Lightning Network

Haoran Qi
10/26/2018

Background

"If a tree falls in the forest and no one is around to hear it, does it make a sound?"

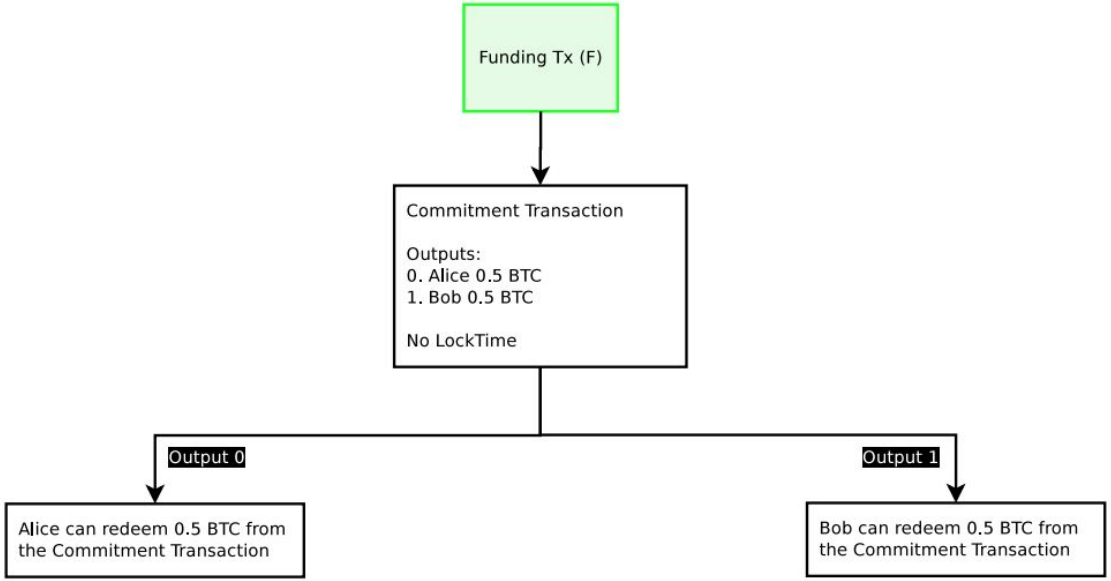
Payment Channels

- Uses multi-sig
- Allows two people to send transactions to each other without hitting the Bitcoin blockchain

Bidirectional Payment Channels

- Funding Transaction
- SIGHASH_NOINPUT
- Commitment Transactions

Bidirectional Payment Channels



Funding Tx (F)

Commitment Transaction

Outputs:
0. Alice 0.5 BTC
1. Bob 0.5 BTC

No LockTime

Output 0

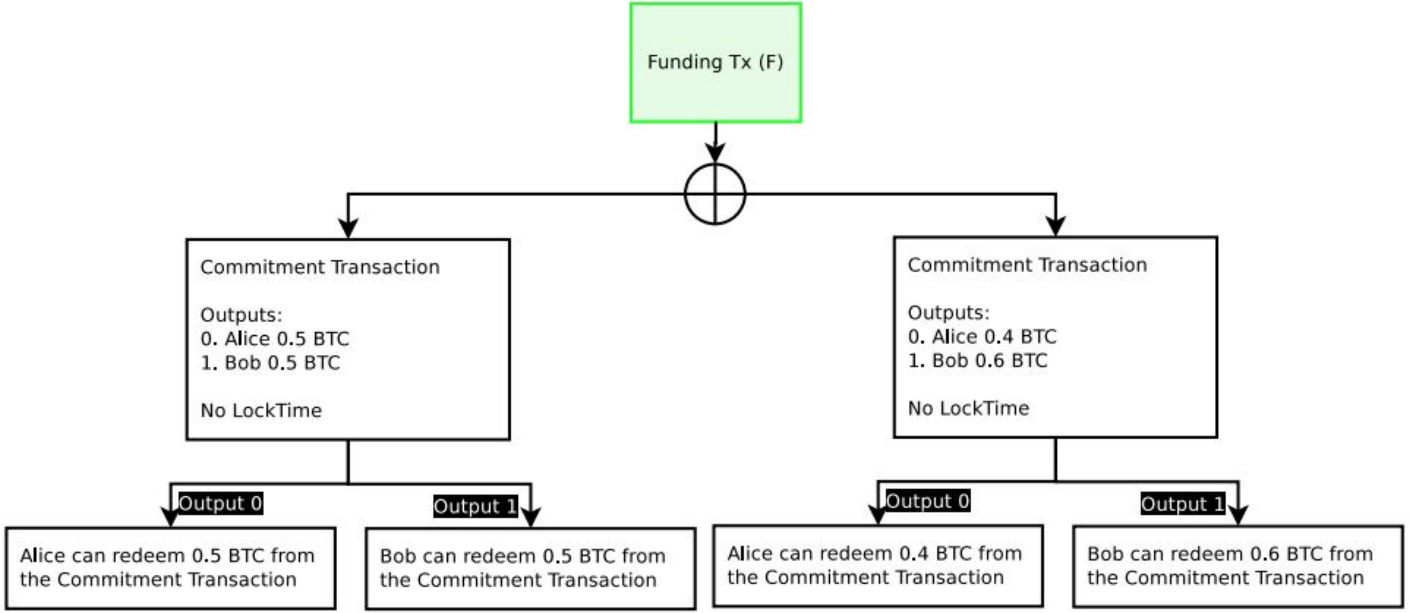
Output 1

Alice can redeem 0.5 BTC from the Commitment Transaction

Bob can redeem 0.5 BTC from the Commitment Transaction

Figure 1: A naive broken funding transaction is described in this diagram. The Funding Transaction (F), designated in green, is broadcast on the blockchain after all other transactions are signed. All other transactions spending from the funding transactions are not yet broadcast, in case the counterparties wish to update their balance. Only the Funding Transaction is broadcast on the blockchain at this time.

