On the way to Omniledger: adding transaction batching and ByzcoinX to skipchains

Raphaël Dunant

DEDIS lab

Supervisor: Linus Gasser

Responsible: Prof. Bryan Ford

Omniledger improvements

- Block state storing
- Transaction Batching
- Improve decentralised Signing

Summary

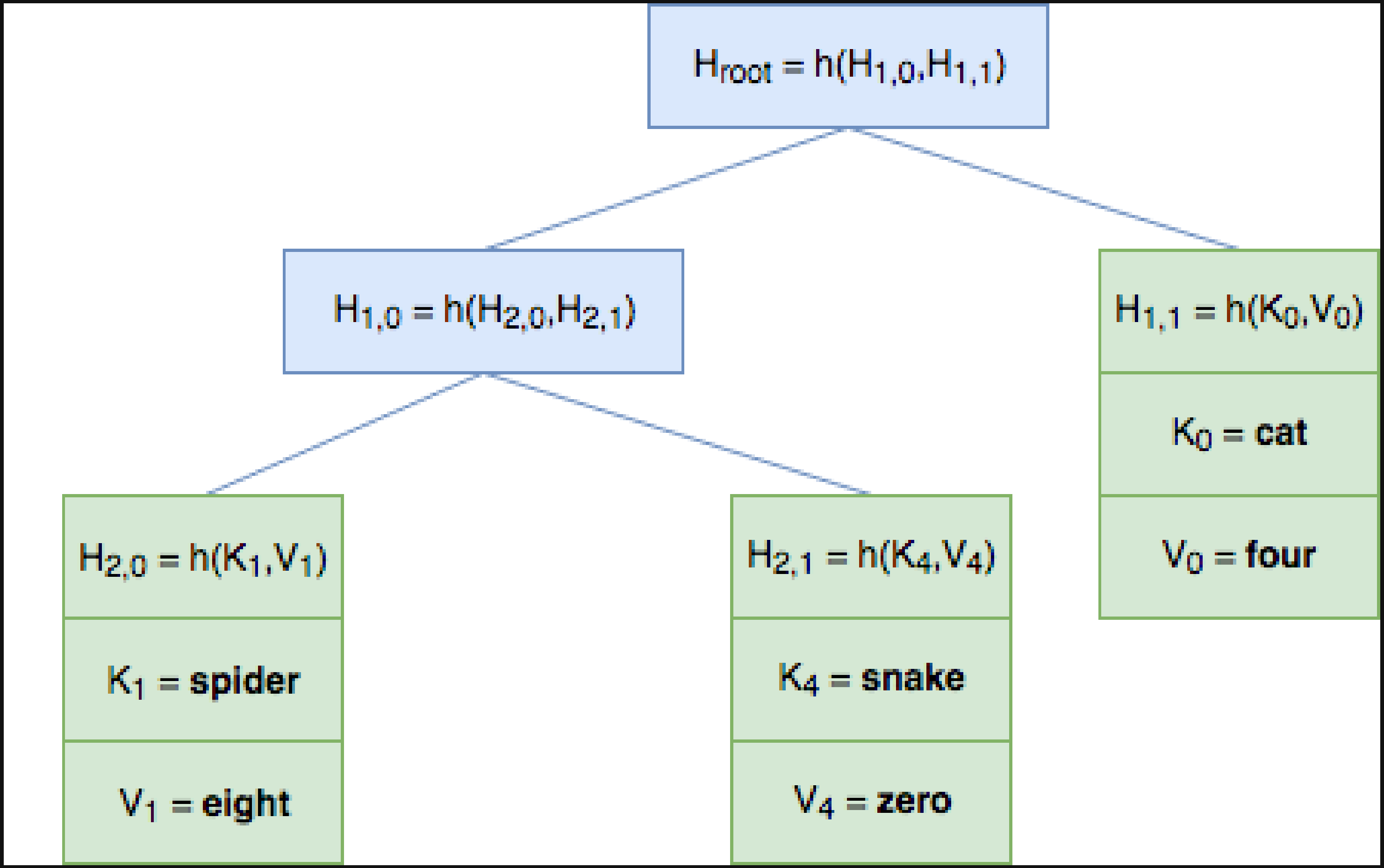
- Introduction (done)
- Collections
- ByzcoinX Quick Answers
- Simulation results
- Conclusion (results, lessons learned, etc.)

