Analyzing Ripple Consensus

Jake Ginesin, Ryan Zhu

Ripple: what is it?

- Ripple: a company that facilitates financial transactions
- XRP: Ripple's "distributed" ledger that underpins the business

3rd Largest Crypto by Market Cap

#	Name	Price	1h %	24h %	7d %	Market Cap
1	Bitcoin BTC	$95,586.92	▲0.37%	▲0.32%	▲2.70%	$1,891,719,408,714
2	Ethereum ETH	$3,569.19	▲0.40%	▼0.85%	▲7.95%	$429,880,594,023
3	XRP XRP	$2.56	▲1.48%	▼4.75%	▲86.94%	$145,983,964,554
4	Tether USDT	$1.00	▼0.00%	▲0.01%	▲0.00%	$134,711,686,774
5	Solana SOL	$224.32	▲1.02%	▲0.66%	▼1.97%	$106,610,175,454

Ripple Consensus

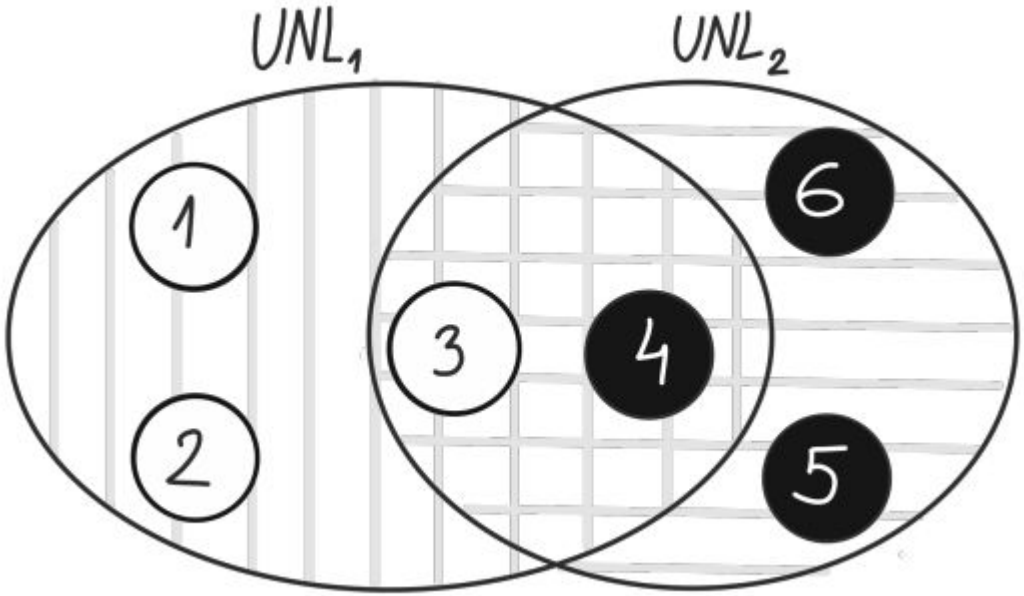
- *Different* from other crypto: no proof-of-work, nor proof-of-stake
- Rather, it is a *modified Byzantine Agreement Protocol*

Ripple Consensus

Two main protocol quirks:

- Nodes assume a *Unique Node List (UNL)*: a set of trusted nodes. A node only requires consensus within its UNL.
- Different UNLs *assumed* to have overlap

Ripple Consensus



src: A Security Analysis of Ripple Consensus, 2020

Ripple Consensus

Three Consensus Phases:

- **Phase Open:** all nodes gossip transaction proposals to each other
- **Phase Establish**: agree on proposal with UNL via successive consensus rounds bounded by heartbeat timers (!? requires synchronization)
- **Phase Accepted:** applying the agreed upon proposal, go back to open

Ripple Consensus

Standard protocol properties:

- **Validity:** correct transactions are eventually executed
- **Agreement:** if a correct node executes a transaction, all correct nodes eventually execute it
- **Integrity**: transactions aren’t executed more than once
- **Total Order:** all nodes execute transactions in the same order

Attacking Ripple!