Bidirectional Payment Channels



Funding Tx (F)

Commitment Transaction

Outputs:
0. Alice 0.5 BTC
1. Bob 0.5 BTC

No LockTime

Commitment Transaction

Outputs:
0. Alice 0.4 BTC
1. Bob 0.6 BTC

No LockTime

Alice can redeem 0.5 BTC from the Commitment Transaction

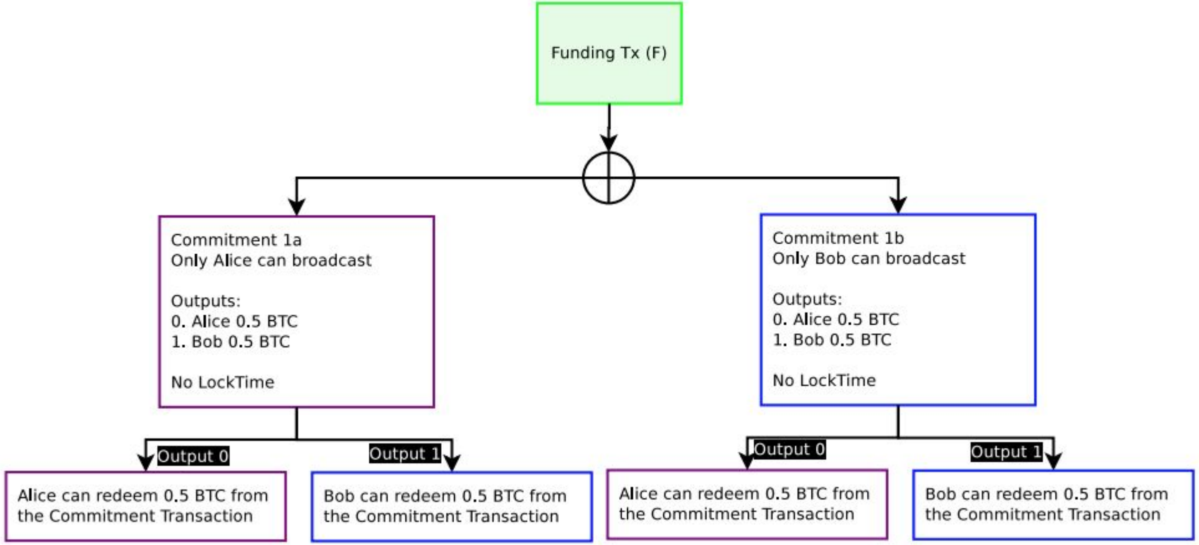
Bob can redeem 0.5 BTC from the Commitment Transaction

Alice can redeem 0.4 BTC from the Commitment Transaction

Bob can redeem 0.6 BTC from the Commitment Transaction

Figure 2: Either of the Commitment Transactions can be broadcast any any time by either party, only one will successfully spend from the single Funding Transaction. This cannot work because one party will not want to broadcast the most recent transaction.

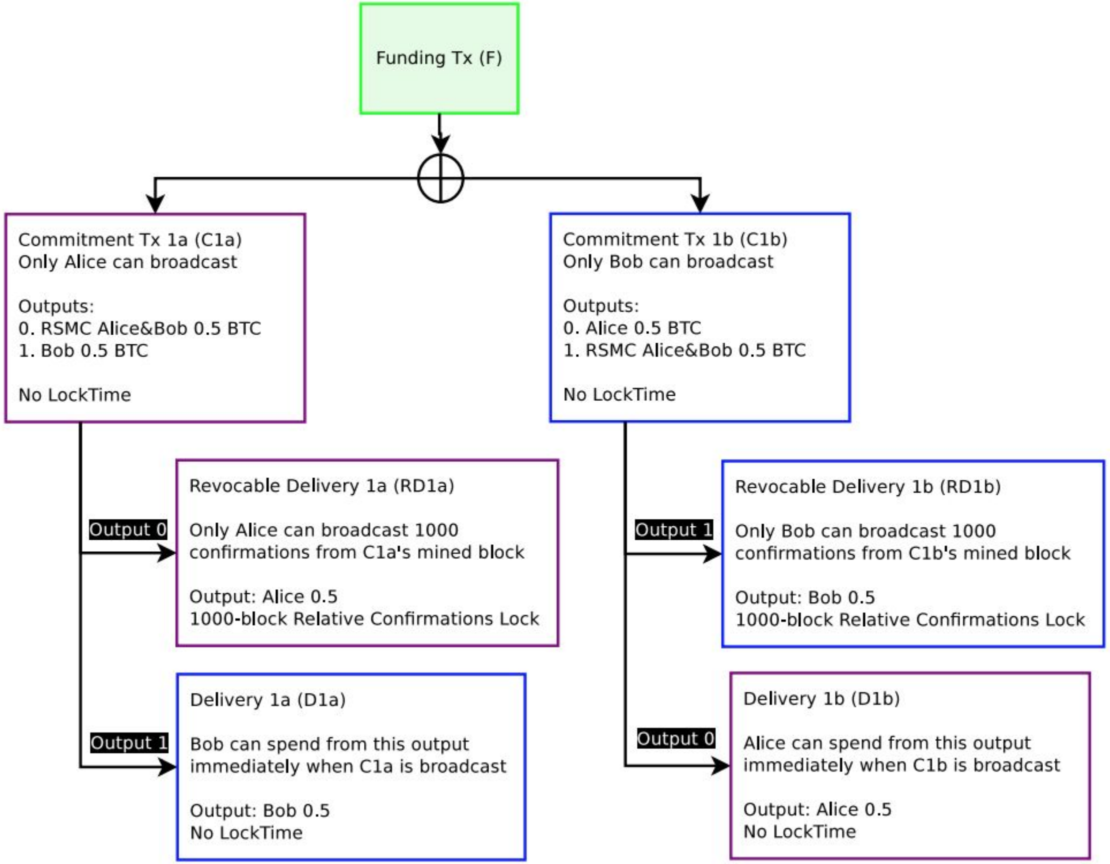
Bidirectional Payment Channels



Funding Tx (F)
Commitment 1a
Only Alice can broadcast
Outputs:
0. Alice 0.5 BTC
1. Bob 0.5 BTC
No LockTime
Commitment 1b
Only Bob can broadcast
Outputs:
0. Alice 0.5 BTC
1. Bob 0.5 BTC
No LockTime
Output 0
Output 1
Alice can redeem 0.5 BTC from the Commitment Transaction
Bob can redeem 0.5 BTC from the Commitment Transaction
Output 0
Output 1
Alice can redeem 0.5 BTC from the Commitment Transaction
Bob can redeem 0.5 BTC from the Commitment Transaction

Figure 3: Purple boxes are unbroadcasted transactions which only Alice can broadcast. Blue boxes are unbroadcasted transaction which only Bob can broadcast. Alice can only broadcast Commitment 1a, Bob can only broadcast Commitment 1b. Only one Commitment Transaction can be spent from the Funding Transaction output. Blame is ascribed, but either one can still be spent with no penalty.

