Cerberus Channels

Incentivizing Watchtowers for Bitcoin

Zeta Avarikioti
Orfeas Thyfronitis-Litos
Roger Wattenhofer
Payment Channels
Payment Channels

Funding transaction
Payment Channels

Commitment transaction

5

4
Payment Channels

Commitment transaction

5 -- 4

2 -- 7

8 -- 1
Lightning Channels

Funding

Commitment

Dispute period

Revocation
Funding

Commitment

Dispute period
Why be a Watchtower?
Why be a Watchtower?

Assuming rational parties and watchtowers…

- Will a party commit fraud?  
  - ✖️
- Will a watchtower get paid?  
  - ✖️
- Will there be a watchtower?  
  - ✖️
- Will a party commit fraud?  
  - ✓
- Will a watchtower get paid?  
  - ✓
- Will there be a watchtower?  
  - ✓
- Will a party commit fraud?  
  - ✖️
Per-update premiums?
Per-update premiums?

Watchtower paid even if inactive!
No incentive to watch chain
Why be an active Watchtower?

Collateral!
Lightning Channels

Funding
On-chain

Commitment
(1)
Published by A

Commitment
(i)
Published by A

Commitment
(i+1)
Published by A

Revocation
Published by B, W

Alice
a

Bob
b

both
a+b

Alice
a

Bob
b

Alice
a_i

Bob
b_i

Alice
a_{i+1}

Bob
b_{i+1}

Bob
a_i
Cerberus Channels

- **Funding** (On-chain): Alice \(a\) → Bob \(b\)
- **Commitment (1)** (Published by A): both \(a+b\)
- **Commitment (i)** (Published by A): Alice \(a_i\) → Bob \(b_i\)
- **Commitment (i+1)** (Published by A): Alice \(a_{i+1}\) → Bob \(b_{i+1}\)
- **Revocation** (Published by B, W): Bob \(a_i+b_i\)
- **Penalty 1** (Published by B): Bob \(c+b_i\)
- **Penalty 2** (Published by B): Bob \(c+b_i\)
- **Collateral** (On-chain): Watchtower \(c\) → Bob & WT \(c\)
- **Reclaim** (Published by W): \(\Delta T WT\) or Bob & WT \(c\)

Alice → Bob & WT
Lightning Channels
Notation

- Multi-signatures: $\sigma_{AB}$
- Timelocks: $\Delta t$
- AND $\land$, OR $\lor$

```
#\sigma_A
\rightarrow a
\rightarrow \#\sigma_B
b
\rightarrow Transaction
\rightarrow (\sigma_A \land \Delta t) \lor \sigma_{AB}
\rightarrow a+b
```
Lightning Channels

\[ \sigma_A \land \Delta t \lor \sigma_{AB} \]

Commitment (1) Published by A

\[ \sigma_{AB} \]

Revocation Published by B, W

\[ \sigma_B \]

On-chain

Commitment (i) Published by A

\[ \sigma_B \]

\[ \sigma_B \]

Commitment (i+1) Published by A

\[ \sigma_B \]

\[ b \]

\[ a \]

\[ a \]
Cerberus Channels

Funding On-chain

Commitment (1) Published by A

σ_{AB} (σ_A \wedge \Delta t) \lor σ_{AB}

a

σ_B

b

a + b

Commitment (i) Published by A

Commitment (i+1) Published by A

σ_{AB} (σ_A \wedge \Delta t) \lor σ_{AB}

a_i

σ_B

b_i

a_{i+1}

σ_B

b_{i+1}

Revocation Published by B, W

σ_B

a_i

Collateral On-chain

Reclaim Published by W

σ_{BW}

σ_W \wedge \Delta T

σ_{BW}

c

c

T >> t
Cerberus Channels

1. Funding On-chain
   - \#\sigma_A
   - \#\sigma_B
   - a
   - b
   - \sigma_{AB}

2. Commitment (1) Published by A
   - (\sigma_A \wedge \Delta t) \lor \sigma_{AB}
   - a
   - \sigma_B
   - b
   - a + b

3. Commitment (i) Published by A
   - (\sigma_A \wedge \Delta t) \lor \sigma_{AB}
   - a_i
   - \sigma_B
   - b_i

4. Commitment (i+1) Published by A
   - (\sigma_A \wedge \Delta t) \lor \sigma_{AB}
   - a_{i+1}
   - \sigma_B
   - b_{i+1}

