

Towards the Formalization of the XRP Ledger Consensus Protocol

*Lara Mauri*¹, *Stelvio Cimato*¹, *Ernesto Damiani*^{1,2}

¹ *Computer Science Department, Università degli Studi di Milano, Milan, Italy*

² *EBTIC - Khalifa University, Abu Dhabi, U.A.E.*

3rd Distributed Ledger Technology Workshop (DLT 2020) – Ancona – February 4th, 2020

Reference

L. Mauri, S. Cimato, E. Damiani

“A Formal Approach for the Analysis of the XRP Ledger Consensus Protocol”

To be published in

Proceedings of the 6th International Conference on Information Systems Security and Privacy, ICISSP 2020, Valletta, Malta, February 25-27, 2020

Current research gaps in DLT research

The majority of current research on Distributed Ledger Technology is focused on identifying improvements to the challenges and limitations in blockchain protocols

- Wasted resources
- Latency
- Size and bandwidth
- Usability
- Versioning, hard forks, multiple chains
- Privacy
- ...



An emerging field that needs further research is the study of the **fundamental mechanisms** and **security properties** of the structure underlying blockchain-based systems

The need for a formal approach

Motivations (1/2)

Detailed analyses and formalizations of existing DL protocols are crucial to

- prove the correctness of the algorithms
- gain confidence that they achieve their goals
- identify their vulnerabilities

The need for a formal approach

Motivations (2/2)

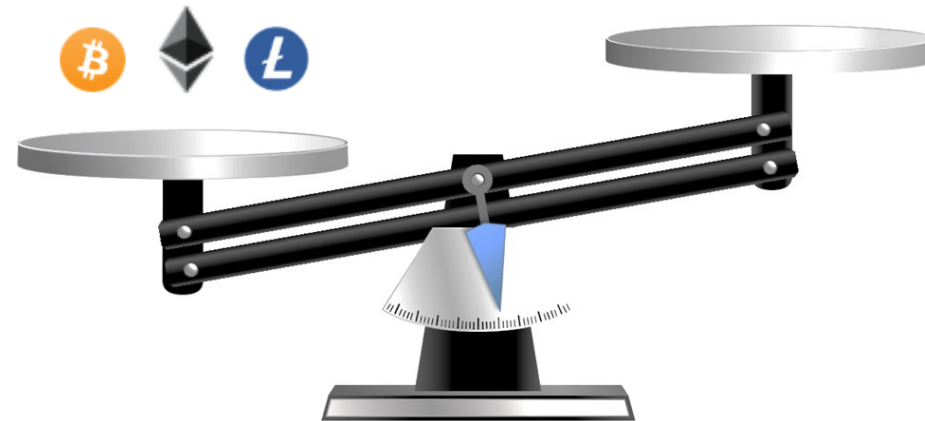
The behavior of permissionless protocols has been rigorously formalized in a number of recent works

Very little work has been devoted to the formalization of protocols consistent with the permissioned setting






Permissionless



Permissioned



XRP Ledger

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	 Bitcoin	\$171.501.601.624	\$9.425,39	\$29.759.440.589	18.195.712 BTC	0,97%	
2	 Ethereum	\$20.929.053.582	\$191,07	\$13.696.266.207	109.533.384 ETH	5,30%	
3	 XRP	\$11.109.251.241	\$0,254300	\$2.189.301.802	43.685.558.183 XRP *	6,54%	

[02/02/2020] Source: <https://coinmarketcap.com/>

XRP Ledger (originally called Ripple) is the third-largest DL network by market capitalization after Bitcoin and Ethereum

XRP Ledger at a glance

Key features

No need for a process of mining to verify transactions



XRP Ledger Consensus Protocol (XRP LCP)

XRP Ledger at a glance

Key features

No need for a process of mining to verify transactions



XRP Ledger Consensus Protocol (XRP LCP)

Based on the idea of subjective trust assumptions



Unique Node List (UNL)

XRP Ledger at a glance

Key features

No need for a process of mining to verify transactions



XRP Ledger Consensus Protocol (XRP LCP)

Based on the idea of subjective trust assumptions



Unique Node List (UNL)

Convergence implies the continuous update of the positions taken by the validators



Sharing of proposals

Issues

The XRP LCP is often described in a vague and not very clear way...

Why is it so difficult to have a clear understanding of how the XRP LCP works?

Issues

The XRP LCP is often described in a vague and not very clear way...

Why is it so difficult to have a clear understanding of how the XRP LCP works?

