



AZTEC Protocol

Tom Waite and Paul Berg



Outline

- 1) Introduction
- 2) What is the AZTEC Protocol
- 3) Our experiences of working at a blockchain startup
- 4) How to follow AZTEC



Intro



We are engineers from AZTEC

Tom



- Imperial Physics MSci (graduated 2018)
- Tried out all sorts at uni:
 - MBDA Missile Systems
 - Robotics research in South Korea
 - BCG
 - Undergrad research assistant at Imperial's Crypto Centre
 - Machine learning MSci project
- Joined AZTEC 6 months ago



We are engineers from AZTEC

Paul



- Software engineer for ~5 years
- Doing Ethereum for ~2 years
- Youngest alumni of Entrepreneur First (19 yo)
- Co-Founder of ChronosProtocol
- Joined AZTEC 3 months ago



**What is
AZTEC?**



Public blockchains have many benefits, but privacy was a problem

Public blockchains have a raft of benefits:

- 1) Single verifiable source of truth
- 2) Counterparty risk significantly reduced - transactions settled atomically by smart contracts
- 3) Reduced fees

But there's a problem!

These blockchains are public - confidential activity can not take place on them

.... OR CAN IT?



AZTEC is a privacy protocol for the Ethereum public blockchain

We use a branch of cryptography called zero-knowledge proofs

- Allows us to validate the logic of transactions, without revealing the confidential values involved. Checkout a confidential transaction on mainnet here:

```
https://etherscan.io/tx/0xdd879c3181a40c80d738320be2fd2f9d919412537d07d252db8ec974343ff0c1
```

The protocol is:

- Extremely efficient, 800-900k gas for one private transaction
- Interoperable with Ethereum based assets

AZTEC will allow financial services to be provided with privacy on public Ethereum



**Our
experiences**



Tom

- 1) Everything is difficult - especially elliptic curve cryptography! 
- 2) Rate of learning in a startup is fast ☐ ☐
- 3) Physics is pretty good prep for problem solving!  ☐



Paul

- 1) Feels like consciously walking towards fire 🔥
- 2) Constantly learning new things 📖
- 3) Must figure a lot of things on your own ☐
- 4) Nevertheless, fun ☐

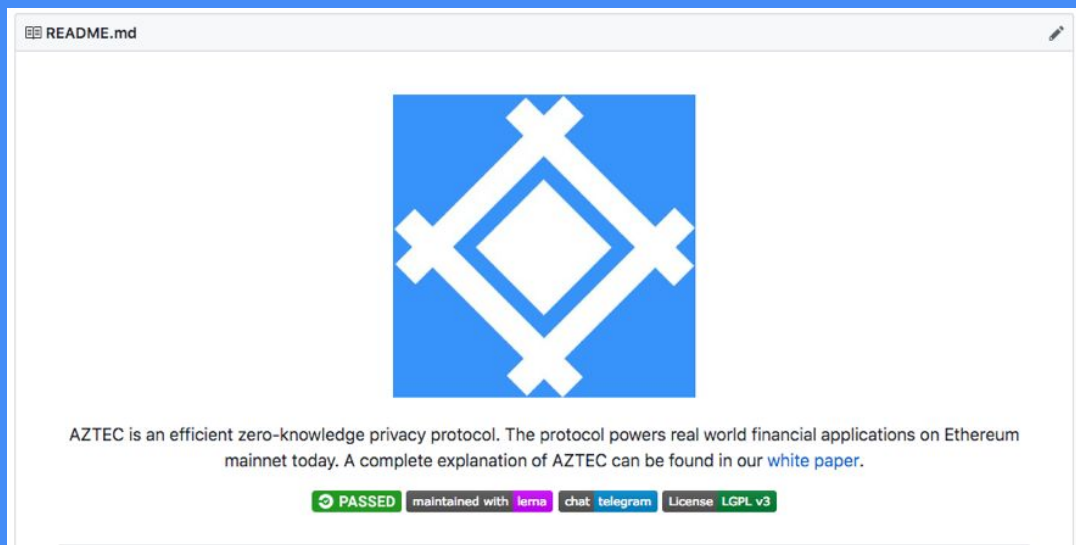


**How to follow
our progress**



Check out AZTEC!

- **Website:** <https://www.aztecprotocol.com/>
- **Github:** <https://github.com/AztecProtocol>
- **Twitter:** <https://twitter.com/aztecprotocol>





Find us on Twitter

@aztecprotocol

@PaulRBerg

@tom_waite_





Questions?