Demo Paper: Atomic Bonded Cross-chain Debt

Amirhossein Khajehpour§
Department of Computer Engineering
Sharif University of Technology
Tehran, Iran
amirhosseinkh@ce.sharif.edu

Fatemeh Bagheri§
Department of Computer Engineering
Sharif University of Technology
Tehran, Iran
fateme.bagheri95@student.sharif.edu

Melika Abdi
Department of Electrical Engineering
Sharif University of Technology
Tehran, Iran
melika.abdi@ee.sharif.edu

***Abstract*—Atomic Bonded Cross-chain Debt (ABCD) is the first non-custodial smart-contract-independent cross-chain atomic bond. Theoretical aspects of ABCD have been presented in the International Conference on Blockchain Technology and Applications (ICBTA) and won the best presentation award. It is the first time a demo of Atomic Bonded Cross-chain Debt is presented.**

1. Introduction

With today's surge of Decentralized Finance (DeFi), new projects appear every day to target one specific market sector. Many exploit the high trading volume of smart-contract-based blockchains [1]–[4], such as Ethereum [5], while leaving other major UTXO based networks like Bitcoin [6]. Devising new instruments to establish a connection between UTXO based networks would allow the over billions of dollars locked value on Bitcoin-like blockchains to be circulated. Several projects try to establish this connection using two different points of view. Some projects build new blockchain networks to share data between different blockchains like Cosmos [7]. However, people are looking for ways to employ existing infrastructure for executing atomic contracts between different blockchains.

Smart-contract-based blockchains support a variety of capabilities found in traditional finance, like loans and bonds and flash loans. Formulating atomic loans in UTXO-based blockchains is one way to preserve the power of these blockchains as well as smart-contract-based ones. [8]. For example, Black et al. proposed an atomic loan protocol [9] that uses Hash Time Lock Contracts (HTLCs) to offer loan position on the Ethereum while accepting collateral on the Bitcoin network. On the other hand, all the lending protocols in DeFi, only provide over-collateralized loans and flash loans. With the powerful abilities of blockchains it is regrettable if a protocol to lend under-collateralized loans with arbitrary time length is missing.

In this work, we present ABCD that is a cross-chain lending protocol between UTXO-based blockchains [10]. There is no collateral required in this protocol and repurchase time length is arbitrary. With such a powerful tool, not only all the lending abilities that are created with smart-contracts are recreated in UTXO-based blockchains, but also novel capabilities are innovated that push the edges of DeFi further away. Furthermore, ABCD only uses HTLCs that makes it fully functional for UTXO-based blockchains.

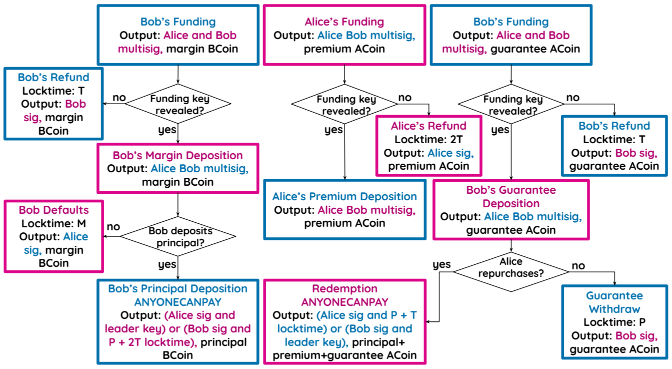
Bob's Funding
Output: Alice and Bob multisig, margin BCoin
Alice's Funding
Output: Alice Bob multisig, premium ACoin
Bob's Funding
Output: Alice and Bob multisig, guarantee ACoin
Bob's Refund
Locktime: T
Output: Bob sig, margin BCoin
no
Funding key revealed?
yes
Funding key revealed?
no
yes
Alice's Refund
Locktime: 2T
Output: Alice sig, premium ACoin
Funding key revealed?
no
yes
Bob's Refund
Locktime: T
Output: Bob sig, guarantee ACoin
Bob's Margin Deposition
Output: Alice Bob multisig, margin BCoin
Alice's Premium Deposition
Output: Alice Bob multisig, premium ACoin
Bob's Guarantee Deposition
Output: Alice Bob multisig, guarantee ACoin
Bob Defaults
Locktime: M
Output: Alice sig, margin BCoin
no
Bob deposits principal?
yes
yes
Alice repurchases?
no
Bob's Principal Deposition
ANYONECANPAY
Output: (Alice sig and leader key) or (Bob sig and P + 2T locktime), principal BCoin
Redemption
ANYONECANPAY
Output: (Alice sig and P + T locktime) or (Bob sig and leader key), principal+ premium+guarantee ACoin
Guarantee Withdraw
Locktime: P
Output: Bob sig, guarantee ACoin

Figure 1. A flowchart for the protocol. All the transactions and their output scrips are shown.

