

Ministry of Education and Science of Ukraine  
NATIONAL UNIVERSITY OF KYIV-MOHYLA ACADEMY  
Department of Informatics of the Faculty of Informatics



**Creation of an atomic cross-chain escrow, which supports EVM, Solana and  
TON**

**Volodymyr Rastiehaiev**

Thesis supervisor - Kyrylo Gorokhovskiyi

# Terms

- Escrow is a financial arrangement where a third party holds and manages assets or funds on behalf of two parties involved in a transaction, releasing them only when agreed-upon conditions are met.
- Atomic escrow is a type of escrow mechanism that ensures a transaction between parties is completed entirely or not at all.

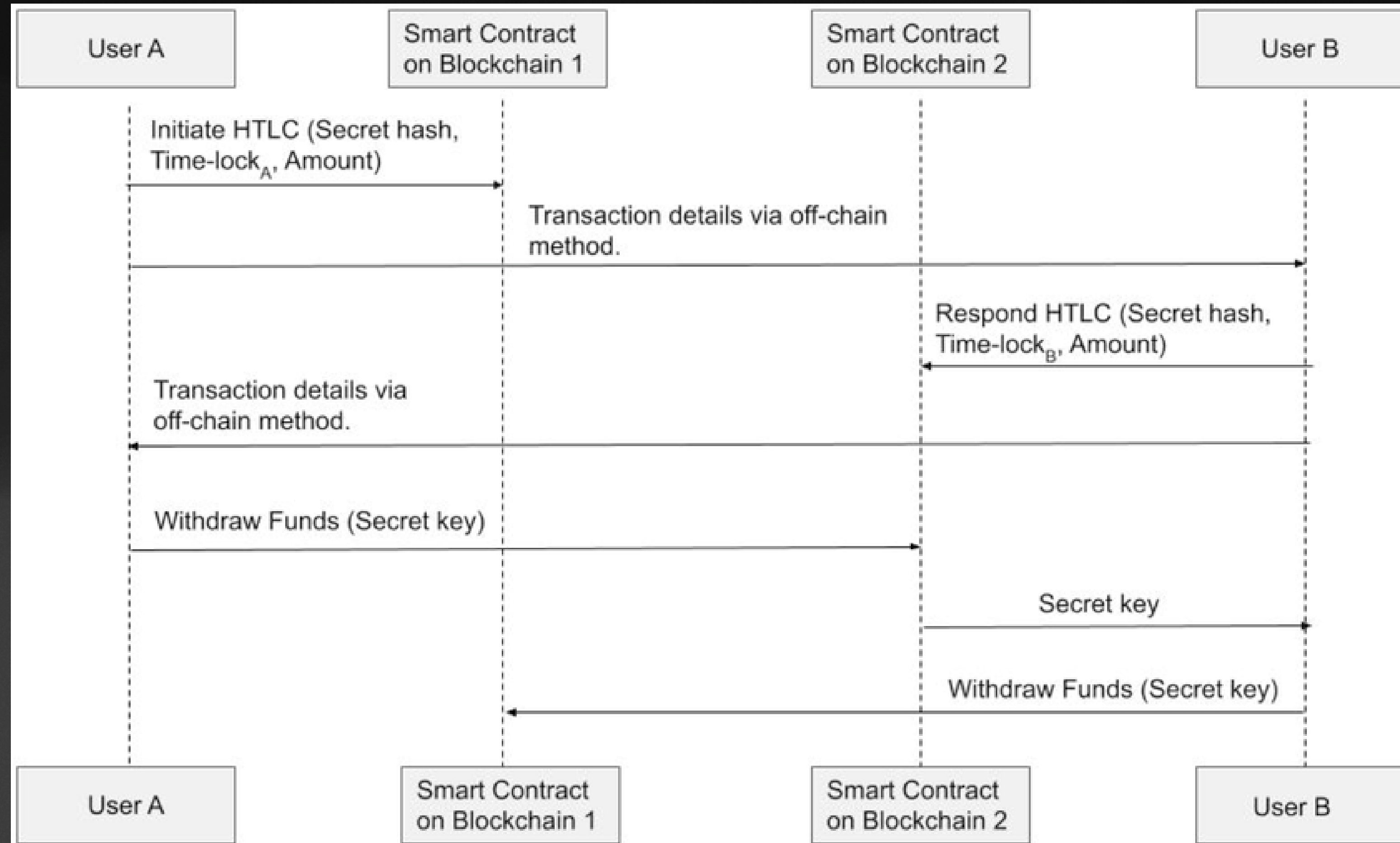
# Objectives

- Addresses the interoperability issue.
- Research approaches.
- Create an HTLC-based atomic cross-chain escrow for Solana, TON and EVM.
- Develop contracts for all mentioned blockchains.

# What is HTLC?

- HTLC (Hashed TimeLock Contract) is a smart contract used to enable secure, time-bound transactions between untrusted parties. It requires the receiver to provide a cryptographic proof (a hash) within a specified time to claim the funds. If the proof isn't provided in time, the sender can reclaim the funds.

