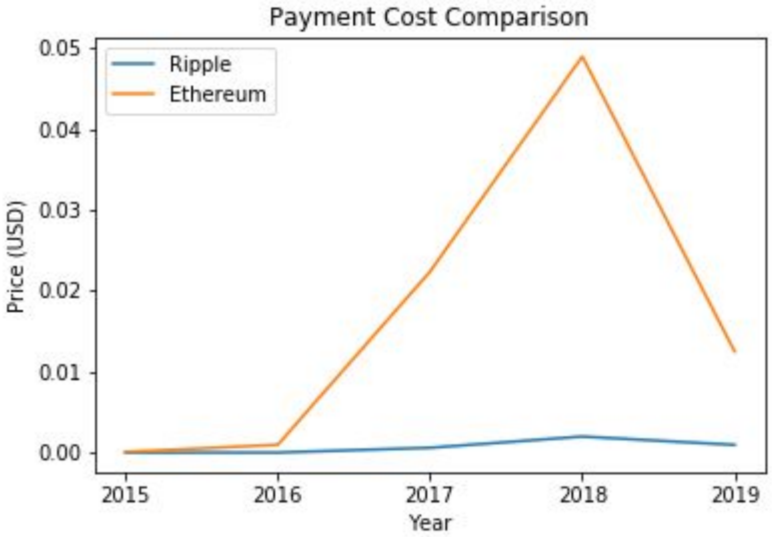
Cost Comparison (Ripple vs Transitive Network)

Offer Creation

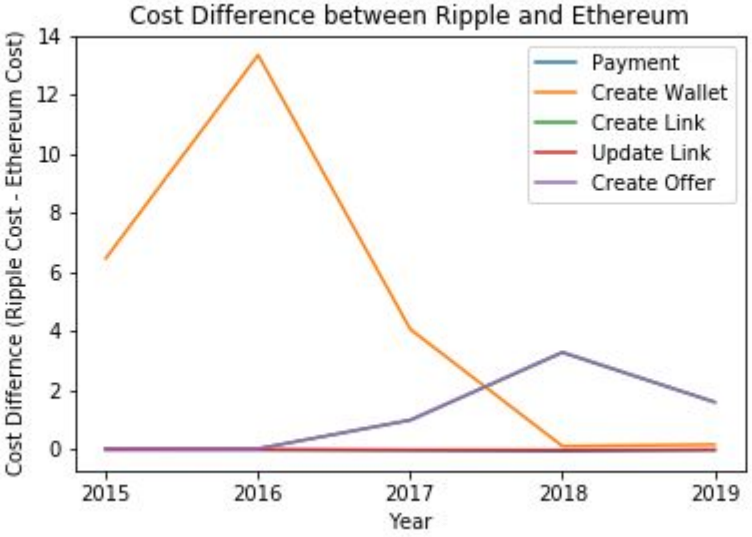


Cost Comparison
(Ripple vs Transitive Network)

Path Based Payments

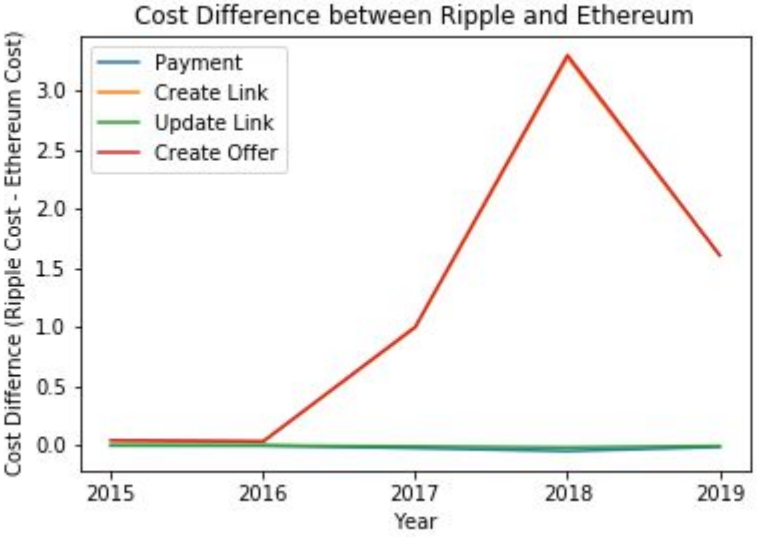


Comparing Difference of Costs (Ripple vs Transitive Network)



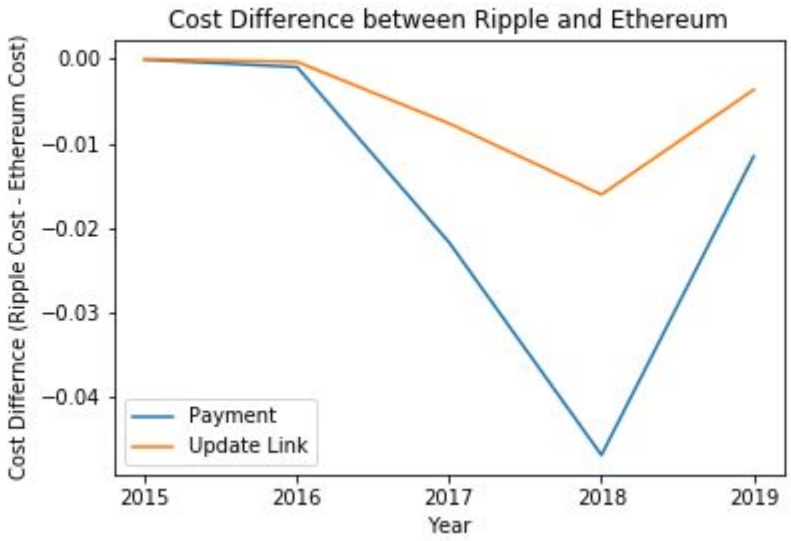
Comparing all the operations

Comparing Difference of Costs (Ripple vs Transitive Network)



Comparing Ratios without Create Wallet

Comparing Difference of Costs (Ripple vs Transitive Network)



Comparing Operations where Ethereum is more expensive; when compared to the first graph, this is small

Future Work: New Features

- Employing off-chain mechanisms to reduce transaction costs
- Introducing new features to credit links
  - Time-outs, interest rates
- Interoperability with other path-based transaction systems
  - Raiden, Lighting network, ...

Future Work: Privacy

- Achieving strong relationship anonymity for transitive network transaction
  - For on-chain network
  - For off-chain network

- Finding paths in transitive network while preserving privacy

Questions?