Jaysonchain

Decentralised Encrypted Messaging with Additional Guarantees

The Problem:

Problems with non-private Blockchains:
Hiding transactions with encryption is not trivial
Hard to prove properties about transactions without making them public to everyone
E.g. Private proof of origin and private proof of path is difficult

Problems with private Blockchains:
Centralized, not everyone can run a node

The Solution:

Decentralised Encrypted Messaging
- All messages are only visible to the receivers account
- Third parties don't know if two accounts are communicating

+ Accounts Have Most Recently Read State
- Accounts can decide to publish which message they have read last

+ Multi-Party Visibility and Proof of Path
- Information about messages can be made visible to trusted parties besides the sender and reciever
- Accounts can prove that forwarded messages haven't been tampered with

One Example:

Mercedes cars have a sensor in their car for measuring the mileage. Alice wants to let Bob know what her mileage is (maybe she wants to sell him the car). Bob trusts mercedes, but doesn't trust Alice. Alice can read her mileage anytime, but Mercedes requires a payment for proving the mileage to third parties. Alice doesn't want Mercedes to know that the proof is for Bob. No one else should know about any of this. Jaysonchain not only makes this possible, but also automates the process for Mercedes. No Mercedes employee is involved.

Other use cases:

Messenger, Quality Control, Supply Chain, Rental System, Auditing...

//TODO:

Proof of Destination:
The sender can prove to a third party that the reciever has indeed received a message

Complete the API for handling all the offchain logic

Exploring even crazier use-cases