5. Revocation Published by B, W
   - \sigma_B
   - a_i
   - \sigma_B
   - a_i

6. Penalty 1 Published by B
   - c
   - \sigma_B
   - a_i
   - c + a_i

7. Collateral On-chain
   - \#\sigma_W
   - c
   - \sigma_{BW}

8. Reclaim Published by W
   - \sigma_W \wedge \Delta T
   - c
   - c
Cerberus Channels

Funding On-chain

Commitment (1) Published by A

Commitment (i) Published by A

Commitment (i+1) Published by A

Revocation Published by B, W

Penalty 1 Published by B

Reclaim Published by W

Collateral On-chain
Cerberus Channels

Funding On-chain

Commitment (1) Published by A

Commitment (i) Published by A

Commitment (i+1) Published by A

Revocation Published by B, W

Penalty 1 Published by B

Reclaim Published by W

Collateral On-chain

#σ_A

σ_{AB}

σ_{A\Delta t}/σ_{AB}

a

σ_B

b

#σ_B

a+b

σ_{A\Delta t}/σ_{AB}

σ_{A\Delta t}/σ_{AB}

σ_{A\Delta t}/σ_{AB}

σ_B

σ_B

σ_B

σ_B

a_i

σ_B

b_i

c_i

a_{i+1}

σ_B

b_{i+1}

c_i

c_i

#σ_W

σ_{BW}

σ_{W\Delta T}

σ_{W\Delta T}

σ_{W\Delta T}

σ_{W\Delta T}

c

c

c

c

a_i+b_i

c_i+b_i

c_i+b_i

c_i+b_i

c_i+b_i

c_i+b_i

c_i+b_i

c_i+b_i

c_i+b_i

c_i+b_i

Cerberus Channels

Funding On-chain
\[ a, b \]

Commitment (1) Published by A
\[ (\sigma_A \land \Delta t) \lor \sigma_{AB} \]
\[ a, \sigma_B \]
\[ a+b \]

Commitment (i) Published by A
\[ (\sigma_A \land \Delta t) \lor \sigma_{AB} \]
\[ a_i, \sigma_B \]
\[ b_i \]

Commitment (i+1) Published by A
\[ (\sigma_A \land \Delta t) \lor \sigma_{AB} \]
\[ a_{i+1}, \sigma_B \]
\[ b_{i+1} \]

Revocation Published by B, W
\[ \sigma_B \]
\[ a_i + b_i \]

Penalty 1 Published by B
\[ \sigma_B \]
\[ c + b_i \]

Reclaim Published by W
\[ \sigma_{BW} \]
\[ c \]

Collateral On-chain
\[ c \]
Cerberus Channels

- **Funding**
  - On-chain
  - #σ_A
  - a
  - #σ_B
  - b

- **Commitment (1)**
  - Published by A
  - σ_{AB}
  - (σ_A^Δt) ∪ σ_{AB}
  - a
  - σ_B^Δt
  - b

- **Revocation**
  - Published by B, W
  - σ_B
  - a_i + b_i

- **Commitment (i)**
  - Published by A
  - a_i
  - σ_B^Δt
  - b_i

- **Commitment (i+1)**
  - Published by A
  - a_{i+1}
  - σ_B^Δt
  - b_{i+1}

- **Penalty 1**
  - Published by B
  - σ_B
  - c + b_i

- **Collateral**
  - On-chain
  - #σ_W
  - c

- **Reclaim**
  - Published by W
  - σ_W^ΔT
  - c
Cerberus Channels

Funding On-chain

Commitment (1) Published by A

σ_{AB} \\ (σ_A \wedge Δt) \lor σ_{AB} \\ a

σ_B \wedge Δt \\ b

Commitment (i) Published by A

σ_{AB} \\ (σ_A \wedge Δt) \lor σ_{AB} \\ a_i

σ_B \wedge Δt \\ b_i

Commitment (i+1) Published by A

σ_{AB} \\ (σ_A \wedge Δt) \lor σ_{AW} \\ a_{i+1}

σ_B \wedge Δt \\ b_{i+1}

Revocation Published by B, W

σ_B \\ a_i + b_i

Penalty 1 Published by B

σ_B \\ c + b_i

Reclaim Published by W

σ_W \wedge ΔT

Collateral On-chain

σ_{BW}

c

#σ_A

a

#σ_B

b

#σ_W

c
Cerberus Channels

Funding
On-chain

Commitment (1)
Published by A

Commitment (i)
Published by A

Commitment (i+1)
Published by A

Revocation
Published by B, W

Penalty 1
Published by B

Reclaim
Published by W

Collateral
On-chain

\#σ_A
\#σ_B
\#σ_W

a
b

σ_{AB}

a + b

(σ_A^\Delta t) \lor σ_{AW}

a

σ_{AW}

σ_{BW}

σ_{BW}

σ_{BW}

(σ_B^\Delta t) \lor σ_{BW}

b

b_i

(σ_B^\Delta t) \lor σ_{BW}

b_{i+1}

σ_B

σ_B

σ_{BW}

σ_{BW}

c

c
Cerberus Channels

Funding On-chain

Commitment (1) Published by A

Commitment (i) Published by A

Commitment (i+1) Published by A

Revocation Published by B, W

Penalty 1 Published by B

Penalty 2 Published by B

Collateral On-chain

Reclaim Published by W
Cerberus Channels

- Incentive-compatible solution
- Extended offline period for channel party
- WT can withdraw the service
- Bitcoin PoC implementation

Limitations:
- Privacy
- Synchrony - Timelocks
Thank you!

Questions?