The Problem of:
Hybrid BFT Protocols

Cyrus Jian Bonyadi

University of Maryland, Baltimore County

Overview

Why would we want a hybrid protocol?

- Some protocols work better in some circumstances than others.
- Some protocols do not work in circumstances where they would be useful.

What aspects of a BFT protocol can we mix?

- Adversarial assumptions (public to private)
- Game theoretical assumptions (permissionless to permissioned)
- Timing assumptions (partially synchronous to asynchronous)

Hybrid Synchrony BFT Protocols

Review of Synchrony

Synchronous

- Works if messages deliver perfectly

Partially Synchronous

- Works even in latent environments

Asynchronous

- Works even when faced with network scheduling adversaries, which naturally appear in TOR and large WAN VPNs [3]

Motivating Theorem and Options for Implementation

Very Trivial Theorem

> If a partially synchronous protocol becomes asynchronous after some time *t*, then the given protocol is asynchronous.

Options

1. Make a new asynchronous protocol that can be functionally partially synchronous.
2. Allow a partially synchronous protocol to operate until asynchrony is required, which then securely switches to an asynchronous protocol.

BFT Consensus Protocols

PBFT (1999, Partially Synchronous)

Quorum-based Protocols (2008, Partially Synchronous)

BFT-SMaRt (2013, Partially Synchronous)

BChain (2014, Partially Synchronous)

HoneyBadgerBFT (2016, Asynchronous)

BEAT (2018, Asynchronous)

Existing Mechanics for Protocol Switching

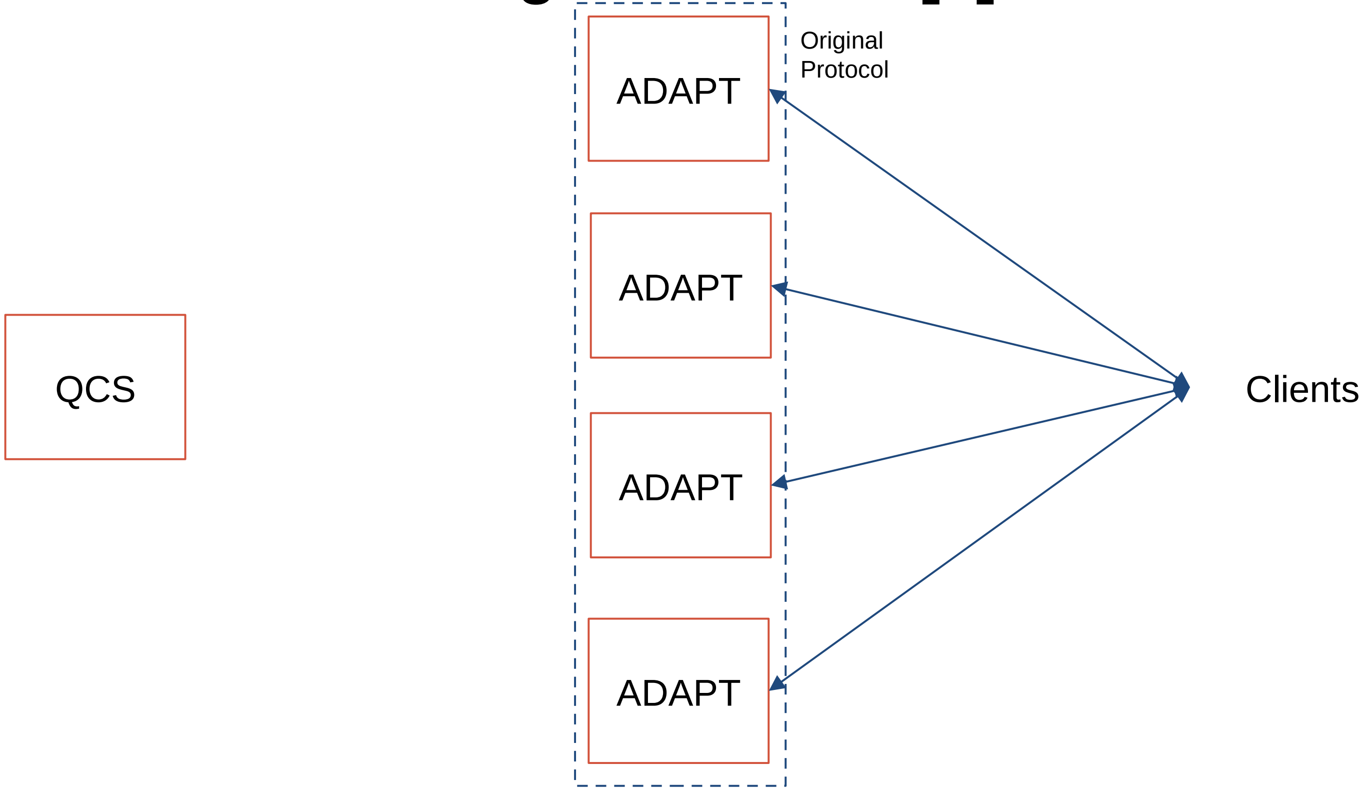
Abstract [2]

