[

swap

2406×1170 269 KB

](https://ethresear.ch/uploads/default/original/2X/1/1a16e6226aa2be5cb205ad5403265fc964e53a51.png)

From Escrow protocols for cryptocurrencies: How to buy physical goods using Bitcoin

I am most interested in 5.4 Escrow Encrypt-and-Swap and 6.3 Group Encrypt-and-Swap. I have dropped away from cryptography for a bit, but this certainly comes up at an economic layer as well. I have no evidence aside from some hacker texts regarding infeasibility of sMPC that have colored the way I think about cryptography since.

Ring signatures and Threshold Signatures are practically dual, but seem an enduring theoretical key. What is the state of the art for automatic PKI signing? Proxy wallets of some sort? I am interested in how to make as much automated as possible, especially on the cryptographic layer.

Transitive trust is the issue that glares as the main problem within this direction of thinking and one of the gravest concerns within the space. I have 3 ETH in my Kovan wallet, so I am ready to rumble.

Have any of you read this paper? I am trying to figure out a bit of a knowledge share, how to discuss fruitfully with the knowledge base this community has.