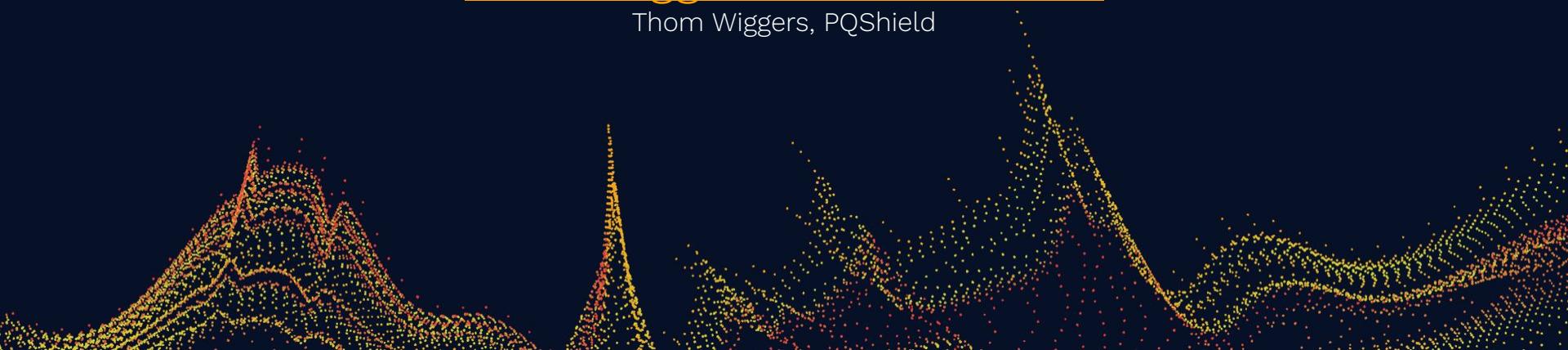


# Hash-based Signatures: State and Backup Management

[draft-wiggers-hbs-state-00](#)

