bitcoin

CS1699: Blockchain Technology and Cryptocurrency

21. Atomic Swaps, Sidechains, and SPV Proofs

Bill Laboon

The Problem

- Assume you want to convert some of your coin X to coin Y. How do you do it?
- Most-common way: centralized exchange (e.g. shapeshift.io)
- Less common way: "decentralized" exchange (e.g. https://localmonero.co/?language=en)
- Even truly "decentralized" exchanges often have a single point of failure (See EtherDelta lawsuit: https://www.forbes.com/sites/michaeldelcastillo/2018/11/09/new-sec-cyber-chief-puts-cryptocurrency-exchanges-on-notice/#796a89552fb8)
- How can we ensure our system continues to operate with high availability using only the blockchains themselves and not a third-party or escrow service?

Atomic Cross-Chain Swaps

- We have seen that we can combine multiple transactions into a single "atomic" transaction in CoinJoin
- Can we do the same thing on multiple blockchains simultaneously, so that I can have a transaction that gives you X amount of Coin X while you give me Y amount of Coin Y, and vice versa?
- Yes, although it is complex and a bit slow!

Alice and Bob Swapping Litecoin for Bitcoin

- Alice generates a refundable deposit of *a* litecoin
- Bob generates a refundable deposit of *b* bitcoin
- Alice claims *b* bitcoin by time $T1$ ($T1 < T2$)
- Bob claims *a* litecoin by time $T2$ ($T2 > T1$)

Alice Generates Refundable Deposit of Litecoin

1. Alice generates a random string x and computes $h = H(x)$
2. Alice generates **DepositA** transaction (which to unlock requires EITHER (knowing x and signed by Bob) OR (signed by Alice and Bob)) on Litecoin network, but does not publish it
3. Alice generates time-locked **RefundA** (which cannot be claimed until after some time T_2) transaction and gets Bob's signature on it
4. Alice now publishes **DepositA** but holds back **RefundA**

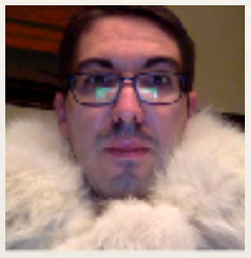
Bob Generates Refundable Deposit of Bitcoin

1. Bob generates **DepositB** (which to unlock requires EITHER (knowing *x* and signed by Alice) OR (signed by Alice and Bob)) but does not publish it
2. Bob generates time-locked **RefundB** (which cannot be claimed until after some time *T1*) and gets Alice's signature on it
3. Bob now publishes **DepositB** but holds back **RefundB**

Decision Point

- Alice decides to complete the swap
  - Alice claims bitcoin by time *T1*, thus revealing *x*
    - Bob now knows *x* and can claim litecoin by time T_2
- Alice changes her mind
  - Bob claims his refund (pre-signed by Alice)
  - Alice claims her refund (pre-signed by Bob)

"Good" Atomic Swap Timeline



Alice

Bob

Generates x

Generates DepositA and RefundA

Publishes h=H(x) and DepositA

Alice claims Bitcoin from DepositB, revealing x

Time

A

B

C

T1

T2

Generates DepositB and RefundB

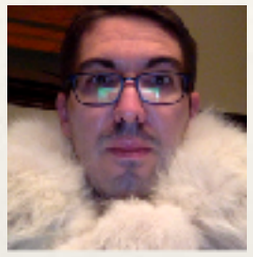
Publishes DepositB

Bob claims Litecoin using x

Can Be Rolled Back at Any Point

- Before A: No transaction broadcast - no danger
- Between A & B: Alice can use refund transaction after T2
- Between B & C: Bob can get refund after T1 but before T2. Alice can get refund after T2.
- After C: Transaction is completed (Alice must spend coin before T1, or Bob can claim refund and keep coins ; Bob must spend coin before T2, or Alice can claim refund)

"Bad Alice" Atomic Swap Timeline



Alice

Bob

Generates x

Generates DepositA and RefundA

~~Publishes h=H(x) and DepositA~~

Alice CANNOT claim Bitcoin from DepositB

Alice keeps her own Litecoin

Time

A

B

C

T1

T2

Generates DepositB and RefundB

DOES NOT Publish DepositB

Bob CANNOT claim Litecoin since x was never revealed

"Bad Bob" Atomic Swap Timeline

Alice

Bob

Generates x

Generates DepositA and RefundA

Publishes h=H(x) and DepositA

Alice CANNOT claim Bitcoin from DepositB

Alice refunded her own Litecoin from RefundA

Time

A

B

C

T1

T2

Generates DepositB and RefundB

~~Publish DepositB~~

Bob CANNOT claim Litecoin since x was never revealed

Benefits of Atomic Swaps

- No middleman
- No counterparty risk
- Entirely decentralized from a trading perspective
- Can be rolled back at any point