- The original white paper is deprecated
- Available documentation is restricted to the developer portal and a recent analysis provided by the creators of Ripple themselves
- The only existing peer reviewed analysis was conducted on the original white paper and showed that some specifications were flawed

Goals of our work

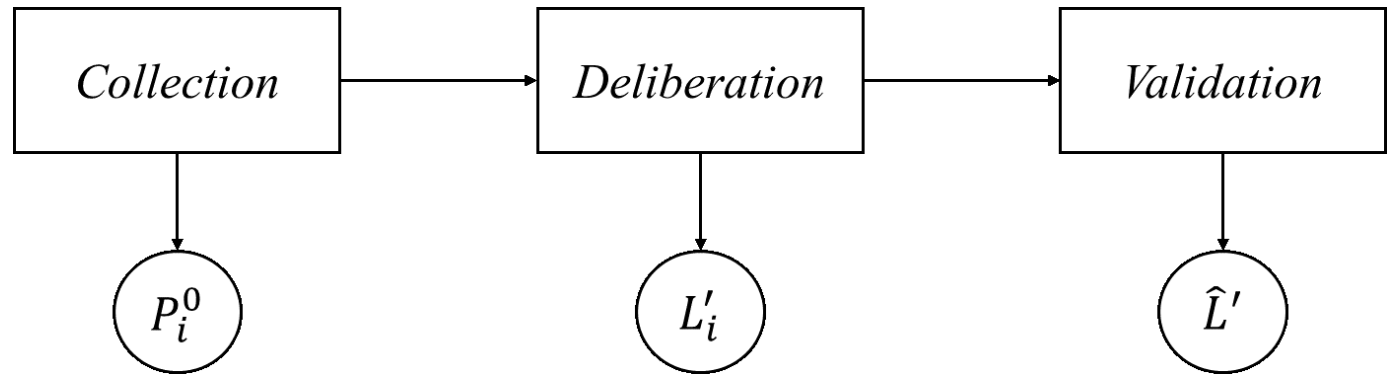
- In-depth description of the XRP LCP for every step
 - by means of a set-theoretic notation and mathematical formulas
- Accurate view of its current security guarantees in terms of safety and liveness
 - their correlation with other protocol components can be leveraged to increase either safety or liveness

Method:

- Direct analysis of the source code
- Careful investigation of all existing documentation relating to XRP Ledger

A look to our approach

N_v	The set of validators
i	A validator in the network
UNL_i	i 's Unique Node List
n_i	The size of UNL_i
tx	A single transaction
T	A set of transactions
T_Q	The set of queued transactions
\tilde{T}_I	The set of new transactions
q_c	The consensus quorum
q_v	The validation quorum
\tilde{L}_i	i 's open ledger
\tilde{L}_i^c	i 's closed ledger
L_i'	i 's last closed ledger
\hat{L}	The last fully validated ledger
P_i	i 's proposal of transactions
D_i	i 's set of disputed transactions
σ_i	i 's validation



Output of each phase from the perspective of a single validator i

$$P_i^0 = \{tx : tx \in T, T \in \tilde{L}_i^c\}$$

$$L_i' = \hat{L} \cup \{tx \in P_i^r : v(P_i^r) \geq q_c\}$$

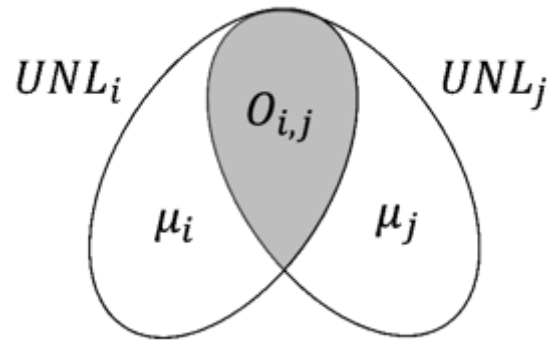
$$\hat{L}' = L_x' : (x = i \vee x \in UNL_i) \wedge (|\Sigma_{L_x'}| \geq q_v)$$

Security properties

Safety: If an honest node fully validates a ledger L , then all honest nodes cannot fully validate a contradictory ledger $L' \neq L$

Liveness: If an honest node broadcasts a valid proposal P to all honest nodes, then P will eventually be accepted by all nodes and included in a fully validated ledger

How to guarantee more safety or liveness (1/3)



$$n_i = |UNL_i|$$
$$n_j = |UNL_j|$$

$$O_{i,j} > \frac{n_j}{2} + n_i - q_v + t_{i,j}$$

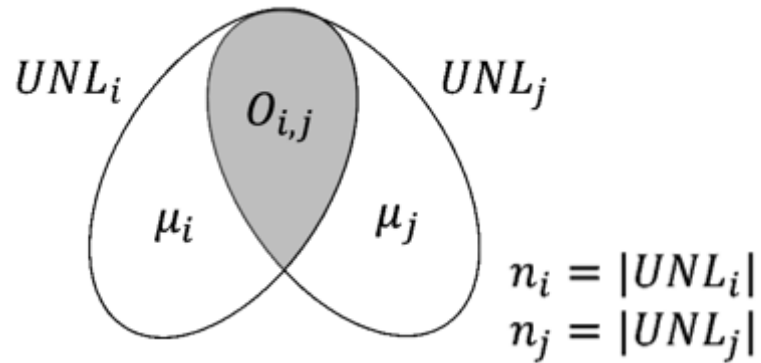
$$q_v > \frac{3n_i}{4} + \frac{\mu_i}{4} + \frac{\mu_j}{4}$$

- Safety fault tolerance $t_s < -\frac{n_i}{2} - \frac{\mu_i}{2} - \frac{\mu_j}{2} + q_v$
- Liveness fault tolerance $t_l < n_i - q_v$