Revocable Sequence Maturity Contract (RSMC)



Funding Tx (F)

Commitment Tx 1a (C1a)
Only Alice can broadcast

Outputs:
0. RSMC Alice&Bob 0.5 BTC
1. Bob 0.5 BTC

No LockTime

Commitment Tx 1b (C1b)
Only Bob can broadcast

Outputs:
0. Alice 0.5 BTC
1. RSMC Alice&Bob 0.5 BTC

No LockTime

Output 0

Revocable Delivery 1a (RD1a)

Only Alice can broadcast 1000 confirmations from C1a's mined block

Output: Alice 0.5
1000-block Relative Confirmations Lock

Output 1

Delivery 1a (D1a)

Bob can spend from this output immediately when C1a is broadcast

Output: Bob 0.5
No LockTime

Output 1

Revocable Delivery 1b (RD1b)

Only Bob can broadcast 1000 confirmations from C1b's mined block

Output: Bob 0.5
1000-block Relative Confirmations Lock

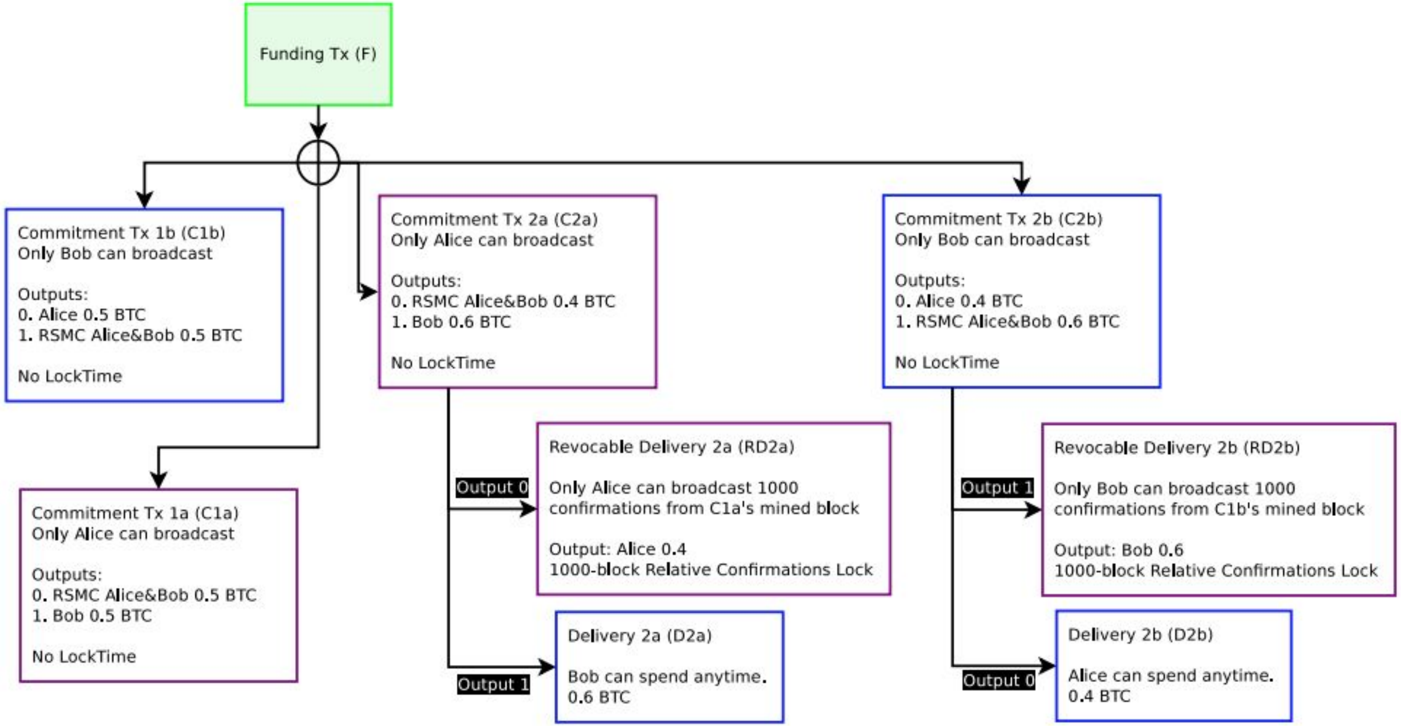
Output 0

Delivery 1b (D1b)

Alice can spend from this output immediately when C1b is broadcast

Output: Alice 0.5
No LockTime

Figure 4: The Funding Transaction F, designated in green, is broadcast on the blockchain after all other transactions are signed. All transactions which only Alice can broadcast are in purple. All transactions which only Bob can broadcast is are blue. Only the Funding Transaction is broadcast on the blockchain at this time.



Funding Tx (F)

Commitment Tx 1b (C1b)
Only Bob can broadcast

Outputs:
0. Alice 0.5 BTC
1. RSMC Alice&Bob 0.5 BTC

No LockTime

Commitment Tx 2a (C2a)
Only Alice can broadcast

Outputs:
0. RSMC Alice&Bob 0.4 BTC
1. Bob 0.6 BTC

No LockTime

Commitment Tx 2b (C2b)
Only Bob can broadcast

Outputs:
0. Alice 0.4 BTC
1. RSMC Alice&Bob 0.6 BTC

No LockTime

Commitment Tx 1a (C1a)
Only Alice can broadcast

Outputs:
0. RSMC Alice&Bob 0.5 BTC
1. Bob 0.5 BTC

No LockTime

Output 0

Revocable Delivery 2a (RD2a)

Only Alice can broadcast 1000 confirmations from C1a's mined block

Output: Alice 0.4
1000-block Relative Confirmations Lock

Output 1

Delivery 2a (D2a)

Bob can spend anytime.
0.6 BTC

Output 1

Revocable Delivery 2b (RD2b)

Only Bob can broadcast 1000 confirmations from C1b's mined block

Output: Bob 0.6
1000-block Relative Confirmations Lock

Output 0

Delivery 2b (D2b)

Alice can spend anytime.
0.4 BTC

Figure 7: Four possible transactions can exist, a pair with the old commitments, and another pair with the new commitments. Each party inside the channel can only broadcast half of the total commitments (two each). There is no explicit enforcement preventing any particular Commitment being broadcast other than penalty spends, as they are all valid unbroadcasted spends. The Revocable Commitment still exists with the C1a/C1b pair, but are not displayed for brevity.