# HTLC diagram



HTLC sequence diagram

# EVM

- EVM has two main types of accounts:
  - Externally Owned Accounts (EOA) – Controlled by private keys, used by users to send transactions and hold ETH or tokens.
  - Contract Accounts – Controlled by code, execute logic when triggered by transactions or messages.
- Smart contracts store both code and state on EVM.

# Solana

- In Solana, accounts store data and are central to the execution of programs.
- There are two main types of accounts:
  - Data Accounts - These store persistent data and are used by programs to maintain state.
  - Program Accounts - These contain the compiled executable code and are marked as executable.
- On Solana, programs are stateless and require accounts that store state to be passed on invoke.



# TON

- In TON, everything is a smart contract with its own code and persistent data.
- Unlike Solana and EVM, TON is asynchronous:
  - Actor Model: Each smart contract is an independent actor that communicates via messages, similar to concurrent systems.
  - Contracts execute only when they receive messages. All communication between contracts is asynchronous, enabling parallelism but making it important for developer to think about contracts interactions and architecture.

# Technologies used

- For hashing algorithm, keccak256 was chosen as it is available in all of three blockchains and is needed to achieve compatibility with EVM.
- EVM:
  - Solidity language for smart contracts
  - Hardhat js framework for testing & deploying
- Solana:
  - Rust language for smart contracts & testing
  - Solana-sdk library for deploying smart contracts & blockchain interactions
  - Litesvm library for smart contract testing
- TON:
  - Tolk language for smart contracts
  - Blueprint js framework for testing & deployment

# EVM

 **TRANSACTION ACTION**  
Transfer 0.02  WETH to 0x492e07e261b155948e42E5C3BC24F8c63FbEeD9A

[ This is a Sepolia **Testnet** transaction only ]

**Transaction Hash:** 0x82897e73aa781cc2cc3adc198b8e8e75b93cf6f7ecea4b379ea2a54e91652baa [🔗](#)

**Status:** Success


**Block:** 8414844 12306 Block Confirmations


**Timestamp:** 41 hrs ago (May-27-2025 03:21:00 AM UTC)

**From:** 0x4491E8cB85C4EF5bAA91011af966c53b9305241 [🔗](#)

**Interacted With (To):** [📄](#) 0x492e07e261b155948e42E5C3BC24F8c63FbEeD9A [🔗](#) ✓

**ERC-20 Tokens Transferred:** All Transfers Net Transfers

▶ **From** 0x4491E8cB...3b9305241 [🔗](#) **To** 0x492e07e2...63FbEeD9A [🔗](#) **For** 0.02  ERC-20: Wrapped Ethe... (WETH) [🔗](#)

**Value:**  0 ETH



**Transaction Fee:** 0.000000331125206542 ETH

**Gas Price:** 0.001725698 Gwei (0.000000000001725698 ETH)

createTrade transaction on Sepolia testnet

2025

# EVM

 **TRANSACTION ACTION**  
Transfer 0.02  WETH to 0x01e154E74bf881fe9ABD8aB8b6628cDa92b164f7

[ This is a Sepolia **Testnet** transaction only ]

**Transaction Hash:** 0xe2498851a496c692974817d79a0bc83996babf63dafff3e0dcb5c38f7102293f [🔗](#)

**Status:** Success


**Block:** 8414921 12252 Block Confirmations


**Timestamp:** 40 hrs ago (May-27-2025 03:36:36 AM UTC)

**From:** 0x01e154E74bf881fe9ABD8aB8b6628cDa92b164f7 [🔗](#)

**Interacted With (To):** [0x492e07e261b155948e42E5C3BC24F8c63FbEeD9A](#) [🔗](#) ✓

**ERC-20 Tokens Transferred:** All Transfers Net Transfers

▶ **From** [0x492e07e2...63FbEeD9A](#) [🔗](#) **To** [0x01e154E7...a92b164f7](#) [🔗](#) **For** 0.02  ERC-20: Wrapped Ethe... (WETH) [🔗](#)

**Value:**  0 ETH



**Transaction Fee:** 0.000156233554175125 ETH

**Gas Price:** 1.500442297 Gwei (0.000000001500442297 ETH)

Withdraw transaction on Sepolia testnet

2025

# EVM

 **TRANSACTION ACTION**  
Transfer 0.02  WETH to 0x4491E8cB85C4EF5bAAAd91011af966c53b9305241

[ This is a Sepolia **Testnet** transaction only ]

Transaction Hash: 0x1c1044bdab34a75bee14bea9cf9b1cd2e2de5b0f7c10432baf9fc80df8f78734 [🔗](#)

Status: Success


Block: 8414831 12350 Block Confirmations


Timestamp: 41 hrs ago (May-27-2025 03:18:24 AM UTC)

From: 0x4491E8cB85C4EF5bAAAd91011af966c53b9305241 [🔗](#)

Interacted With (To): 0x492e07e261b155948e42E5C3BC24F8c63FbEeD9A [🔗](#) ✓

ERC-20 Tokens Transferred: All Transfers Net Transfers

▶ From 0x492e07e2...63FbEeD9A [🔗](#) To 0x4491E8cB...3b9305241 [🔗](#) For 0.02  ERC-20: Wrapped Ethe... (WETH) [🔗](#)

