JoinMarket

-or-

Finding a Risk-Free Rate for Bitcoin

Adlai Chandrasekhar
JoinMarket Contributor

Scaling Bitcoin 2016 - Milan

Chris Oldwood @chrisoldwood · Oct 1

When you're cooking with mushrooms is it possible to substitute one sort for any other because they're fungible?

9 16

Chris Oldwood @chrisoldwood · Oct 1

When you're cooking with mushrooms is it possible to substitute one sort for any other because they're fungible?

9 16 •••

“Once, however, money has been digitized, one of the services available for purchase can be the anonymous transfer of funds."

Eric Hughes, 1994-08-03

What is Privacy?

What is Privacy?

- Anonymity is always within a set

What is Privacy?

- Anonymity is always within a set
  - "Kid Sister" vs Government

What is Privacy?

- Anonymity is always within a set
- "Kid Sister" vs Government
- Hiding vs Deniability

Prior Art (2011 - 2014)

Prior Art (2011 - 2014)

- Users attempt to unlink Bitcoins using altcoins and centralized sites

Prior Art (2011 - 2014)

- Users attempt to unlink Bitcoins using altcoins and centralized sites
- Sites dedicated to unlinking, commonly known as "mixers" or "tumblers"

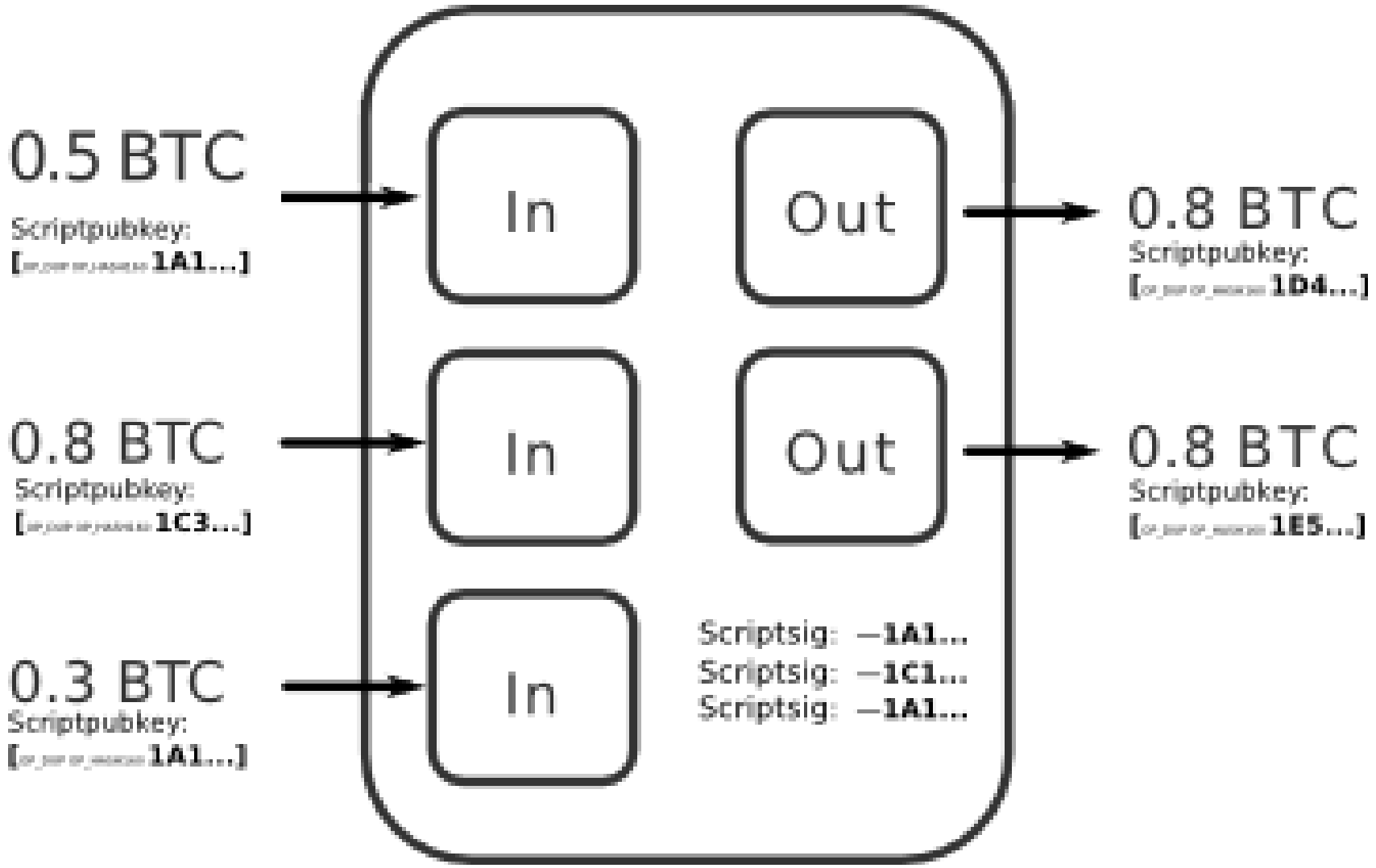
Prior Art (2011 - 2014)