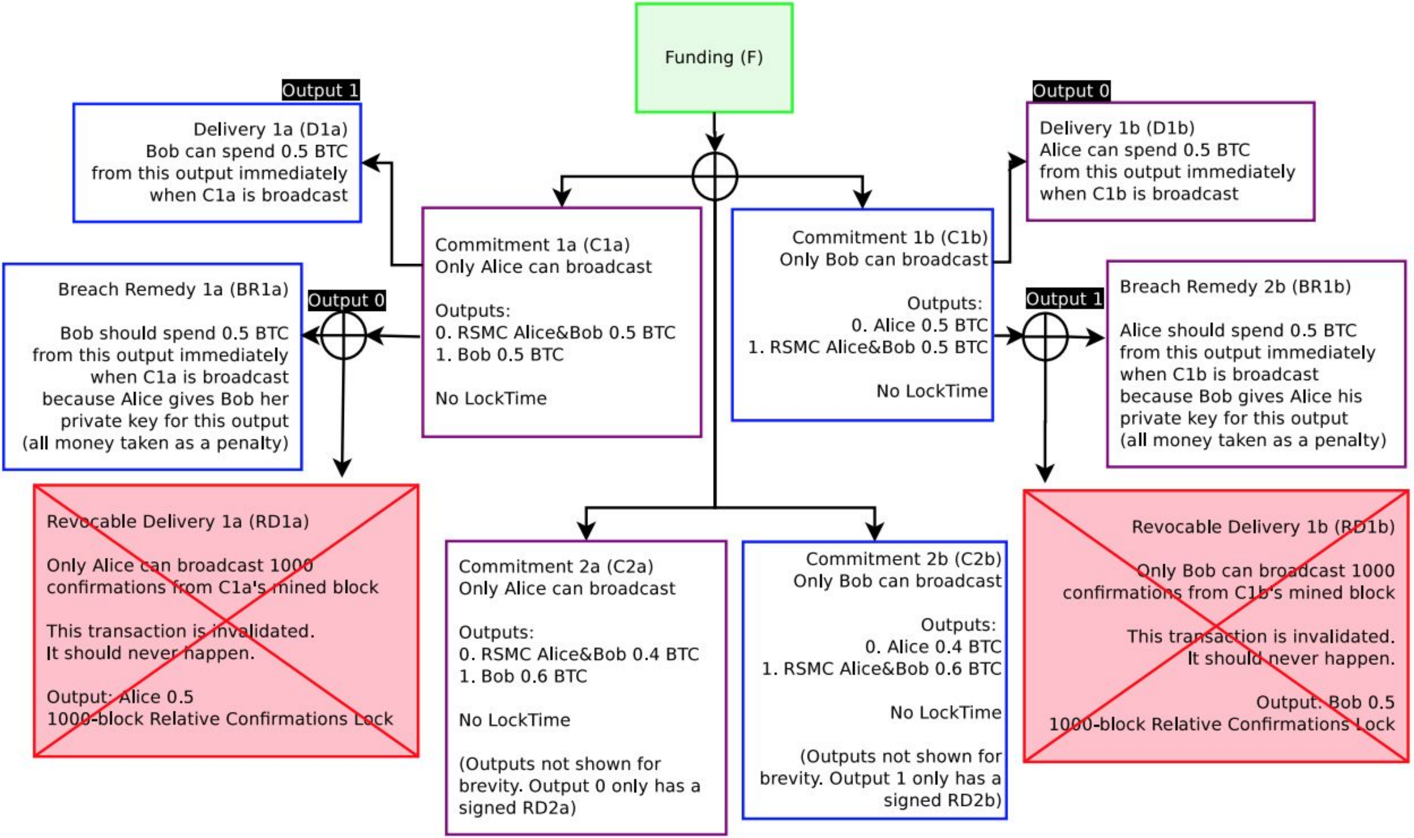
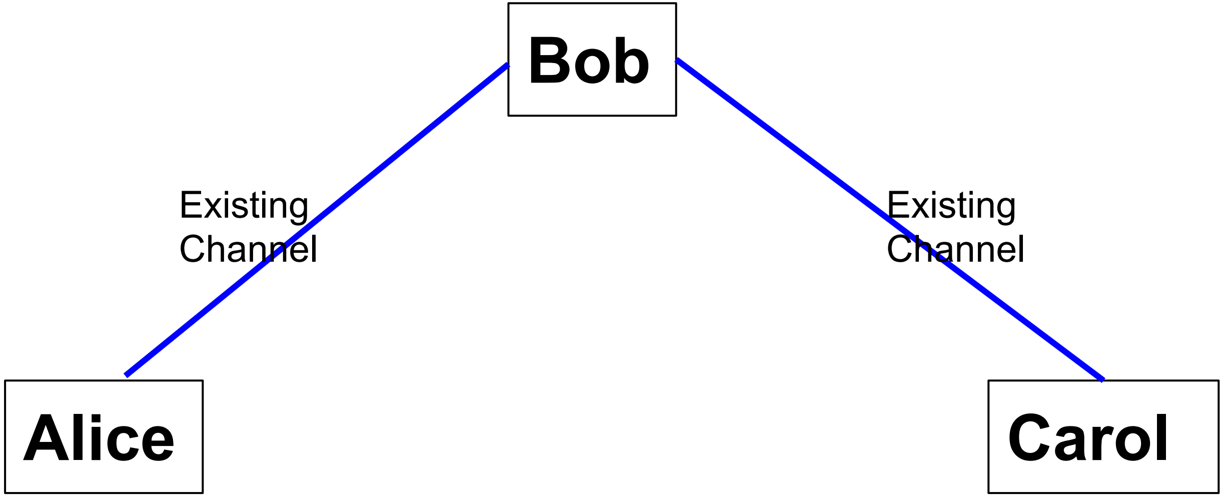