DEDIS

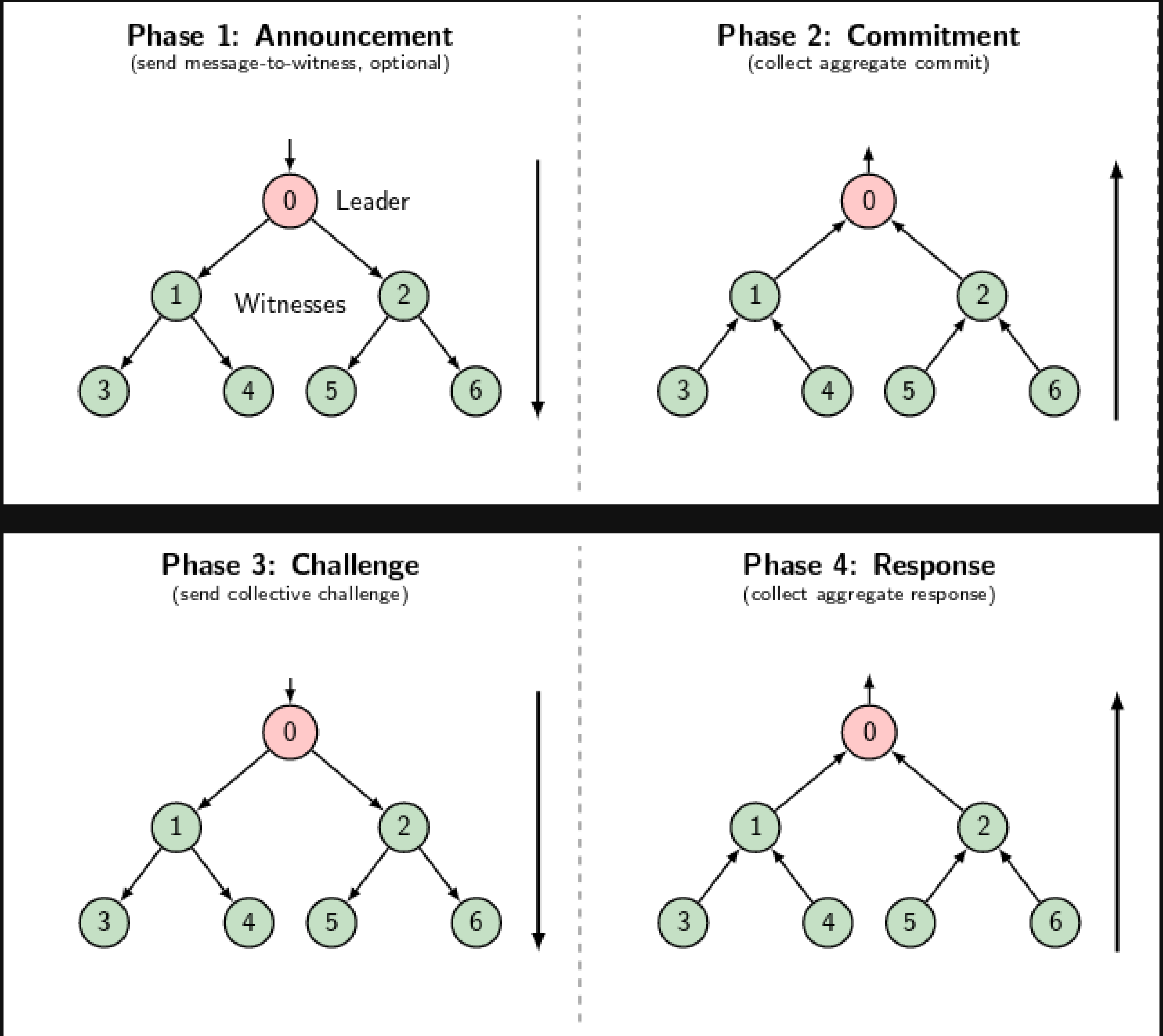
EPFL

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Patricia Merkle Tree



ByzcoinX: Decentralized Witness Cosigning



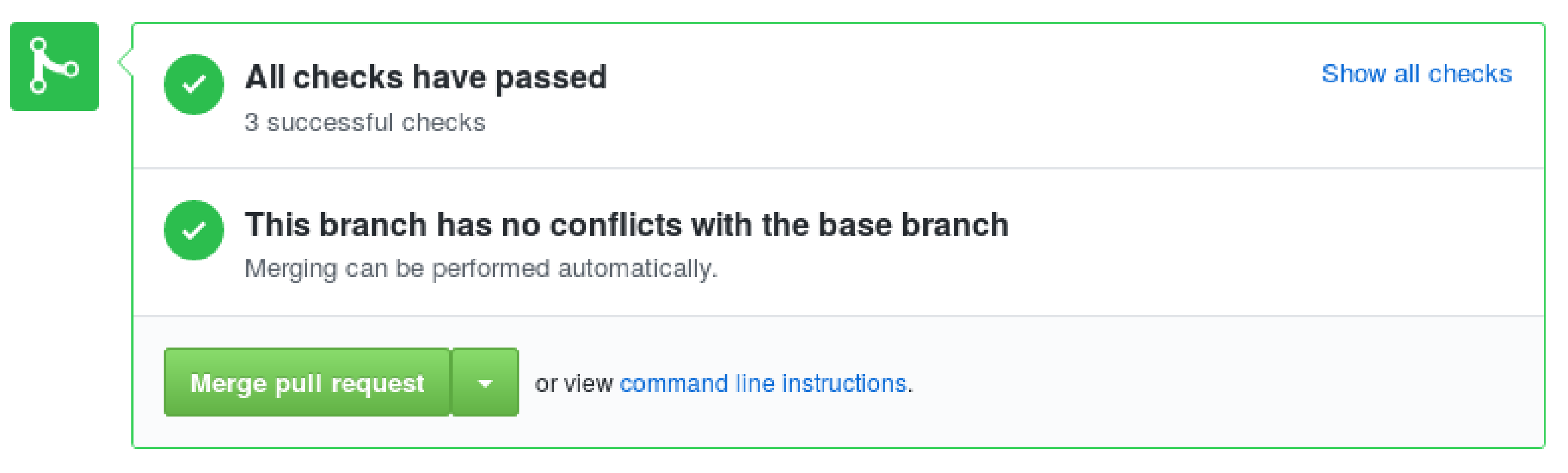
Objectives

- Understand and Document complete collection library