A consensus protocol providing results that can be relied upon is preferable: $t_s \geq n_i - q_v$

Safety and liveness tolerances can vary according to the assumptions made on the UNLs overlapping size, the validation quorum and the tolerated Byzantine nodes

How to guarantee more safety or liveness (2/3)



Unique UNL

Overlapping UNLs

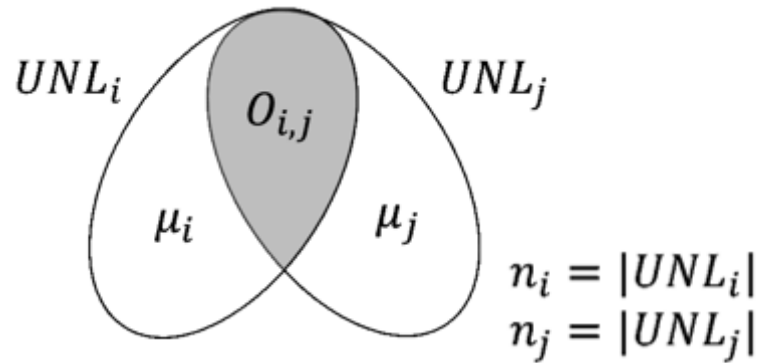
$$O_{i,j} > \frac{n_j}{2} + n_i - q_v + t_{i,j}$$

$$q_v > \frac{3n_i}{4} + \frac{\mu_i}{4} + \frac{\mu_j}{4}$$

$$t_s < -\frac{n_i}{2} - \frac{\mu_i}{2} - \frac{\mu_j}{2} + q_v$$

$$t_l < n_i - q_v$$

How to guarantee more safety or liveness (3/3)



$$O_{i,j} > \frac{n_j}{2} + n_i - q_v + t_{i,j}$$

$$q_v > \frac{3n_i}{4} + \frac{\mu_i}{4} + \frac{\mu_j}{4}$$

$$t_s < -\frac{n_i}{2} - \frac{\mu_i}{2} - \frac{\mu_j}{2} + q_v$$

$$t_l < n_i - q_v$$

Unique UNL

$$n_i = n_j = n$$

$$\mu_i = \mu_j = 0$$

$$q_v > (3/4)n$$

$$t_s < (1/4)n$$

$$t_l < (1/4)n$$

$$q_v = 0.8n$$

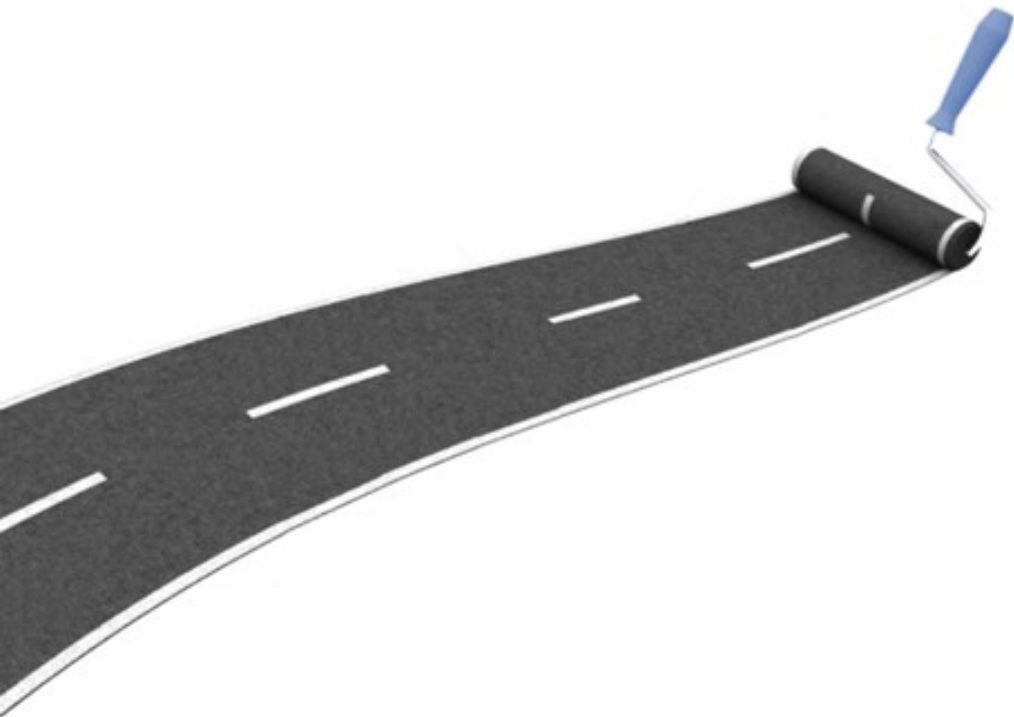
as required by the current
XRP LCP specification

$$t_s < (3/10)n$$

$$t_l < (1/5)n$$

Concluding remarks

We have taken the first steps towards the complete analysis of the XRP Ledger Consensus Protocol



Next steps...

- additional security properties
- extended formalism
- automated verification tools
- different models of computation



THANKS

LARA MAURI

lara.mauri@unimi.it