The Best of Both Worlds: Byzantine Agreement Protocols for (but not limited to) Chickens

Julian Loss and Tal Moran
Setting:

- Old Mc Donald’s Crypto Farm
- Farm and pen are separated by road
Classical Problem From Crypto/Distributed Computing:

- Chickens trying to decide whether to cross street
- Problem: Birds of a feather flock together!
- How can they ensure that all of them cross at once?
Solution: Run Protocol for Byzantine Agreement!

- Agreement ensures that all chickens cross street at once
- Chickens are connected via gossiping network
Problem: What if some of the chickens are actually malicious Ducks?

- Ducks may try to prevent agreement!
- Protocol must be secure in the presence of duck-minority!
Two Types of Protocols

- Let the number of chickens be \( n \).
- Use synchronized clocks: Can tolerate up to \( n/2 \) ducks by proceeding in lockstep fashion.

Problem: Chickens don’t have watches. Must use sunrise to synchronize instead!

Synchronous rounds take a whole day!
Two Types of Protocols

- Let the number of chickens be $n$.
- Without synchronization: Can tolerate up to $n/3$ ducks.
- Chickens can agree very fast...
- but can tolerate only $n/3$ ducks :(
QUESTION:

Is there a protocol which is both fast AND resilient?

Is it optimal?
Check out our paper on EPRINT!

• Combining Asynchronous and Synchronous Byzantine Agreement: The Best of Both Worlds

• Julian Loss and Tal Moran

• URL: ia.cr/2018/235
Open Question:

Why did the chickens try to cross the road in the first place?
THANKS FOR LISTENING!