Thom Wiggers, PQShield

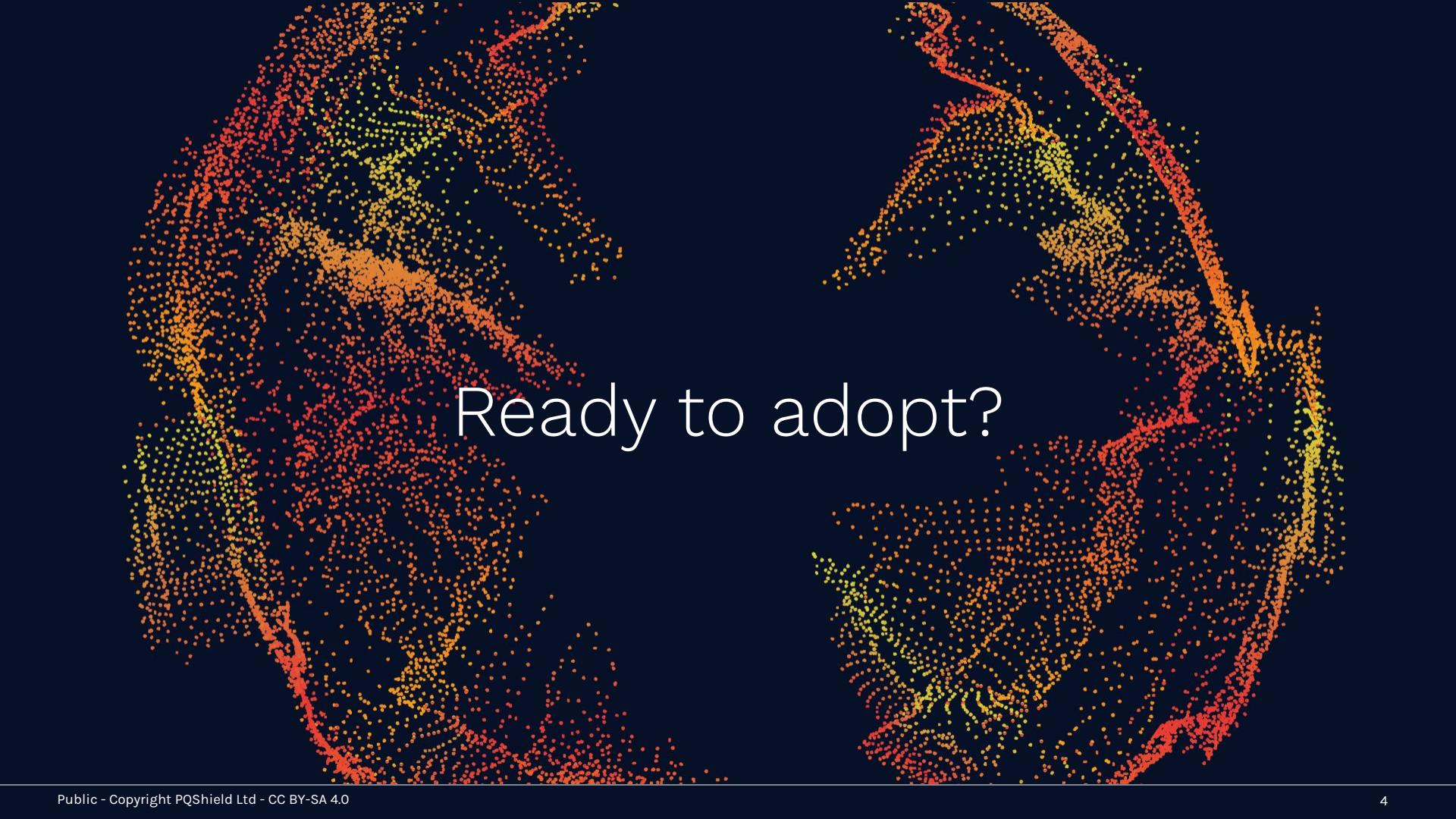


# Guidance for state management (repeat from IETF119)

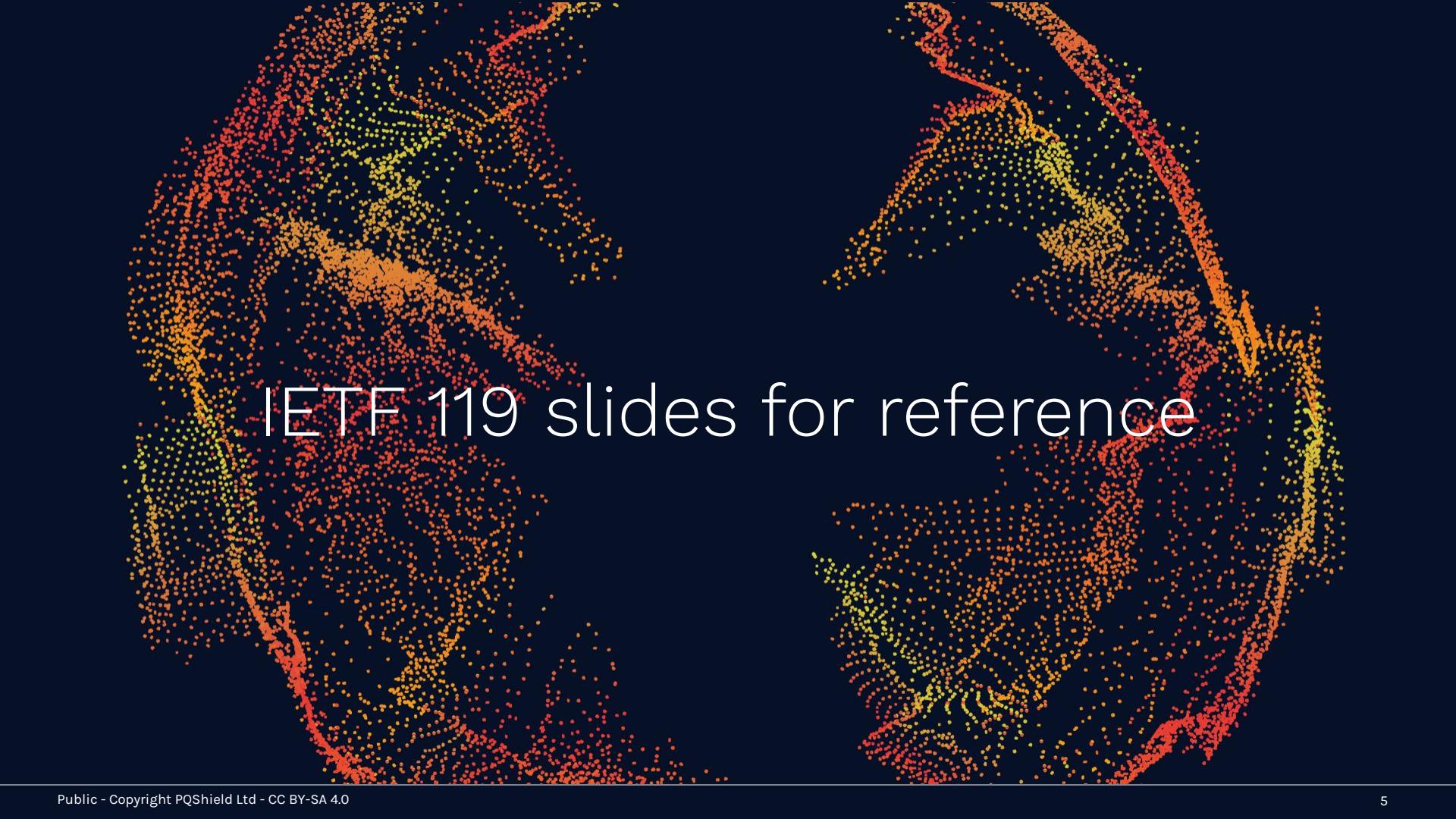
- Dealing with state is hard
- Dealing with state is scary
- “Thou **MUST NOT** use a key more than once” – but how?
  - You **SHOULD** use ~~SPHINCS~~<sup>+</sup> SLH-DSA if possible
  - You **SHOULD** probably use an HSM
- How do you reliably deploy S-HBS schemes?
- And what about backups?

# Discussion on mailing list

- People seem to agree this is worth documenting