- Improve drastically running time of ByzcoinX

- Have nice, documented, tested code

Collections Code Cleaning



All checks have passed

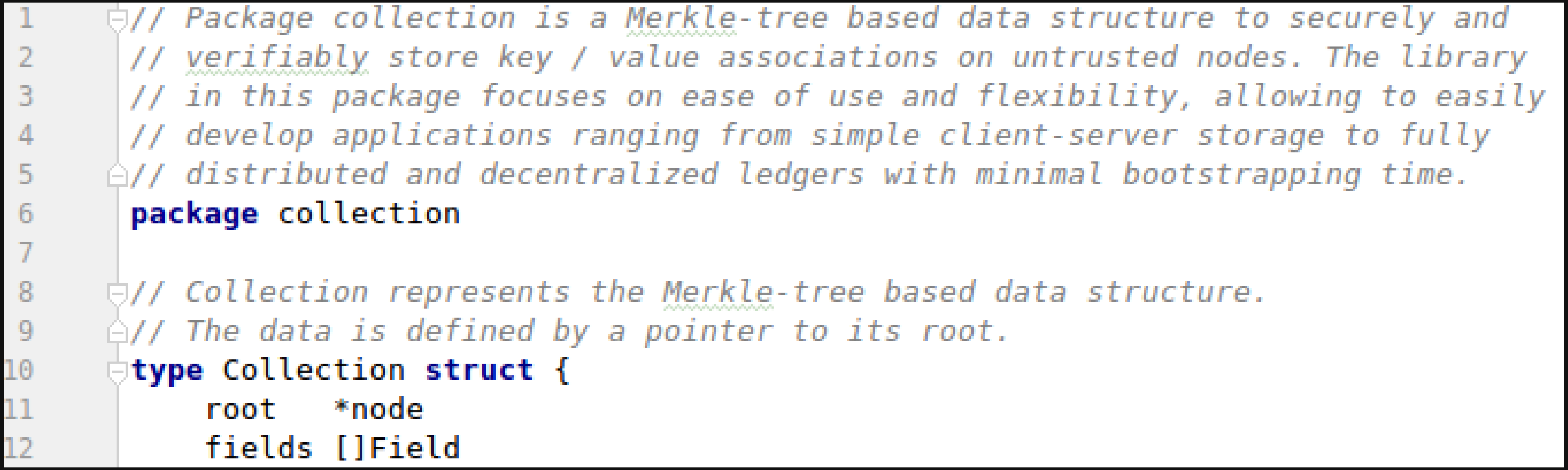
3 successful checks

Show all checks

This branch has no conflicts with the base branch

Merging can be performed automatically.