Switching protocol for partially synchronous BFT protocols, which enables switching after the current protocol fails, which is primarily determined by some timing mechanism

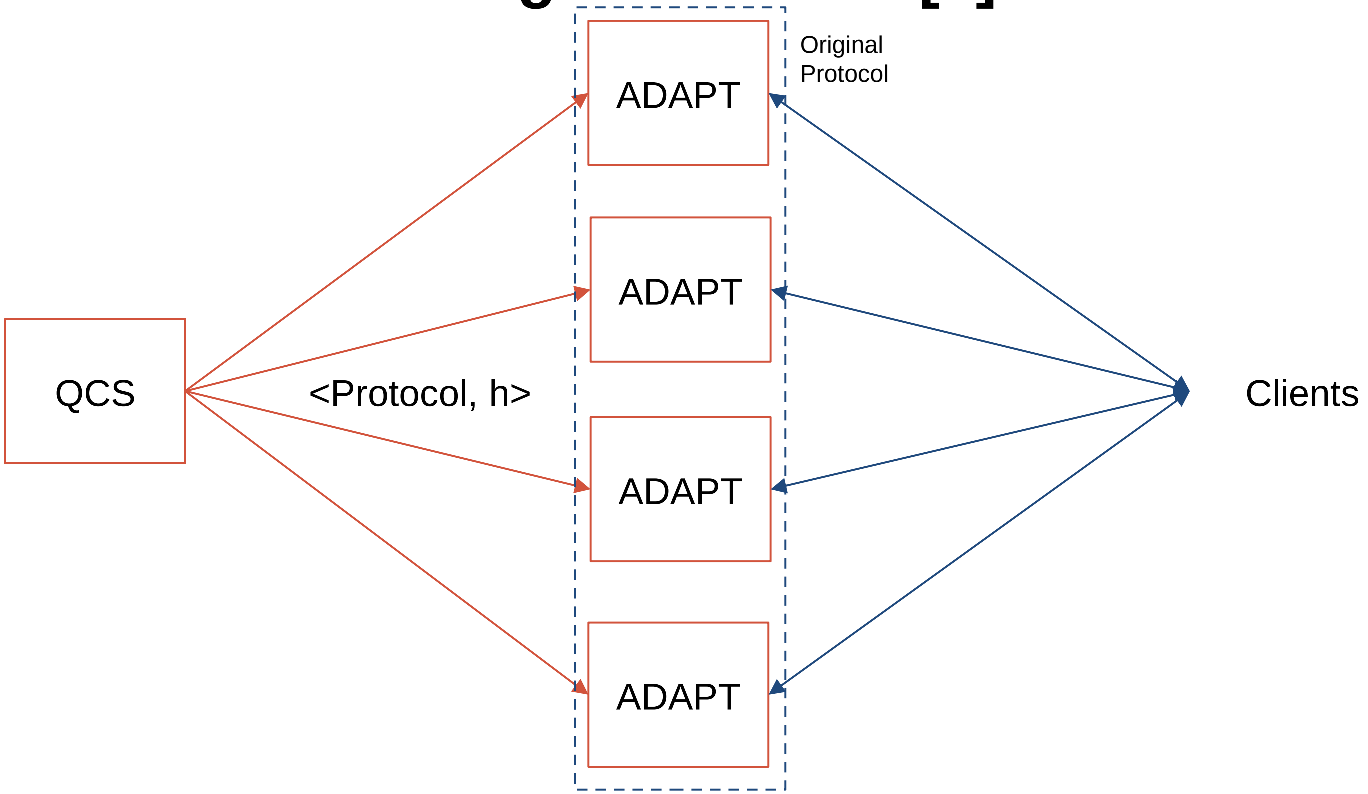
ADAPT [1]

