Buttcoin: A Purr-to-Purr Electronic Cat System

Saratoshi Nagamoto
saratoshin@gmx.com
www.buttcoin.fun

Abstract. A purely peer-to-peer version of electronic cats would allow online pets to be sent directly from one party to another without going through an event planner. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-booking. We propose a solution to the double-booking problem using a purr-to-purr network. The network pawprints the cat actions by hashing them into an ongoing tail of hash-based proof-of-fur, forming a record that cannot be changed without redoing the proof-of-fur. The longest tail not only serves as a proof of the species of cat witnessed, but proof that it came from the largest pool of CPU (central purring unit) power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace cat-nappers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-fur tail as proof of what happened while they were gone.

1. Introduction

Cat image sharing on the Internet has come to rely almost exclusively on technology companies serving as trusted third parties to provide web services. While the system works well enough for most transactions, it still suffers from the inherent weakness of the trust based model. Completely non-reversible cat actions are not really possible, since technology companies cannot avoid mediating disputes. The cost of mediation increases cat action costs, limiting the minimum practical cat action size and cutting off the possibility for small casual cat actions, and there is a broader cost in the loss of ability to make non-reversible cat actions for non-reversible cuteness. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their cat owners, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical cats, but no mechanism exists to make payments over a cat channel without a trusted party.

What is needed is an electronic cat system based on cryptographic proof instead of trust, allowing any two willing parties to share cat actions directly with each other without the need for a trusted third party. Cat actions that are computationally impractical to reverse would protect sellers from fraud, and routine hooded crow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-booking problem using a purr-to-purr distributed timestamp server to generate computational proof of the chronological order of cat actions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.