- Users attempt to unlink Bitcoins using altcoins and centralized sites
- Sites dedicated to unlinking, commonly known as "mixers" or "tumblers"
- Greg Maxwell proposes CoinJoin and CoinSwap, (former gains limited traction, latter: **none**)

Prior Art (2011 - 2014)

- Users attempt to unlink Bitcoins using altcoins and centralized sites
- Sites dedicated to unlinking, commonly known as "mixers" or "tumblers"
- Greg Maxwell proposes CoinJoin and CoinSwap, (former gains limited traction, latter: **none**)
  - DarkWallet offers P2P CoinJoin but lacks consistent liquidity (users must wait)

The Simplest “Smart” Contract



JoinMarket Goals

JoinMarket Goals

- No counterparty risk

JoinMarket Goals

- No counterparty risk
- Weak / Granular Privacy

JoinMarket Goals

- No counterparty risk
- Weak / Granular Privacy
- Liquidity / High Availability

JoinMarket Goals

- No counterparty risk
- Weak / Granular Privacy
- Liquidity / High Availability
- Compatible with Bitcoin protocol

JoinMarket Goals

- No counterparty risk
- Weak / Granular Privacy
- Liquidity / High Availability
- Compatible with Bitcoin protocol
- "*Cypherpunks write code*"

JoinMarket’s Innovation

JoinMarket’s Innovation

Compensate participantion!

JoinMarket’s Innovation

Compensate participantion!

- Incentivize availability

JoinMarket’s Innovation

Compensate participantion!

- Incentivize availability
- Attract additional liquidity

JoinMarket Roles

Participant / "Maker"	Initiator / "Taker"

JoinMarket Roles

Participant / "Maker"	Initiator / "Taker"
Continuous Participation	Sporadic Participation

JoinMarket Roles

Participant / "Maker"	Initiator / "Taker"
Continuous Participation	Sporadic Participation
Merely signs provided TX	Coordinates and assembles TX

JoinMarket Roles

Participant / "Maker"	Initiator / "Taker"
Continuous Participation	Sporadic Participation
Merely signs provided TX	Coordinates and assembles TX
Provides liquidity, **earns fees**	Pays fees to consume liquidity

JoinMarket Roles

Participant / "Maker"	Initiator / "Taker"
Continuous Participation	Sporadic Participation
Merely signs provided TX	Coordinates and assembles TX
Provides liquidity, **earns fees**	Pays fees to consume liquidity
Slight Privacy Gain	Larger Privacy Gain

First JoinMarket Protocol

Participant / "Maker"	Initiator / "Taker"

First JoinMarket Protocol

Participant / "Maker"	Initiator / "Taker"
Advertise liquidity and rate (publicly)	

First JoinMarket Protocol

Participant / "Maker"	Initiator / "Taker"
Advertise liquidity and rate (publicly)	
	Send chosen offer, coinjoin amount, and encryption key

First JoinMarket Protocol

Participant / "Maker"	Initiator / "Taker"
Advertise liquidity and rate (publicly)	
	Send chosen offer, coinjoin amount, and encryption key
Reply with own encryption key	