Problems with Atomic Swaps

- Slow (MUCH slower than a centralized exchange)
- Need to find a trading partner - might lead to being centralization at this level
- Time-bounded; if you don't claim your coins at the proper time, you will lose them!
- Vulnerable to DOS (by Alice/Bob backing out after coins committed)
- Very slim chance that block production times line up in such a way that $T_2 < T_1$ or other weirdness (as block production time is probabilistic - *essentially* random following a power distribution)

Sidechains

- "Altcoins on Bitcoin" - Provide additional functionality while providing a bilateral peg to Bitcoin
- Escrow Bitcoin, but allow users to transfer back and forth between sidechain and main chain
- To truly do this, would need to extend Bitcoin - but can essentially have all the features by a simple hack

"The SPV Trick"

- Use SPV (Simplified Payment Verification) to look for evidence that transactions they care about are in longest branch that has received x verifications
- Scripts could just verify that a particular transaction occurred in the sidechain using SPV

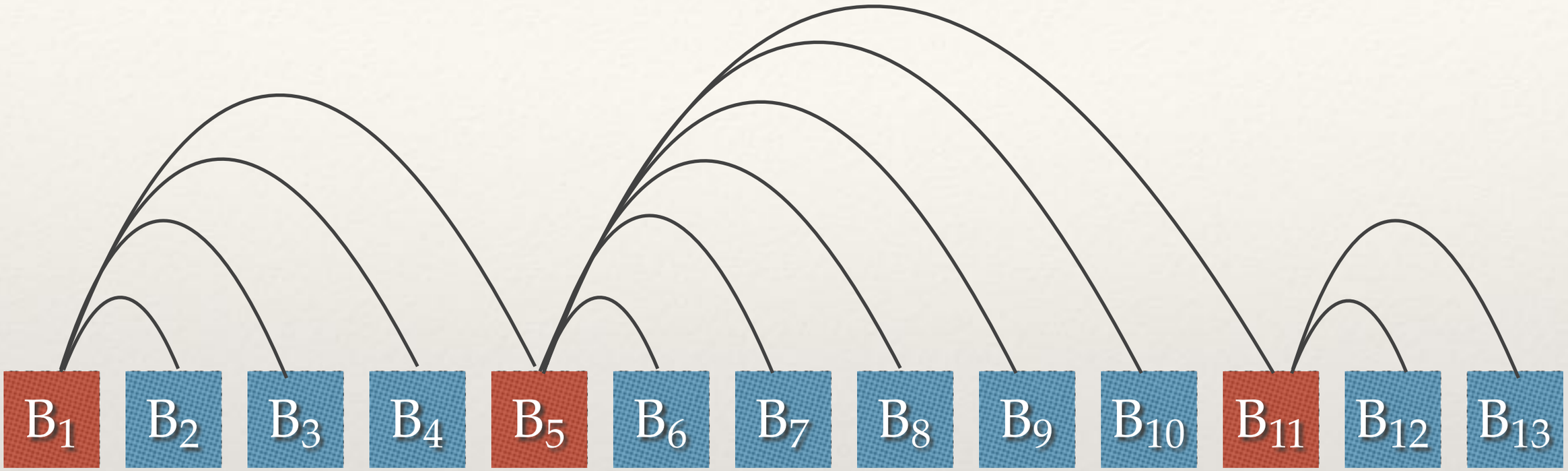
SPV Proofs

- Need Bitcoin to verify legitimacy of sidechain coins
- User provides:
  - Proof of inclusion in sidechain transactions
    - Sidechain block headers showing certain number of confirmations
- Can be contested; must wait a provisional period after submitting proof
- Not foolproof from a sidechain perspective; but DOES ensure that Bitcoin itself is not harmed by any sidechain

SPV Proofs via PoW Samples

- What if we have very "fast" (i.e., short time between blocks) sidechains? Even a SPV Bitcoin node may not be able to keep up.
- We can use skiplists to "sample" PoW and estimate total work generated in a sublinear manner
- Skiplist points only to blocks where $h < (target/m)$
  - Should be evenly distributed since hash for each block should be in a uniform distribution *(0, target)*

Skiplist with $h < target/4$



B1 **Block where $h < (target/4)$**

B2 **Block where $h >= (target/4)$ and $h < target$**

Notable Bitcoin Sidechains

- Mastercoin, later rebranded Omni - Used for asset and token management - https://www.omnilayer.org/
- Drivechain - Platform for generating your own sidechains - http://www.drivechain.info/
- Liquid Network- Bilateral peg to Bitcoin (with native asset L-BTC) with faster settlement times - https://blockstream.com/liquid/