



# CloakCoin Cloak System

Whitepaper FAQ

This document comprises a number of Frequently Asked Questions that have come up in forums and messages to the CloakCoin development team.

**1. Aren't you afraid people will be questioning the mixer function, like who's behind the accounts, etc.?**

People will always question everything in crypto world. This is ok and part of the peer review process.

**2. Does cloak have its own exchange? Or does it work through existing exchanges?**

Cloak does not have its own exchange, the system will work through existing exchanges.

**3. Doesn't this system add centralization on the exchanges? What if governments or forces compromise the exchange(s)?**

The system is decoupled from the exchanges. The exchanges are acting as "dead drops" in the transaction flow.

**4. Won't there be a lot of transaction latency as transactions hop from exchange to exchange?**

No, because transactions don't hop from exchange to exchange.

**5. Will this be hard to use? Will the user have to go to a bunch of different places to cloak?**

It will be easy for the user to cloak through a button click in the wallet.

#### **6. Who decides what sites will be the mixers?**

At the moment, the Cloak development team will be operating the mixer engines.

#### **7. What does "anonymous via exchange" mean, how does it work?**

The exchanges act as dead drops in the system. Elsewhere on the network there are "listening post" nodes, the transaction fulfilment nodes. These peers watch the block chain for activity to the dead drop addresses, and proceed based on their observation. This design also insulates the cloak environment from exchanges failing etc. as it is not dependent on any one exchange.

#### **8. Wouldn't a fully decentralized, trustless system baked into the network protocol be more of the "holy grail"?**

It would be the Holy Grail, but also has a high level of complexity. Nobody has successfully implemented such a system yet without running into technical roadblocks and network problems. Cloak is instead starting with an achievable design that can be put into live operation rapidly and then be evolved over time to reach the grail.

#### **9. What about the API nodes, don't these add centralization and a failure point?**

The API nodes will be load-balanced and DDOS protected.

#### **10. Who operates the API nodes? Who chooses who gets to be an API node?**

The API nodes will be operated by the Cloak development team.

#### **11. What if a hostile government spies on the API node?**

Because there is decoupling in the system, they could only obtain the 2nd piece of the puzzle (dead drop and recipient addresses).

#### **12. How is this different from existing mixing services and "stealth" mechanisms from other coins?**

In the Cloak system there is no direct correlation from source address to destination address. The source, dead drops, and listening posts are decoupled from each other. The environment only knows about dead drops and recipients for transaction forwarding. Other mixing services log the entire transaction chain, making them vulnerable to compromise.

**13. Can you provide a detailed technical design of the system evolution, with specifics on the cryptography and technology?**

We have provided the whitepaper/brief write up and diagrams for Phase 1 of the Cloak System. We are not yet comfortable releasing detailed technical information on Phase 2 (fully decentralized architecture) as it would give away our competitive advantage. Phase 1 will quickly provide a usable system in live production, and will also generate great scenario/use case data that can inform the design of Phase 2. The Phase 2 implementation is a much longer development cycle. Suffice it to say that there is open source technology out there that can be leveraged to achieve the Phase 2 goal, but nobody has put the pieces together yet.