What is Bitcoin?

Bitcoin is the *world’s first successful cryptocurrency* whose value is not endorsed by a central institution or bank, but by the perception of its users.

An identity in Bitcoin consists of a public-private key pair, the public key is transformed into a Bitcoin address to ‘receive’ bitcoins and the private key is needed to ‘authorise’ payments by providing a digital signature. This is a *pseudonymous identity* – as the public-private key pair are not linked to any real-world identity.

In fact, users are recommended to create a new Bitcoin address for every new payment to help preserve their privacy. This is necessary as all Bitcoin transactions are sent over the peer to peer network and ultimately stored on the Blockchain – the decentralised public ledger that is stored by most users of the network.

As all transactions are public knowledge – an eavesdropper can link a user’s balance or payment destinations if their Bitcoin address is used more than once.

Attacking the Payment Protocol

I have discovered two attacks on Bitcoin’s Payment Protocol:

- **The Silkroad Trader Attack** allows a customer to undetectably route a payment to an illicit trader via an honest merchant

- **The Marketplace Trader** Attack allows a malicious trader to trick a customer into completing a purchase by claiming all payments are handled by a “trusted” merchant – ultimately leading to the customer loosing their bitcoins.

The Silkroad Trader is an attack on the Payment Protocol as the merchant lacks authenticated evidence that the refund address received during the protocol had in fact came from the customer.

The Marketplace Trader is an attack on both Payment Processor’s current refund policy as the refund address is sent using an external method of communication such as e-mail, which is not good enough to protect the customer.

We have proposed that the customer should **authenticate the refund address** by providing a digital signature for the Payment Message from the same address used to authorise the payment.

BIP70: Payment Protocol

The Payment Protocol is a community accepted standard and is supported by the two main Bitcoin Payment Processors Bitpay and Coinbase, who offer this service to **150,000+ merchants**.

1) The merchant sends the customer a Payment Request that is signed using their websites X.509 certificate’s private key.

2) The customer can check the merchant’s identity using before authorising the payment – which sends their transaction and a refund Bitcoin address to the merchant.

3) The merchant replies with an acknowledgement to state the transaction and refund address has been received.

Authenticated Key Exchange over Bitcoin

In the world of Bitcoin – the traditional methods for authenticated key exchange such as Public-Key Infrastructure (PKI) and Password-based Authenticated Key Exchange (PAKE) are not good enough to allow two pseudonymous users to set up a secure end to end communication channel as the former relies on an endorsed real-world identity and the latter relies on a pre-shared password.

Our attack on the Payment Protocol is the perfect example of why the traditional authentication methods are not satisfactory for cryptocurrencies as the payment information needs to be endorsed by the same pseudonymous user that authorised the payment.

We have proposed a new concept which we call **Bitcoin-Based Authenticated Key Exchange** that leverages information stored in the Blockchain to allow two pseudonymous users to authenticate and communicate securely.

This proposal also presents the first **post-payment protocol** for Bitcoin that allows the merchant to authenticate messages from the same pseudonymous user that authorised the payment.