Funding (F)
Output 1
Delivery 1a (D1a)
Bob can spend 0.5 BTC
from this output immediately
when C1a is broadcast
Commitment 1a (C1a)
Only Alice can broadcast
Outputs:
0. RSMC Alice&Bob 0.5 BTC
1. Bob 0.5 BTC
No LockTime
Output 0
Delivery 1b (D1b)
Alice can spend 0.5 BTC
from this output immediately
when C1b is broadcast
Commitment 1b (C1b)
Only Bob can broadcast
Outputs:
0. Alice 0.5 BTC
1. RSMC Alice&Bob 0.5 BTC
No LockTime
Breach Remedy 1a (BR1a)
Bob should spend 0.5 BTC
from this output immediately
when C1a is broadcast
because Alice gives Bob her
private key for this output
(all money taken as a penalty)
Output 0
Output 1
Breach Remedy 2b (BR1b)
Alice should spend 0.5 BTC
from this output immediately
when C1b is broadcast
because Bob gives Alice his
private key for this output
(all money taken as a penalty)
Revocable Delivery 1a (RD1a)
Only Alice can broadcast 1000
confirmations from C1a's mined block
This transaction is invalidated.
It should never happen.
Output: Alice 0.5
1000-block Relative Confirmations Lock
Commitment 2a (C2a)
Only Alice can broadcast
Outputs:
0. RSMC Alice&Bob 0.4 BTC
1. Bob 0.6 BTC
No LockTime
(Outputs not shown for
brevity. Output 0 only has a
signed RD2a)
Commitment 2b (C2b)
Only Bob can broadcast
Outputs:
0. Alice 0.4 BTC
1. RSMC Alice&Bob 0.6 BTC
No LockTime
(Outputs not shown for
brevity. Output 1 only has a
signed RD2b)
Revocable Delivery 1b (RD1b)
Only Bob can broadcast 1000
confirmations from C1b's mined block
This transaction is invalidated.
It should never happen.
Output: Bob 0.5
1000-block Relative Confirmations Lock

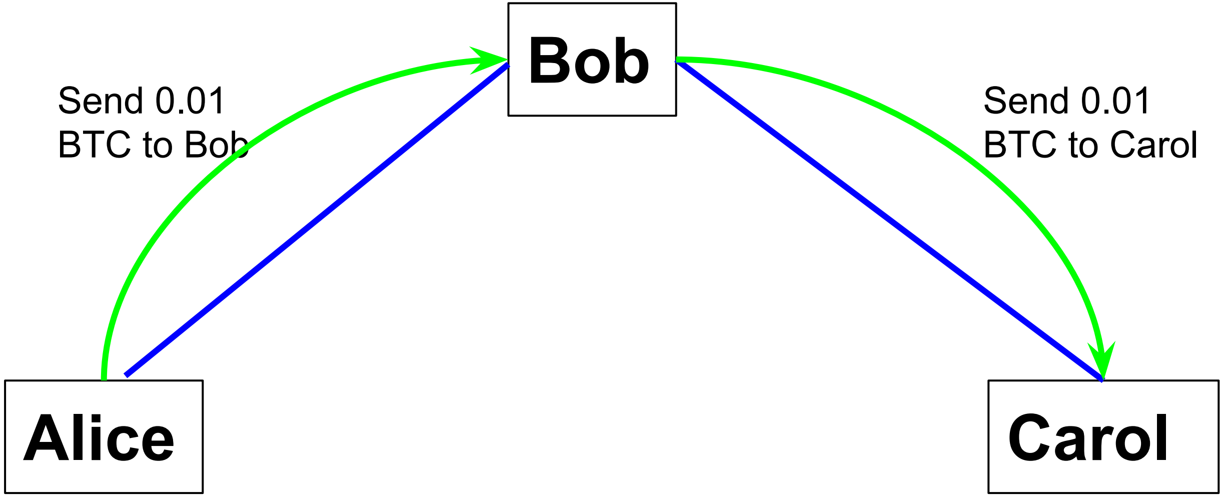
Figure 8: When C2a and C2b exist, both parties exchange Breach Remedy transactions. Both parties now have explicit economic incentive to avoid broadcasting old Commitment Transactions (C1a/C1b). If either party wishes to close out the channel, they will only use C2a (Alice) or C2b (Bob). If Alice broadcasts C1a, all her money will go to Bob. If Bob broadcasts C1b, all his money will go to Alice. See previous figure for C2a/C2b outputs.

3 Party Payments



Alice wants to pay Carol, they both have a channel open with Bob

3 Party Payments



Bob

Send 0.01 BTC to Bob

Send 0.01 BTC to Carol

Alice

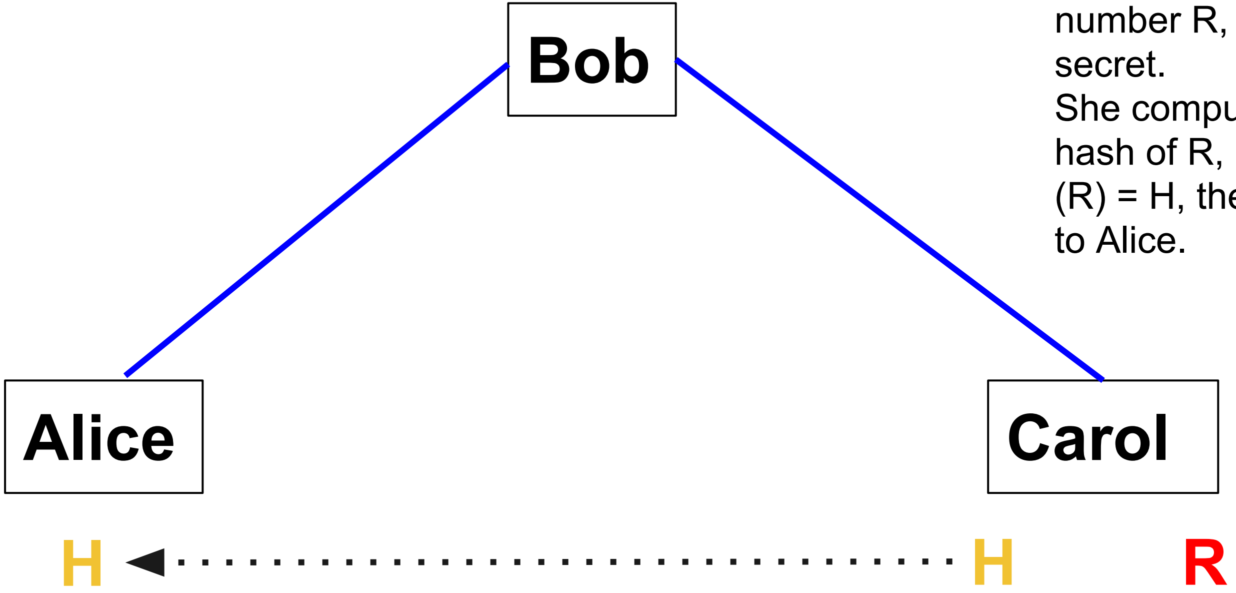
Carol

Problem: Bob can simply keep the 0.01 BTC
Problem: Carol can claim she never got the coins!