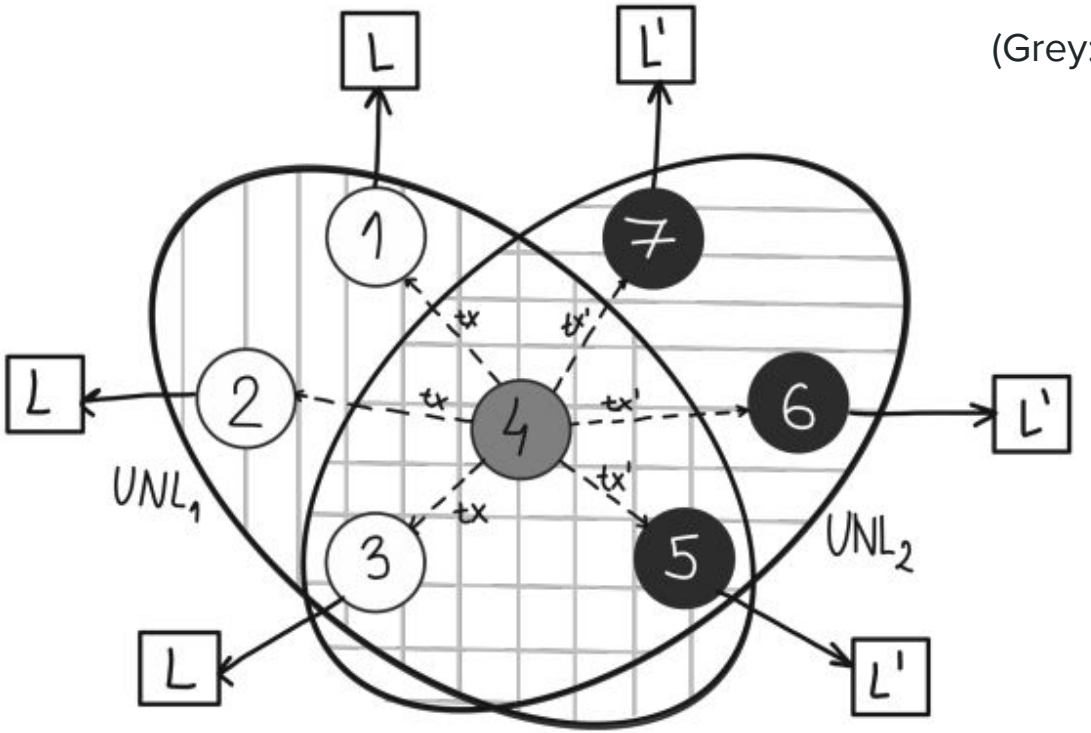
Security Analysis of Ripple Consensus

Ignacio Amores-Sesar[1]
University of Bern
ignacio.amores@inf.unibe.ch

Christian Cachin[1]
University of Bern
cachin@inf.unibe.ch

Jovana Mićić[1]
University of Bern
jovana.micic@inf.unibe.ch

Attacking Ripple!



(Grey: Byzantine)

Commit 9e48fc0

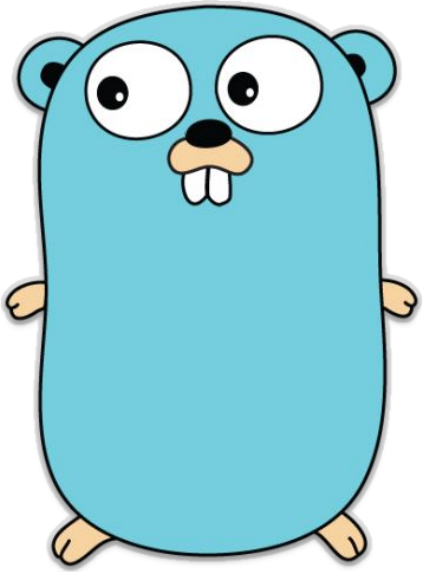
Bronek authored 2 weeks ago · ✕ 8 / 18 · Verified

Fix potential deadlock (#5124)

```
21     #define RIPPLE_BASICS_SCOPE_H_INCLUDED
22
23     #include <exception>
24   + #include <mutex>
25     #include <type_traits>
26     #include <utility>
27
```

