# Trustless Asset Swaps

Bitshares and HTLC

### BSIP xxxx: HTLC

- Background: Escrow
  - Put an amount of an asset on hold (transfer to escrow agent)
  - Release the hold (transfer all or some) when certain conditions exist
- What is different with HTLC
  - Escrow with tight conditions
    - Put an amount of an asset on hold (no transfer agent)
    - Release the hold after a certain date/time (a.k.a. the Time Lock)
      - Or
    - Transfer the funds when the "preimage" is presented (a.k.a. the Hash Lock)

### How Hashed and Time Lock Contracts work:

- Alice creates an HTLC and places it on the Bitshares Blockchain
  - Amount of an asset that is put on hold
  - Who should receive the asset (i.e. Bob's account)
  - Hash and size of her "preimage"
    - 8A45F62F47476BEED04FED43D498E7C2FD6055D3AB28013E670651AC9FF1725F
  - Time after which Alice can release her funds back into her account
- What can happen
  - Bob presents the preimage and the funds are moved to his account
    - o Or
  - Time passes and the funds return to Alice's account

### Interesting Use Cases

- Regular purchases
  - Bob is guaranteed that Alice has the amount of the asset necessary
    - Funds are reserved until a specific time
- Asset swaps without the exchange
  - Alice and Bob agree to exchange assets at a certain price
  - Alice makes an HTLC that contains a certain hash (generated from preimage)
  - o Bill makes an HTLC that contains the same hash
  - When Alice executes Bill's contract, Bill can see the preimage used, and can execute Alice's contract.
- Cross-Chain Atomic Swaps
  - Chains must support HTLC (or use middleware)

## HTLC Support on other blockchains:

	ABY	втс	всн	BLK	DASH	DCR	DOGE	ETH	GRS	LTC	XMR	PART	SYS	VIA	VTC	xzc	ZEC	ERC20
ABY	,	5/8	5/8	5/8	5/8	5/8	4/8	5/8	5/8	5/8	2/8	5/8	5/8	5/8	5/8	5/8	5/8	5/8
втс	5/8		7/8	5/8	7/8	8/8	6/8	7/8	5/8	8/8	2/8	8/8	7/8	7/8	8/8	8/8	6/8	5/8
всн	5/8	7/8		5/8	7/8	7/8	6/8	5/8	5/8	7/8	2/8	7/8	7/8	7/8	7/8	5/8	5/8	5/8
BLK	5/8	5/8	5/8		5/8	5/8	4/8	5/8	5/8	5/8	2/8	5/8	5/8	5/8	5/8	5/8	5/8	5/8
DASH	5/8	7/8	7/8	5/8		7/8	6/8	5/8	5/8	7/8	2/8	7/8	7/8	7/8	7/8	5/8	5/8	5/8
DCR	5/8	8/8	7/8	5/8	7/8		6/8	7/8	5/8	8/8	2/8	8/8	7/8	7/8	8/8	8/8	5/8	5/8
DOGE	4/8	6/8	6/8	4/8	6/8	6/8		4/8	4/8	6/8	1/8	6/8	6/8	6/8	6/8	4/8	4/8	4/8
ETH	5/8	7/8	5/8	5/8	5/8	7/8	4/8		5/8	7/8	2/8	7/8	5/8	5/8	7/8	7/8	5/8	5/8
GRS	5/8	5/8	5/8	5/8	5/8	5/8	4/8	5/8		5/8	2/8	5/8	5/8	5/8	5/8	5/8	5/8	5/8
LTC	5/8	8/8	7/8	5/8	7/8	8/8	6/8	7/8	5/8		2/8	8/8	7/8	7/8	8/8	8/8	5/8	5/8
XMR	2/8	2/8	2/8	2/8	2/8	2/8	1/8	2/8	2/8	2/8		2/8	2/8	2/8	2/8	2/8	2/8	2/8
PART	5/8	8/8	7/8	5/8	7/8	8/8	6/8	7/8	5/8	8/8	2/8		7/8	7/8	8/8	8/8	5/8	5/8
SYS	5/8	7/8	7/8	5/8	7/8	7/8	6/8	5/8	5/8	7/8	2/8	7/8		7/8	7/8	5/8	5/8	5/8
VIA	5/8	7/8	7/8	5/8	7/8	7/8	6/8	5/8	5/8	7/8	2/8	7/8	7/8		7/8	5/8	5/8	5/8
VTC	5/8	8/8	7/8	5/8	7/8	8/8	6/8	7/8	5/8	8/8	2/8	8/8	7/8	7/8		8/8	5/8	5/8
xzc	5/8	8/8	5/8	5/8	5/8	8/8	4/8	7/8	5/8	8/8	2/8	8/8	5/8	5/8	8/8		5/8	5/8
ZEC	5/8	6/8	5/8	5/8	5/8	5/8	4/8	5/8	5/8	5/8	2/8	5/8	5/8	5/8	5/8	5/8		5/8
ERC20	5/8	5/8	5/8	5/8	5/8	5/8	4/8	5/8	5/8	5/8	2/8	5/8	5/8	5/8	5/8	5/8	5/8	5/8

### What needs to be done to make this useful:

- Wallets / Websites
  - Mini-Gateway "Trustless" transfers of assets across chains
    - No self-issued asset is necessarily needed
    - Transaction transparency
  - Wallet Support Ways to create, examine, and execute HTLCs
- Current status of BSIP
  - Talk about it
  - Shoot holes in it
  - Make it better

### What I do:

- Issues
- PRs
- BitShares Improvement Proposals (BSIPs)

Working for the Bitshares Community is somewhat unique:

- Team Accountability
- Personal Accountability
- Worldwide team
- Anyone can contribute (please understand: BitShares coding standards)

### About me: John Jones

- Software development for a long time
- (almost) always on back-end development
- (almost) always in banking / finance / insurance
- bitshares-core team since near the start of the current worker proposal

Email: jmjatlanta@gmail.com	Telegram: jmjatlanta
Skype: jmjatlanta	Keybase: jmjatlanta
Twitter: jmjatlanta	Bitsharestalk.com: jmjatlanta
LinkedIn: jmjatlanta	Website: jmjatlanta.com