Hash-Locked Contracts

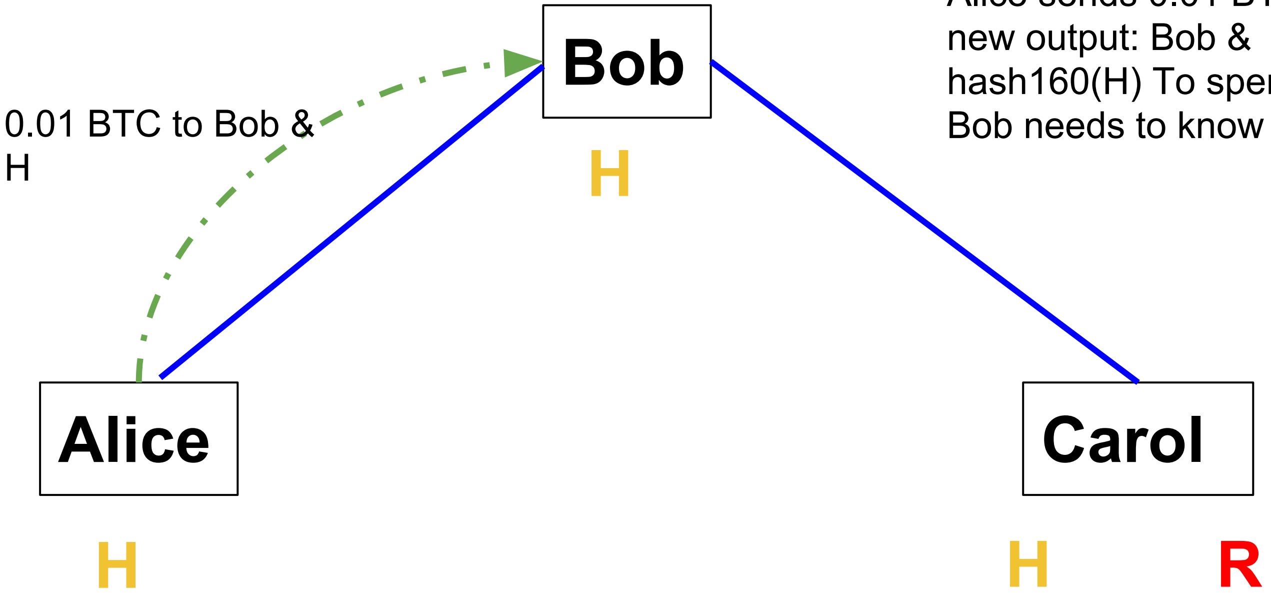
- Using one-way hash functions, Alice can prove she sent funds to Carol off-chain
- Pay to Contract
  - Knowledge of secret R hashed into hash H proves Receipt
  - Receiver signs a contract stating if R is disclosed funds have been received

Hash-Locked Contracts



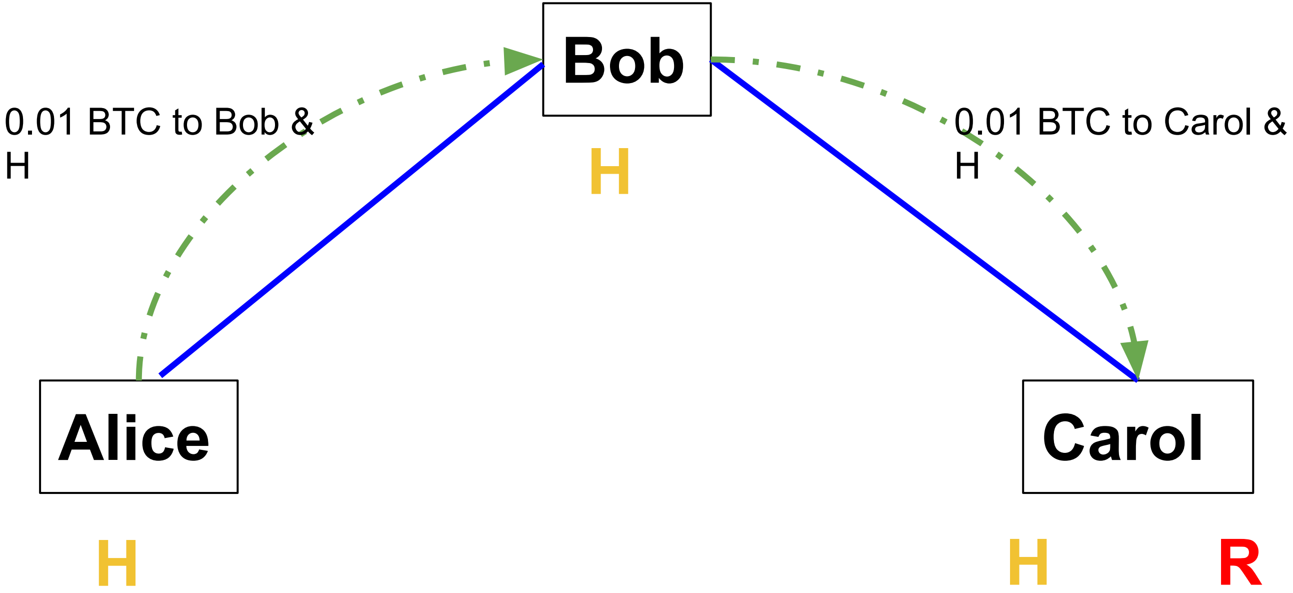
Carol makes a random number R, and keeps it secret.
She computes the hash of R, hash (R) = H, then sends it to Alice.