In ABCD, the seller of the bond gets some principal from the buyer, uses it for some trades, and repurchases it before a certain time. In this protocol, there is a secret on the bond buyer's principal so that the principal is not spendable until the secret is revealed by the buyer. Thus, the bond seller has to use the hash of this secret in all her trades. She can only exercise the trades when she pays her debt back, and hence the buyer reveals the secret. The seller also pays an arbitrary amount to the buyer as a premium to incentivize him. In this demo, Alice is the bond seller who borrows the principal and pays the premium, Bob is the bond buyer who lends the principal and gets the premium. Carol is the party with whom Alice makes another trade before paying Bob's principal back. Alice takes the principal from Bob in the Bitcoin testnet, performs an atomic swap with Carol between Bitcoin and Litecoin testnets, and pays Bob's principal back in Bitcoin. This is the normal way the protocol goes on. Of course, at any point, some coalition may decide to stop the procedure or intentionally deviate from the protocol in order to maximize their utility. The protocol supports situations where any set of parties behave

§. Equal contribution

978-0-7381-1420-0/21/$31.00 ©2021 IEEE

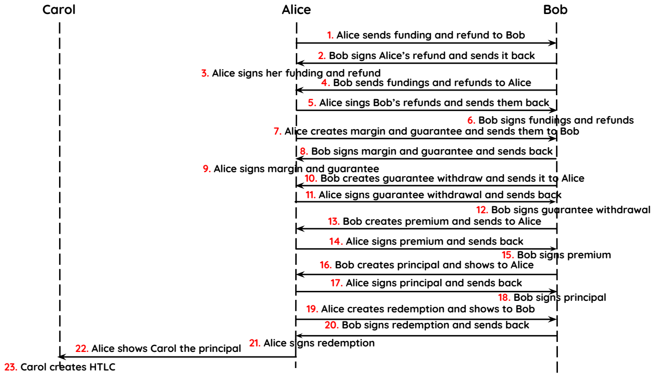
Carol
Alice
Bob
1. Alice sends funding and refund to Bob
2. Bob signs Alice's refund and sends it back
3. Alice signs her funding and refund
4. Bob sends fundings and refunds to Alice
5. Alice sings Bob's refunds and sends them back
6. Bob signs fundings and refunds
7. Alice creates margin and guarantee and sends them to Bob
8. Bob signs margin and guarantee and sends back
9. Alice signs margin and guarantee
10. Bob creates guarantee withdraw and sends it to Alice
11. Alice signs guarantee withdrawal and sends back
12. Bob signs guarantee withdrawal
13. Bob creates premium and sends to Alice
14. Alice signs premium and sends back
15. Bob signs premium
16. Bob creates principal and shows to Alice
17. Alice signs principal and sends back
18. Bob signs principal
19. Alice creates redemption and shows to Bob
20. Bob signs redemption and sends back
21. Alice signs redemption
22. Alice shows Carol the principal
23. Carol creates HTLC

Figure 2. Initialization phase

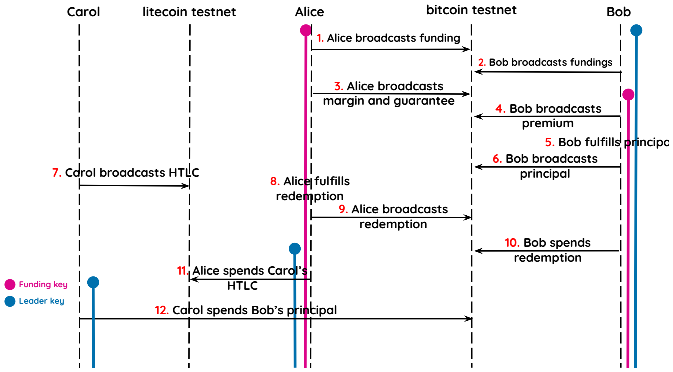
Carol
litecoin testnet
Alice
bitcoin testnet
Bob
1. Alice broadcasts funding
2. Bob broadcasts fundings
3. Alice broadcasts margin and guarantee
4. Bob broadcasts premium
5. Bob fulfills principa
6. Bob broadcasts principal
7. Carol broadcasts HTLC
8. Alice fulfills redemption
9. Alice broadcasts redemption
10. Bob spends redemption
11. Alice spends Carol's HTLC
12. Carol spends Bob's principal
● Funding key
● Leader key

Figure 3. Commitment phase. Pink and blue bars indicate which party is aware of which secret and when.

abnormally. If Bob defaults, he will be punished by losing his margin. If either Alice or Carol defaults, Bob will gain the premium anyway. Finally, if Alice and Carol adhere to the protocol, and Bob avoids unlocking the principal, then Alice can punish Bob by acquiring Bob's guarantee amount.