Modification of Abstract which allows protocols to be switched upon potential performance improvements.

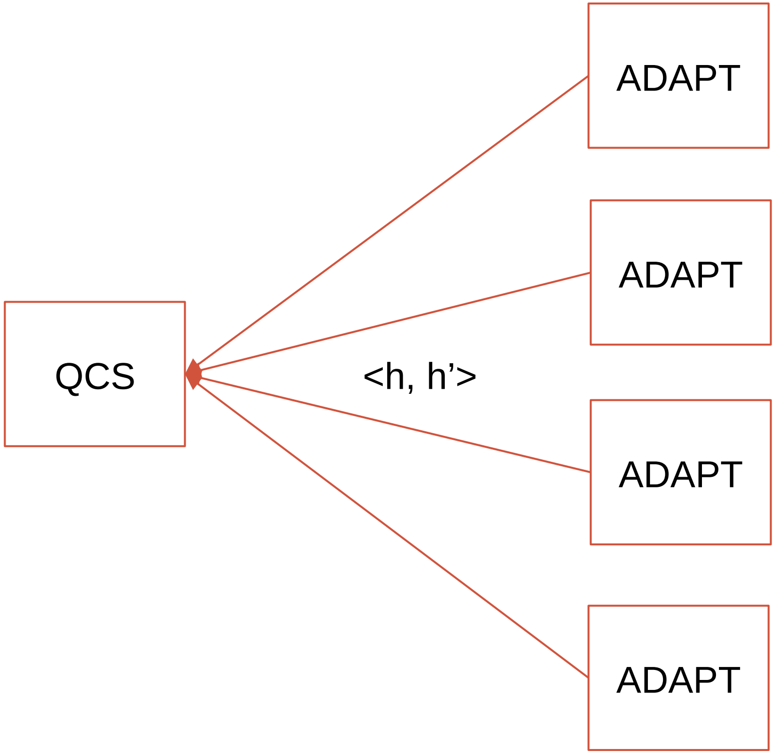
Basic Secure Switching Mechanics [1]



Basic Secure Switching Mechanics [1]