Our Contributions

Mechanizing the protocol in SPIN



Creating a simple reference impl in Go

SPIN Mechanization: relatively simple, WIP

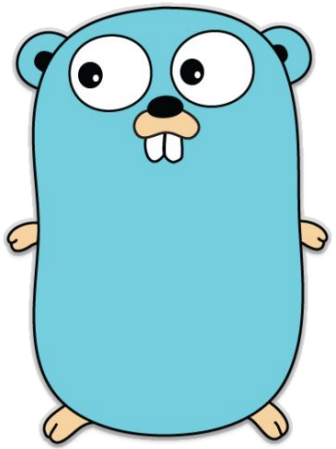
- About 500 lines of Promela
- Mechanized the Ripple properties in LTL
- Able to reproduce the attack (with the help of KORG, an attack synthesis tool)

```
OPEN:
  // simulate some shared and some unique transactions
  if
  :: atomic { new_tx = global_tx_num; }
  :: true -> atomic {
      global_tx_num++;
      new_tx = global_tx_num;
    }
  fi
  nt.proposal = new_tx;
  for (iter : 0 .. NUM_SERVERS) {
    if
    :: iter != serverId -> tn_sub[iter] ! nt;
    fi
  }

  do // receive transactions from other peers, building a proposal
  :: true -> atomic {
      for (iter : 0 .. NUM_SERVERS) {
```

Reference Implementation in Go

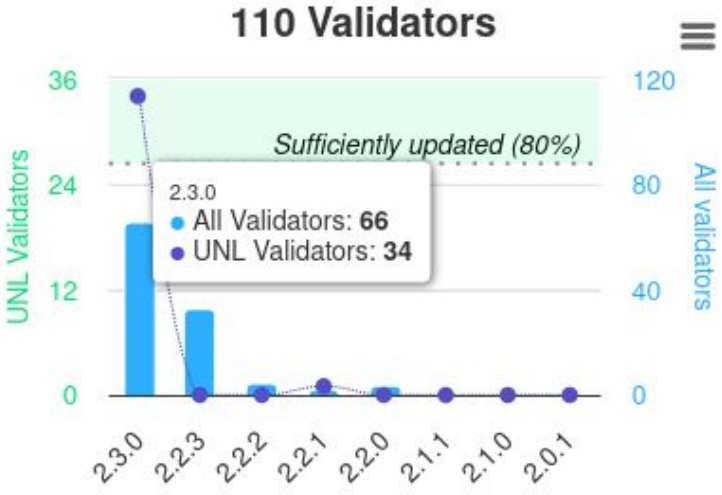
- In-progress reference implementation based on the SPIN model
- Replication of the attacker scenario



Discussion: so what?

- The Ripple paper went unaddressed outside of the academic community? WHY?
- In practice, Ripple is *highly centralized* w/ one main UNL

(via xrpscan.com)



What is going on!?

- Does anyone actually *use* Ripple as a service? No lol.
- Ripple (the company) only made **583k** in fees last year
- But, Ripple raked in **250mil** in investment
- ... and spent **100mil** fighting the SEC in court
- r/ripple and r/xrp is all speculation lmao
- And of course, Ripple (the company) owns 50% of XRP

What is going on pt 2

According to Forbes and an SEC filing, Ripple makes most of their money essentially laundering XRP through an Asian subsidiary

Is Ripple a scam?

Yes.

Q&A?

Biblio

[1] B. Chase and E. MacBrough, “Analysis of the XRP Ledger Consensus Protocol,” Feb. 20, 2018, arXiv: arXiv:1802.07242. doi: 10.48550/arXiv.1802.07242.

[2] I. Amores-Sesar, C. Cachin, and J. Mićić, “Security Analysis of Ripple Consensus,” Nov. 30, 2020, arXiv: arXiv:2011.14816. Accessed: Nov. 18, 2024. [Online]. Available: http://arxiv.org/abs/2011.14816

[3] B. Chase and E. MacBrough, “Analysis of the XRP Ledger Consensus Protocol,” Feb. 20, 2018, arXiv: arXiv:1802.07242. doi: 10.48550/arXiv.1802.07242.