- Possible additions to the current document:
  - When should S-HBS be considered in the first place? ([Issue #2](#))
  - More approaches?



Ready to adopt?

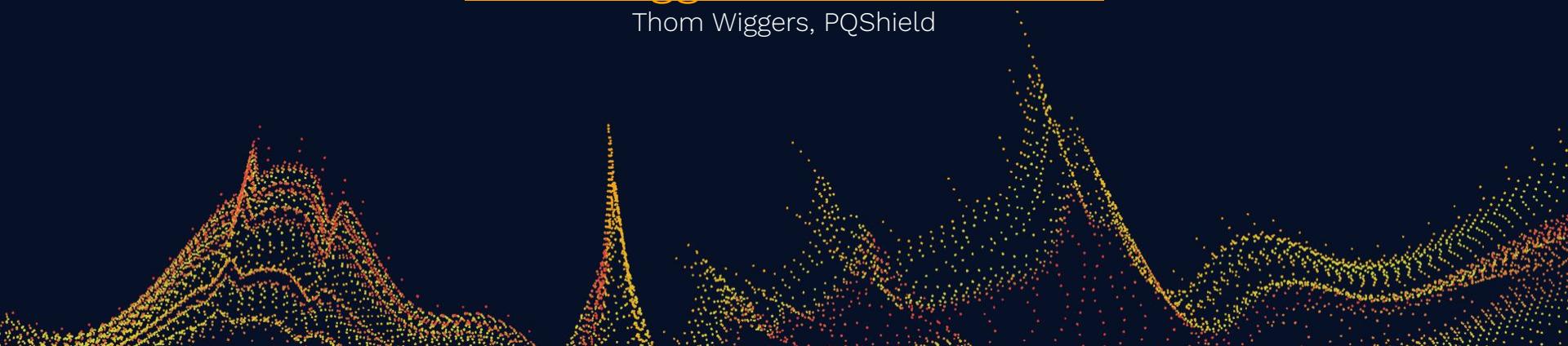
The background of the slide features a dark blue gradient with a subtle, abstract pattern of colored dots. These dots are concentrated in specific regions, creating a map-like effect. The colors used are primarily red, orange, yellow, and green, which are characteristic of a choropleth map. The overall aesthetic is modern and minimalist.