Messages beyond this point are encrypted

First JoinMarket Protocol

Participant / "Maker"	Initiator / "Taker"
Advertise liquidity and rate (publicly)	
	Send chosen offer, coinjoin amount, and encryption key
Reply with own encryption key	

Messages beyond this point are encrypted

Send signature of encryption key using input utxo pubkey

First JoinMarket Protocol

Participant / "Maker"	Initiator / "Taker"
Advertise liquidity and rate (publicly)	
	Send chosen offer, coinjoin amount, and encryption key
Reply with own encryption key	

Messages beyond this point are encrypted

	Send signature of encryption key using input utxo pubkey
Send inputs, desired output and change addresses (all signed)	

First JoinMarket Protocol

Participant / "Maker"	Initiator / "Taker"
Advertise liquidity and rate (publicly)	
	Send chosen offer, coinjoin amount, and encryption key
Reply with own encryption key	

Messages beyond this point are encrypted

	Send signature of encryption key using input utxo pubkey
Send inputs, desired output and change addresses (all signed)	
	Construct transaction using each participant’s inputs and outputs

First JoinMarket Protocol

Participant / "Maker"	Initiator / "Taker"
Advertise liquidity and rate (publicly)	
	Send chosen offer, coinjoin amount, and encryption key
Reply with own encryption key	

Messages beyond this point are encrypted

	Send signature of encryption key using input utxo pubkey
Send inputs, desired output and change addresses (all signed)	
	Construct transaction using each participant’s inputs and outputs
Sign constructed transaction	

First JoinMarket Protocol

Participant / "Maker"	Initiator / "Taker"
Advertise liquidity and rate (publicly)	
	Send chosen offer, coinjoin amount, and encryption key
Reply with own encryption key	

Messages beyond this point are encrypted

	Send signature of encryption key using input utxo pubkey
Send inputs, desired output and change addresses (all signed)	
	Construct transaction using each participant’s inputs and outputs
Sign constructed transaction	
	Sign and broadcast

Leakage, Leakage, Leakage!

Leakage, Leakage, Leakage!

- Initiator signs last... or not at all

Leakage, Leakage, Leakage!

- Initiator signs last... or not at all

- Information learned during an incomplete run of the protocol is thus **free**

Leakage, Leakage, Leakage!

- Initiator signs last... or not at all
- Information learned during an incomplete run of the protocol is thus **free**
- Malicious initiator can snoop which coins are provided by which participants

Leakage, Leakage, Leakage!

- Initiator signs last... or not at all
- Information learned during an incomplete run of the protocol is thus **free**
- Malicious initiator can snoop which coins are provided by which participants
- By June 2016, most initiations failed to complete (real usage also increased)

Second JoinMarket Protocol

Second JoinMarket Protocol

- Same overall sequence as first version

Second JoinMarket Protocol

- Same overall sequence as first version
- Every message is signed

Second JoinMarket Protocol

- Same overall sequence as first version
- Every message is signed
- Takers publish a unique-per-UTXO commitment before makers reveal inputs

Second JoinMarket Protocol

- Same overall sequence as first version
- Every message is signed
- Takers publish a unique-per-UTXO commitment before makers reveal inputs
- Malicious snoop must create fresh commitments, putting a cost on the attack

Future Directions

Future Directions

- Wallet Integrations (Electrum, Core)

Future Directions

- Wallet Integrations (Electrum, Core)
- Hybrid Mode (make while you take)

Future Directions

- Wallet Integrations (Electrum, Core)
- Hybrid Mode (make while you take)
  - Interface Cleanup (API-ification)

Future Directions

- Wallet Integrations (Electrum, Core)
- Hybrid Mode (make while you take)
- Interface Cleanup (API-ification)
- Statistics on economic activity

Future Directions

- Wallet Integrations (Electrum, Core)
- Hybrid Mode (make while you take)
- Interface Cleanup (API-ification)
- Statistics on economic activity
- Gauge privacy improvement

Future Directions

- Wallet Integrations (Electrum, Core)
- Hybrid Mode (make while you take)
- Interface Cleanup (API-ification)
- Statistics on economic activity
- Gauge privacy improvement
- CoinSwap

THIS SLIDE LEFT
INTENTIONALLY BLANK