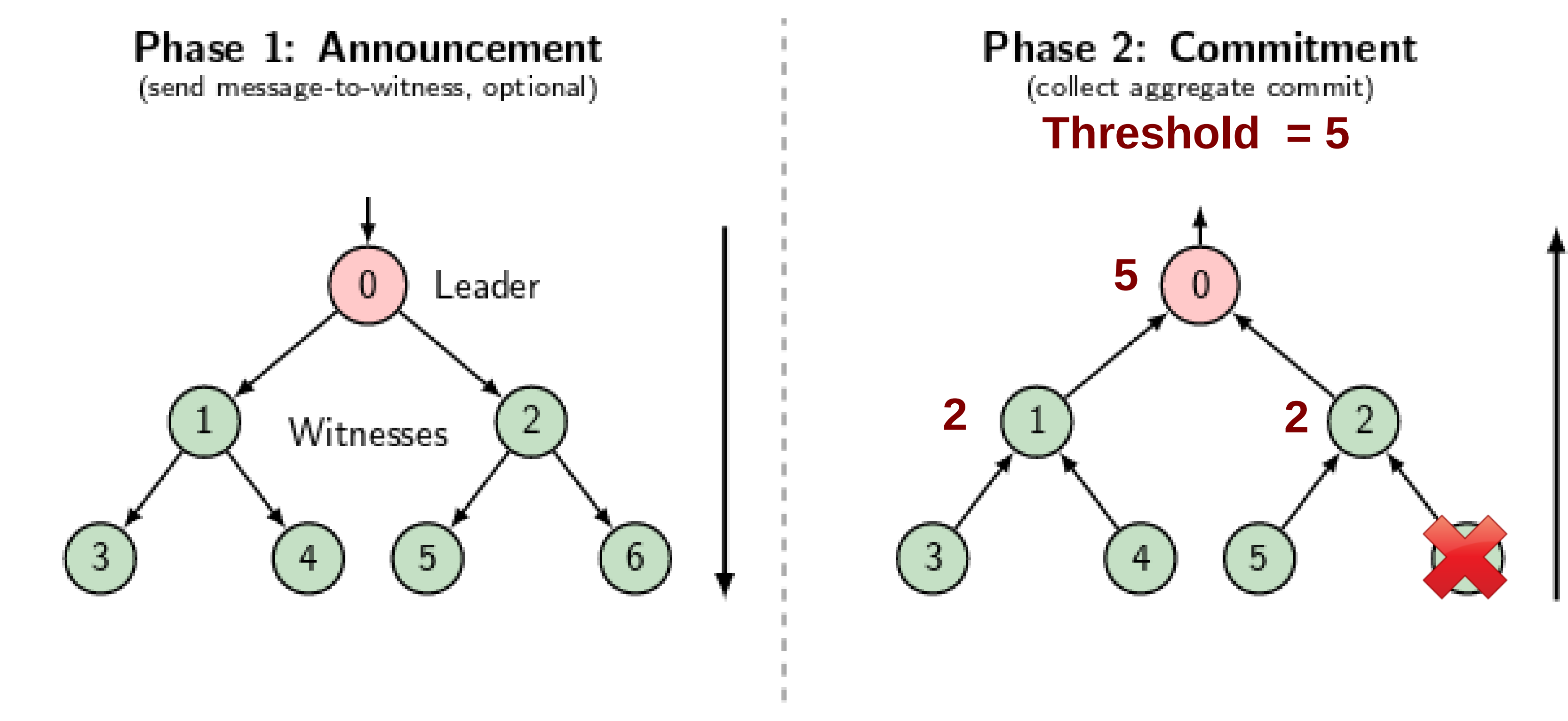
or view command line instructions.