IETF 119 slides for reference

# Hash-based Signatures: State and Backup Management

[draft-wiggers-hbs-state-00](#)

Thom Wiggers, PQShield



# Joint work

Many thanks to Kaveh Bashiri, Stefan Kölbl, Jim Goodman, Stavros Kousidis, and Bruno Coulliard.

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: 22 August 2024

T. Wiggers  
PQShield  
K. Bashiri  
BSI  
S. Kölbl  
Google  
J. Goodman  
Crypto4A Technologies  
S. Kousidis  
BSI

19 February 2024

Hash-based Signatures: State and Backup Management  
[draft-wiggers-hbs-state-00](#)

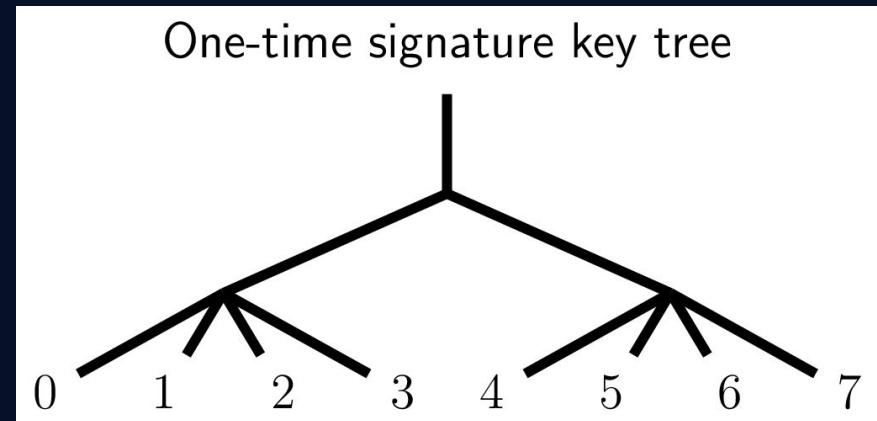
## Abstract

Stateful Hash-Based Signature Schemes (S-HBS) such as LMS, HSS, XMSS and XMSS<sup>MT</sup> combine Merkle trees with One-Time Signatures (OTS) to provide signatures that are resistant against attacks using large-scale quantum computers. Unlike conventional stateless digital signature schemes, S-HBS have a state to keep track of which OTS keys have been used, as double-signing with the same OTS key allows forgeries.

This document provides guidance and documents security considerations for the operational and technical aspects of deploying systems that rely on S-HBS. Management of the state of the S-HBS, including any handling of redundant key material, is a sensitive topic, and we discuss some approaches to handle the associated challenges. We also describe the challenges that need to be resolved before certain approaches should be considered.

# Stateful hash-based signatures

- A list of one-time use signature keys
- Key reuse  $\Rightarrow$  game over
- Keeping track of which signatures have been consumed is super important.
  - We call this the state



# Guidance for state management

- Dealing with state is hard
- Dealing with state is scary
- “Thou **MUST NOT** use a key more than once” – but how?
  - You **SHOULD** use ~~SPHINCS~~<sup>+</sup> SLH-DSA if possible
  - You **SHOULD** probably use an HSM
- How do you reliably deploy S-HBS schemes?
- And what about backups?