Hash-Locked Contracts



Alice sends 0.01 BTC to a new output: Bob & hash160(H) To spend it, Bob needs to know R

Hash-Locked Contracts



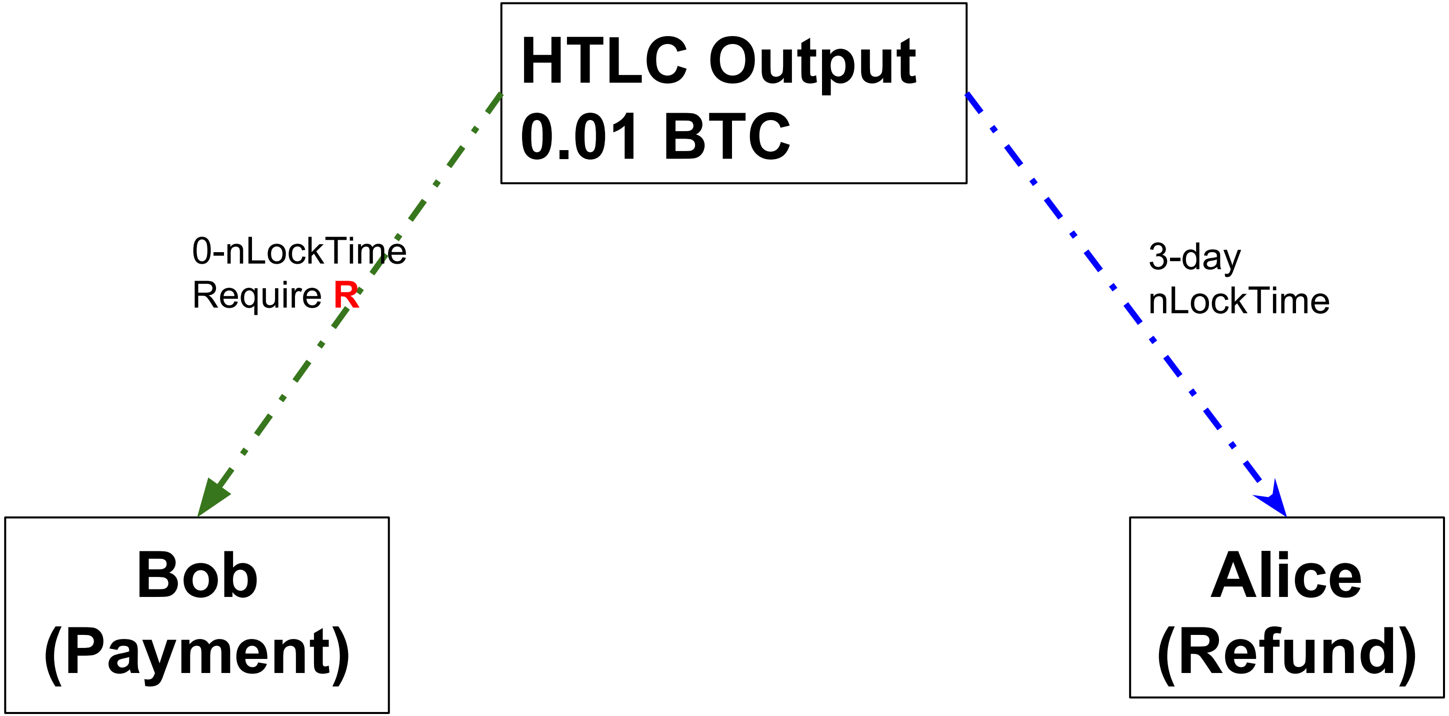
Problem

- If Carol refuses to disclose R, she will hold up the channel between Alice and Bob
    - If her channel expires after Alice and Bob’s she can steal funds by redeeming the hashlock!

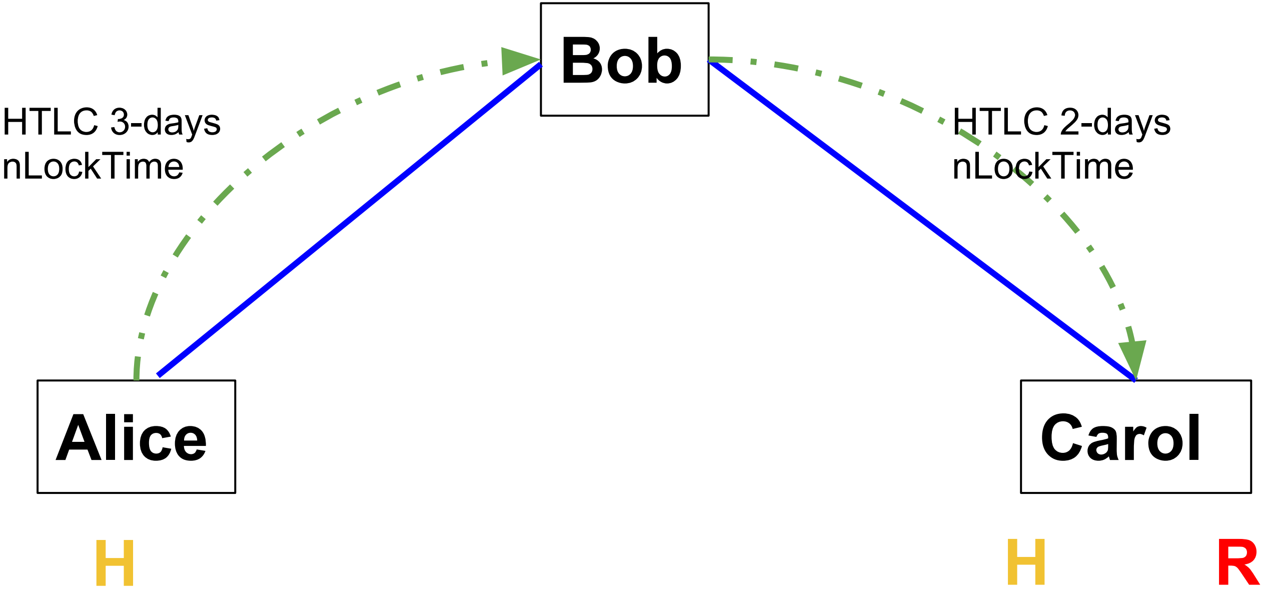
Hashed Time-Lock Contract (HTLC)