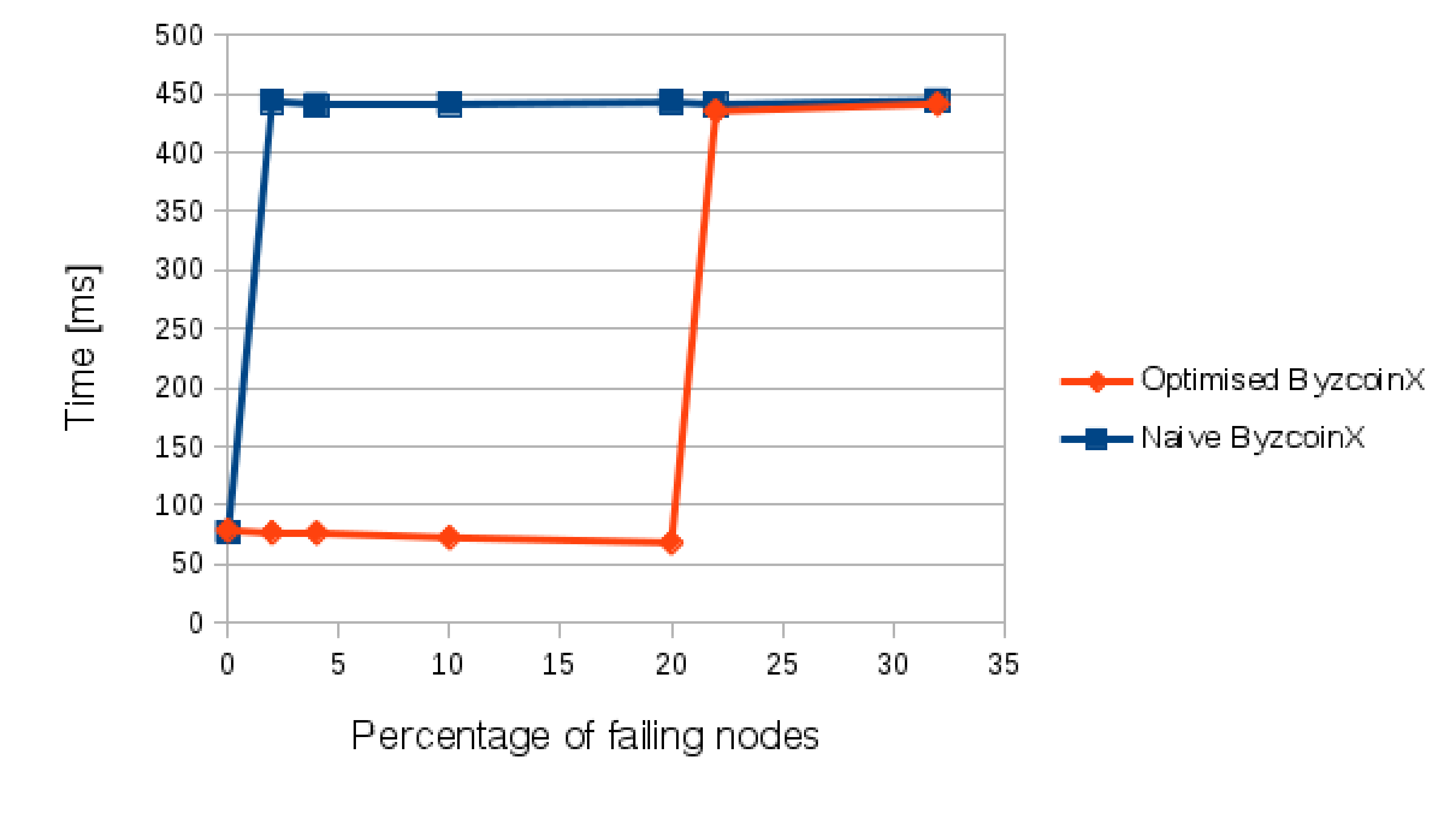
```go
// Package collection is a Merkle-tree based data structure to securely and
// verifiably store key / value associations on untrusted nodes. The library
// in this package focuses on ease of use and flexibility, allowing to easily
// develop applications ranging from simple client-server storage to fully
// distributed and decentralized ledgers with minimal bootstrapping time.
package collection

// Collection represents the Merkle-tree based data structure.
// The data is defined by a pointer to its root.
type Collection struct {
    root   *node
    fields []Field
```

ByzcoinX Quick Answers



Simulation results



- 50 Nodes, 6 Subleaders, Default Leafs Timeout: 417ms, average of 10 tries
- Threshold: ⌈ 2/3 · 50 ⌉ = 34
- 2.9 GHz, 4 Core, 4MB cache, 8GB DDR3-1600 RAM

Future work

- Collections
  - Store on hard drive
  - Handle transactions conflicts more finely
- ByzCoinX
  - Add backward Compatibility
  - Rework Timeouts
  - Improve security
- Add more unit tests

Conclusion

- Complete, working and reusable collections code
- Quick ByzcoinX performances
- Will be used in production
- Scalable and tested
- Can still get better
- Personal improvement