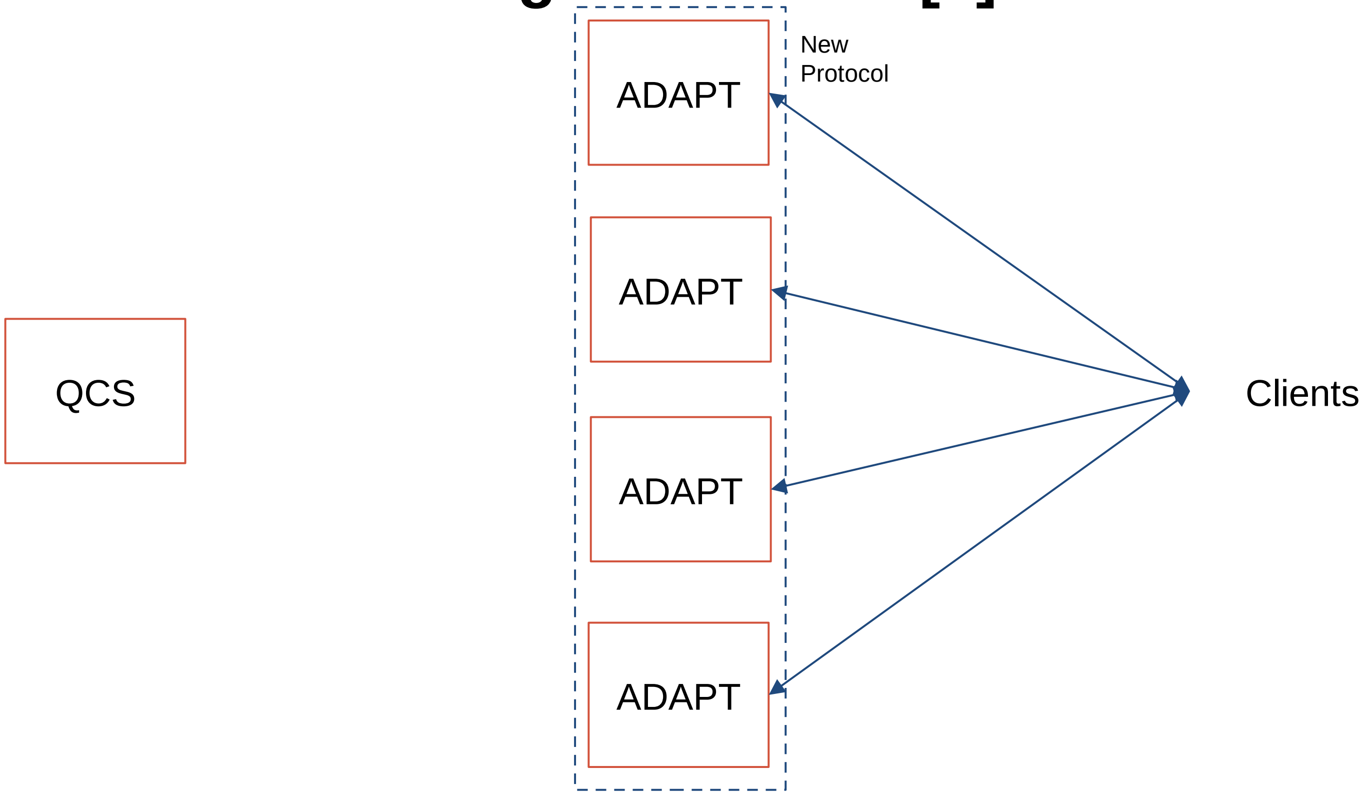
Basic Secure Switching Mechanics [1]



Cancel current transactions and initialize them under the new protocol.

Clients

Basic Secure Switching Mechanics [1]



Conclusions about Problems in Asynchrony

The existing protocols exist in partially synchronous environments and are thus trivially susceptible to network scheduling adversaries.

> The QCS can be too good, and we may consistently wish to switch protocols before any transactions finish.

There are likely other adversarial conditions beyond the network scheduling adversary that are not yet considered.

Future Work

FLEX: a switching protocol for using mixed synchrony protocols interchangeably.

- Security Proof (In Progress)
- Algorithm Development (In Progress)
- Implementation
- Experimentation

References

[1] Jean-Paul Bahsoun, Rachid Guerraoui, and Ali Shoker. 2015. Making BFT Protocols Really Adaptive. In Proceedings of the 2015 IEEE International Parallel and Distributed Processing Symposium (IPDPS '15). IEEE Computer Society, Washington, DC, USA, 904-913. DOI=http://dx.doi.org/10.1109/IPDPS.2015.21

[2] Rachid Guerraoui, Nikola Knežević, Vivien Quéma, and Marko Vukolić. 2010. The next 700 BFT protocols. In Proceedings of the 5th European conference on Computer systems (EuroSys '10). ACM, New York, NY, USA, 363-376. DOI=http://dx.doi.org/10.1145/1755913.1755950

[3] Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi, and Dawn Song. 2016. The Honey Badger of BFT Protocols. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). ACM, New York, NY, USA, 31-42. DOI: https://doi.org/10.1145/2976749.2978399

Discussion of Problems Found in Other Types of Hybrid BFT Protocols