

Formalização do protocolo da segunda camada

Guilherme e Flavio

Formalizaçao de protocolos

- **Com a formalização de protocolos, é possível demonstrar teoremas relacionados a esses protocolos**
-

Objetivos

- Programar o protocolo
- A partir do código, usar ele para definir o protocolo
- Criar e provar teoremas importantes

Bibliografia

- Formalizing and Implementing Distributed Ledger Objects
<http://www.cs.ucy.ac.cy/~chryssis/pubs/AGKN2018.pdf>
- Monotonic Prefix Consistency in Distributed Systems
<https://arxiv.org/pdf/1710.09209.pdf>
- Understanding the Lightning Network
<https://bitcoinmagazine.com/articles/understanding-the-lightning-network-part-building-a-bidirectional-payment-channel-1464710791/>

Bi-Directional Payment Channel (B)

Opening transaction (recorded on blockchain)

From: Alice	5 BTC
Bob	5 BTC
Signed:	
Alice	Bob
To: Alice Bob	
10 BTC	
Required to unlock:	
Alice Sig	Bob Sig

THE CHANNEL STAYS OPEN

OR

Commitment Transaction
Alice can sign and broadcast

From: Alice Bob	10 BTC
Signed:	
Bob	
Alice Sign here:	
To: Bob	
5 BTC ✓	
Required to Unlock:	
Bob Sig	
To: Alice Bob	5 BTC
Required to Unlock:	
Bob Sig	2 🔒
or:	Alice Sig

Commitment Transaction
Bob can sign and broadcast

From: Alice Bob	10 BTC
Signed:	
Alice	
Bob Sign here:	
To: Alice	
5 BTC ✓	
Required to unlock:	
Alice Sig	
To: Alice Bob	5 BTC
Required to Unlock:	
Alice Sig	2 🔒
or:	Bob Sig

1 🔑

1000 Blocks

OR

Bob can block with

1000 Blocks

OR

Alice can block with



From: Alice Bob	5 BTC
Alice sign here:	
To: Alice	
5 BTC ✓	
Required to unlock:	
Needs Signature	

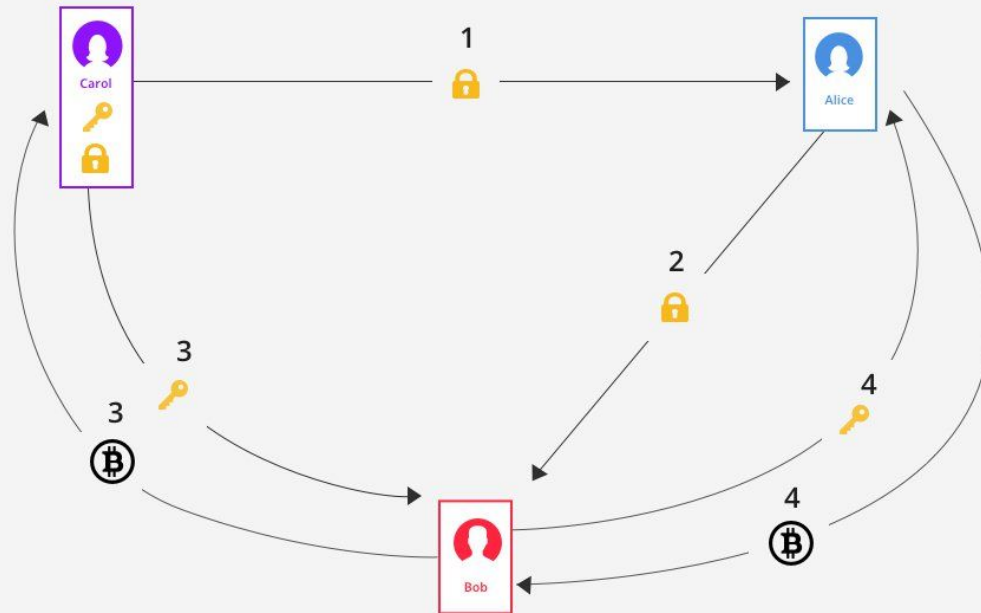
From: Alice Bob	5 BTC
Bob sign here:	
2 🔒	
To: Bob	5 BTC ✓
Required to unlock:	
Bob Sig	

From: Alice Bob	5 BTC
Bob sign here:	
To: Bob	
5 BTC ✓	
Required to unlock:	
Bob Sig	

From: Alice Bob	5 BTC
Alice sign here:	
2 🔒	
To: Alice	5 BTC ✓
Required to unlock:	
Alice Sig	

Network

 Hash  Value



Materiais

- Livros teóricos, papers, sites

Tecnologias

- Haskell
- Agda
- Criptomoedas