# Contents of the draft

- Terminology
- Requirements
- Operational considerations
- Some potential solutions for state management and backups
- Evaluation of certain approaches for specific setups
- Both within and beyond SP800-208's key export ban

## Example: “Can’t we just use time?”

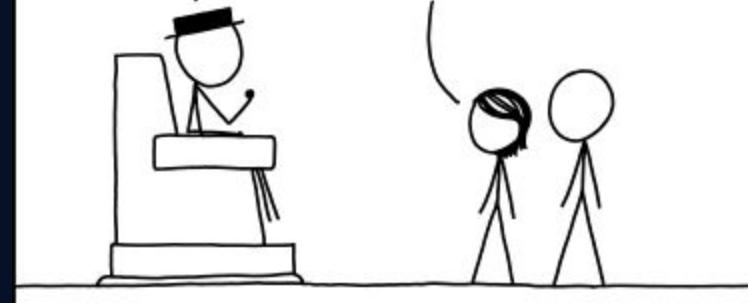
- Divide time into epochs
- Only allow one signature per epoch
- Clock makes sure that you know which states are okay?
- Profit?

... THEN, AFTER OUR DRONES TAKE CONTROL OF THE CITIES, WE WILL DETONATE THE DEVICES. CALIFORNIA WILL BREAK OFF FROM THE MAINLAND AND DRIFT OUT TO SEA!

HOW FAR OUT TO SEA? WILL IT PUT ANY OF THE CITIES IN THE UTC-9 TIME ZONE?

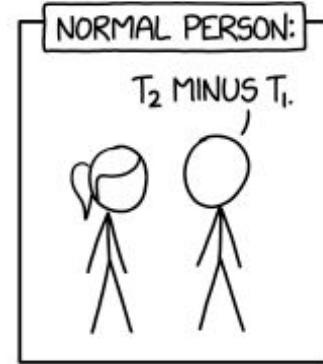
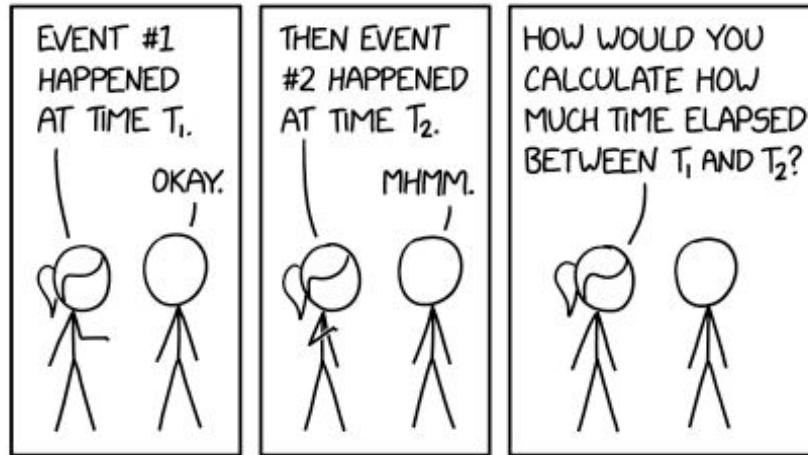
WHAT? I DON'T KNOW.

ONE REQUEST: CAN WE MAKE SURE THIS DOESN'T HAPPEN DURING THE DAYLIGHT SAVING CHANGEOVER?



YOU CAN TELL WHEN SOMEONE'S BEEN A PROGRAMMER FOR A WHILE BECAUSE THEY DEVELOP A DEEP-SEATED FEAR OF TIME ZONE PROBLEMS.

<https://xkcd.com/1883/>



<https://xkcd.com/2867/>

# Bloomberg

• Live TV

Markets ▾

Economics

Industries

Tech

Politics

Businessweek

Opinion

Technology

## Leap Year Software Glitch Closes Fuel Pumps Across New Zealand



By [Matthew Brockett](#)



29 februari 2024 at 00:46 CET



Save

*“Our HSM vendor told us to please not roll out any configuration changes tomorrow”*