2. Transactions

Fig. 1 shows the flow of the protocol and all the transactions. Transactions included in the ABCD are the followings:

- Funding: There are three funding transactions, one for Alice and two for Bob. In order to spend the funding transactions, either the *funding key* has to be revealed or a certain amount of time has to be passed. The former represents the normal case, while the latter happens if Alice does not reveal the key.
- Refund: In case of any abnormal action from the other party, each party can use the refund to take the funding amount back.
- Margin Deposition and Guarantee Deposition: Using these transactions Alice moves Bob's fundings amount to the next step and also reveals the funding key. After confirming margin deposition and guarantee deposition transactions, Bob's refund transactions no longer work.
- Premium Deposition: When Alice reveals the funding key, Bob broadcasts this transaction to pay the premium to himself and both parties go to the next stage.
- Redemption: This transaction is used for Alice to repurchase the bond. This is an any-one-can-pay transaction which means at the time of creating, not all the inputs need to be clear. Alice can later fulfill the transaction and pay her debt back.
- Bob's Principal Deposition: Bob has to broadcast this transaction before M locktime. By doing this, he is lending the principal to Alice. This transaction can not be spent without knowing the *leader key*. So, Bob does not reveal it until Alice has broadcast the redemption transaction.
- Bob Defaults: If Bob does not deposit the principal before M locktime, Alice will take his margin as a punishment using this transaction.
- Guarantee Withdrawal: If Alice repurchases the bond within the expected time and Bob does not reveal the leader key, then Alice can punish Bob by spending the guarantee amount on the repurchase transaction to herself. Otherwise, Bob can pay the guarantee value back to himself using the guarantee withdrawal transaction.

3. Protocol

The protocol of ABCD consists of two phases, initialization, and commitment.

Initialization Phase: In this phase, the parties create transactions, exchange, and sign them. So, they make sure no one has the chance to cheat on the other. Fig. 2 is an illustration of this phase.

Commitment Phase: In this phase, they broadcast the transactions created in the previous phase dependent on whether they wish to abort everything or continue normally. Fig. 3 shows the steps of this phase in the case that no one defaults. Abnormal cases can occur in cases such as: 1) Alice does not broadcast her funding. 2) Alice broadcasts the refund instead of margin and Bob would do likewise. 3) Bob does not deposit the principal before the M locktime, so Alice broadcasting the Bob defaults transaction would take his margin. 4) Alice does not fulfill the redemption before the P locktime, then Bob would take his margin and guarantee back, and he would not reveal the leader key.

4. Conclusion

In this article, we run an instance of ABCD on Bitcoin testnet and perform a simple atomic swap with the debt and Litecoin testnet tokens. The reference to the implementation of different scenarios of ABCD is accessible in ABCD official github page https://github.com/incentivus/abcd.

References

[1] H. Adams, N. Zinsmeister, and D. Robinson, "Uniswap v2 core," *URl: https://uniswap. org/whitepaper. pdf*, 2020.

[2] “The money market protocol.” https://aave.com. Accessed: 2020.08.22.

[3] “A better money.” https://makerdao.com. Accessed: 2020.08.22.

[4] “Compound is an algorithmic, autonomous interest rate protocol built for developers, to unlock a universe of open financial applications..” https://compound.finance. Accessed: 2020.08.22.

[5] V. Buterin *et al.*, “A next-generation smart contract and decentralized application platform,” *white paper*, vol. 3, no. 37, 2014.

[6] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” tech. rep., Manubot, 2019.

[7] J. Kwon and E. Buchman, “A network of distributed ledgers,” *Cosmos, dated*, pp. 1–41, 2018.

[8] M. Tefagh, F. Bagheri, A. Khajehpour, and M. Abdi, “Capital-free futures arbitrage,” 2020.

[9] M. Black, T. Liu, and T. Cai, “Atomic loans: Cryptocurrency debt instruments,” *arXiv preprint arXiv:1901.05117*, 2019.

[10] M. Tefagh, F. Bagheri, A. Khajehpour, and M. Abdi, “Atomic bonded cross-chain debt,” 2020.