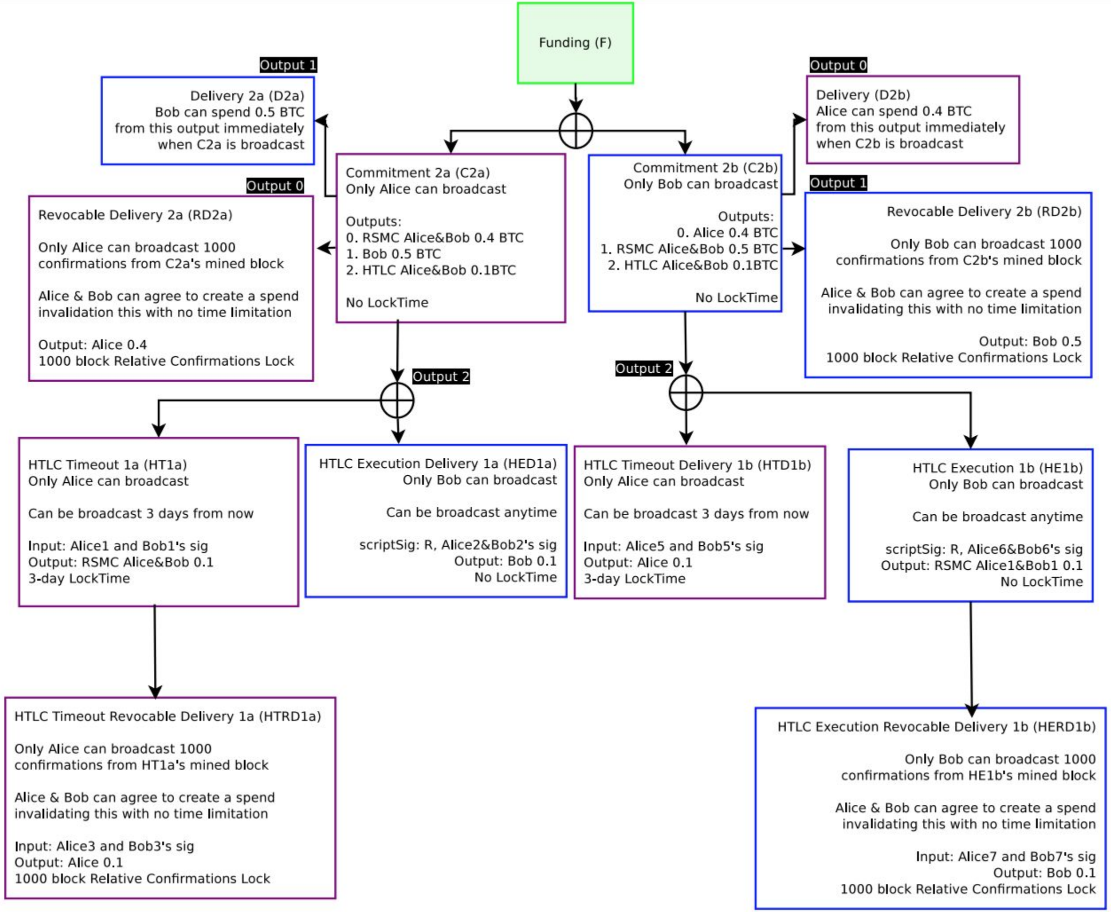
- If Bob can produce to Alice input R from hash H within 3 days, Alice will pay Bob 0.01 BTC
- The above clause is void after 3 days
- Either party may agree to settle terms using other methods if both agree
- Violation of terms incurs a maximum penalty of funds in this contract

Hashed Time-Lock Contract (HTLC)



Hashed Time-Lock Contract (HTLC)





Funding (F)

Output 1

Delivery 2a (D2a)
Bob can spend 0.5 BTC
from this output immediately
when C2a is broadcast

Output 0

Revocable Delivery 2a (RD2a)

Only Alice can broadcast 1000
confirmations from C2a's mined block

Alice & Bob can agree to create a spend
invalidation this with no time limitation

Output: Alice 0.4
1000 block Relative Confirmations Lock

Commitment 2a (C2a)
Only Alice can broadcast

Outputs:
0. RSMC Alice&Bob 0.4 BTC
1. Bob 0.5 BTC
2. HTLC Alice&Bob 0.1BTC

No LockTime

Commitment 2b (C2b)
Only Bob can broadcast

Outputs:
0. Alice 0.4 BTC
1. RSMC Alice&Bob 0.5 BTC
2. HTLC Alice&Bob 0.1BTC

No LockTime

Output 0

Delivery (D2b)
Alice can spend 0.4 BTC
from this output immediately
when C2b is broadcast

Output 1

Revocable Delivery 2b (RD2b)

Only Bob can broadcast 1000
confirmations from C2b's mined block

Alice & Bob can agree to create a spend
invalidating this with no time limitation

Output: Bob 0.5
1000 block Relative Confirmations Lock

Output 2

Output 2

HTLC Timeout 1a (HT1a)
Only Alice can broadcast

Can be broadcast 3 days from now

Input: Alice1 and Bob1's sig
Output: RSMC Alice&Bob 0.1
3-day LockTime

HTLC Execution Delivery 1a (HED1a)
Only Bob can broadcast

Can be broadcast anytime

scriptSig: R, Alice2&Bob2's sig
Output: Bob 0.1
No LockTime

HTLC Timeout Delivery 1b (HTD1b)
Only Alice can broadcast

Can be broadcast 3 days from now

Input: Alice5 and Bob5's sig
Output: Alice 0.1
3-day LockTime

HTLC Execution 1b (HE1b)
Only Bob can broadcast

Can be broadcast anytime

scriptSig: R, Alice6&Bob6's sig
Output: RSMC Alice1&Bob1 0.1
No LockTime

HTLC Timeout Revocable Delivery 1a (HTRD1a)

Only Alice can broadcast 1000
confirmations from HT1a's mined block

Alice & Bob can agree to create a spend
invalidating this with no time limitation

Input: Alice3 and Bob3's sig
Output: Alice 0.1
1000 block Relative Confirmations Lock

HTLC Execution Revocable Delivery 1b (HERD1b)

Only Bob can broadcast 1000
confirmations from HE1b's mined block

Alice & Bob can agree to create a spend
invalidating this with no time limitation

Input: Alice7 and Bob7's sig
Output: Bob 0.1
1000 block Relative Confirmations Lock

Figure 12: If Alice broadcasts C2a, then the left half will execute. If Bob broadcasts C2b, then the right half will execute. Either party may broadcast their Commitment transaction at any time. HTLC Timeout is only valid after 3 days. HTLC Executions can only be broadcast if the preimage to the hash R is known. Prior Commitments (and their dependent transactions) are not displayed for brevity.

References

- https://lightning.network/lightning-network.pdf
- https://lightning.network/lightning-network-paper.pdf

Thank you!

Haoran Qi
10/26/2018