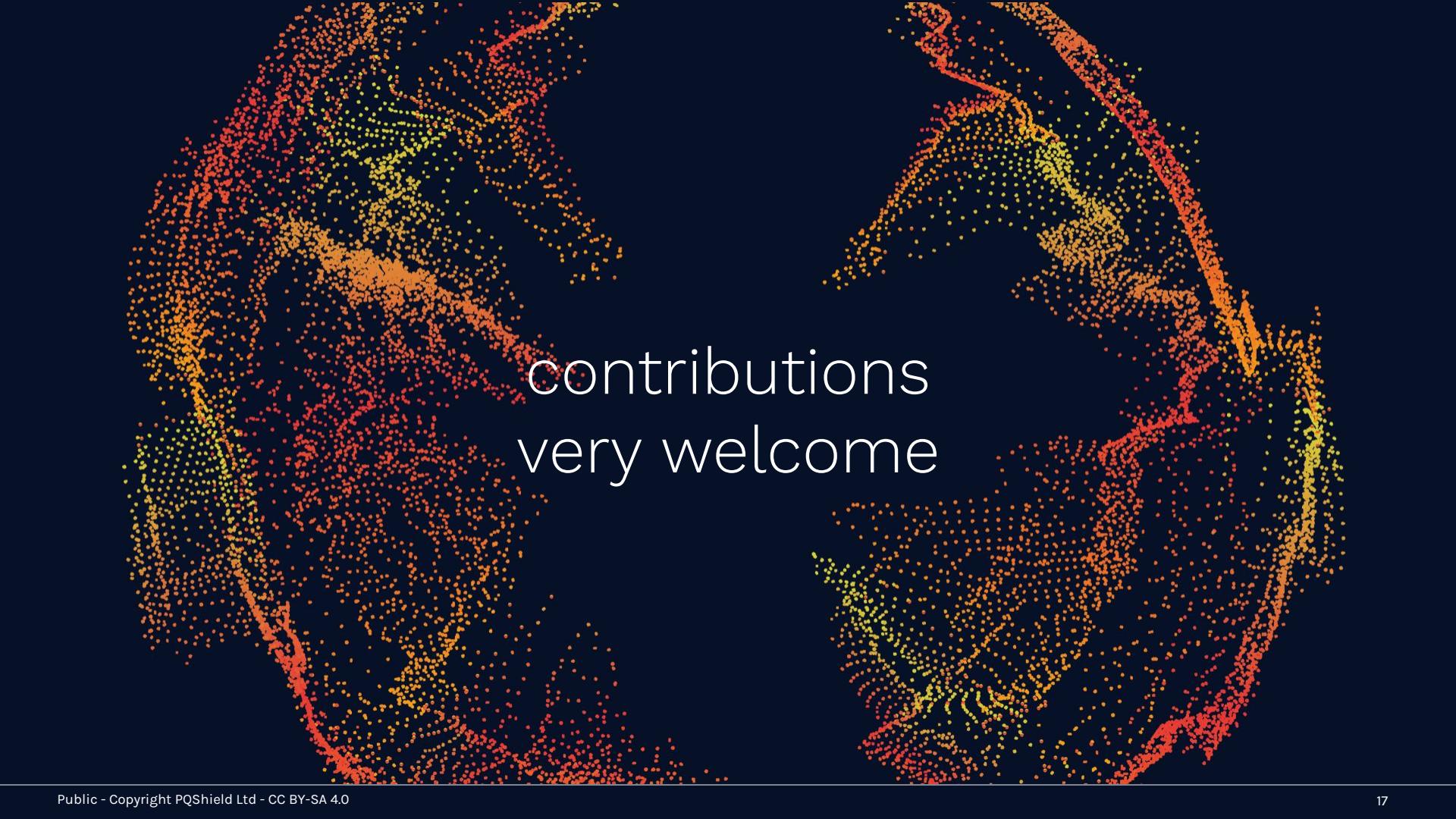
-- My friend who works at a major bank,  
**28 february 2024**

## 5.8. Time-based State Management

[...]

Any time-based approach has a very strict reliance on accurate time-keeping and synchronization of clocks. In particular, we identify that at least the following engineering-related challenges need to be considered:

[16 BCP14 keywords follow]



contributions  
very welcome