Value:  0 ETH

Transaction Fee: 0.000000136001204353 ETH

Gas Price: 0.001675903 Gwei (0.0000000000001675903 ETH)

Refund transaction on Sepolia testnet

2025

# Solana

The screenshot displays a transaction details page for a Solana transaction. The transaction ID is 3wjXay4zp5224axcqiWkeQJcFDBF3eN2EAb8wQqwcfyS5CQUecoPfBb3vd7zZHRs5XLeX5jq3xF2C89ANcNiwomr. The transaction is confirmed as successful with 'Finalized (MAX Confirmations)' and occurred 2 days ago on May 27, 2025, at 03:26:53 +UTC. The transaction actions include interacting with a program, creating two accounts (one with SOL and one with WSOL), and transferring WSOL. The fee is 0.000005 SOL, and 42,839 compute units were consumed. The transaction version is Legacy, and the previous block hash is B6NsjPi9wCBinYBRpk5ae2SZUw9W1TYCKBkgEma4eTc.

Signature	3wjXay4zp5224axcqiWkeQJcFDBF3eN2EAb8wQqwcfyS5CQUecoPfBb3vd7zZHRs5XLeX5jq3xF2C89ANcNiwomr	<a href="#">Inspect Tx</a>
Block & Timestamp	383573026   2 days ago   May 27, 2025 03:26:53 +UTC	
Result	<span>SUCCESS</span>   Finalized (MAX Confirmations)	
Signer	7YP2mhv2BYcGLetxfm73q82fJN6JeeGRfgv7WofhJ1pP	
Transaction Actions	<a href="#">Tx Maps</a> <b>Legacy Mode</b> <span>View Token Account</span>	
<p>Interact with program <a href="#">4Sv5bD...mzeP6Y</a></p> <p>Create <a href="#">CrxW4A...ovfgC9</a> with deposit of <b>0.00195576 SOL</b> from <a href="#">7YP2mh...fhJ1pP</a></p> <p>Create <a href="#">BrREBy...YBnnAH</a> with deposit of <b>0.00203928 SOL</b> from <a href="#">7YP2mh...fhJ1pP</a></p> <p>Transfer from <a href="#">7YP2mh...fhJ1pP</a> to <a href="#">CrxW4A...ovfgC9</a> for <b>0.03 WSOL</b></p>		
Sponsored		
Fee	0.000005 SOL	
Compute Units Consumed	42,839	
Transaction Version	Legacy	
Previous Block Hash	B6NsjPi9wCBinYBRpk5ae2SZUw9W1TYCKBkgEma4eTc	

Deposit transaction on Solana devnet

2025

# Solana

The screenshot displays a transaction details page for a Solana transaction. The transaction is successful and finalized with maximum confirmations. It shows a transfer of 0.03 WSOL from one account to another. The page includes various metadata such as the signature, block number, timestamp, and transaction fee.

Signature	5BTZdbJjA4bFzGTC6H3GCxk2QotoySN74w5vj17RxdHta11BMr7m3qES3sParPLbB6ef6SDSRn5PkFfCyGbdxeXq	<a href="#">Inspect Tx</a>
Block & Timestamp	383573318   2 days ago   May 27, 2025 03:28:49 +UTC	
Result	<span>SUCCESS</span>   Finalized (MAX Confirmations)	
Signer	73kdhJo2TCpNu7ftkCjHLcnaVdH2FteZWLoGXCDUfsQJ	
Transaction Actions	<span>Legacy Mode</span> <span>Summary Mode</span> <span>View Token Account</span>	
	<a href="#">Tx Maps</a>	
	<p>Interact with program <a href="#">4Sv5bD...mzeP6Y</a></p> <p>Transfer from <a href="#">CrxW4A...ovfgC9</a> to <a href="#">73kdhJ...DUfsQJ</a> for <b>0.03</b> WSOL</p>	
Sponsored		
Fee	0.000005 SOL	
Compute Units Consumed	32,201	
Transaction Version	Legacy	
Previous Block Hash	Hdpf4d9aMCCsZcStsQYHdNodiLNmdnYqLmh4Bg4FyXBw	

Withdraw transaction on Solana devnet

2025

# TON

Event overview **Transactions tree** Value flow

(A) Account: <a href="#">0QDdwv7...PeCMeAvk</a>	Interfaces: <code>wallet_v4r2</code>	Hash: <code>f9a28d7b...ca11ffe5</code>	LT: <code>35077726000001</code>
Value: <b>0 TON</b>	Bounce: <code>false</code>	Bounced: <code>false</code>	Total Fees: <b>0.00634165 TON</b> <a href="#">Raw body</a> <span>More ▾</span>
(B) Account: <a href="#">kQAVdN7T...eKwtDwwe</a> Exit code: <code>0</code>	Interfaces: <code>-</code> Status: <code>nonexist → active</code>	Hash: <code>889b1e95...ec881b9a</code> Type: <code>TransOrd</code>	LT: <code>35077729000001</code>
Value: <b>0.05 TON</b>	Bounce: <code>true</code>	Bounced: <code>false</code>	Total Fees: <b>0.0002864 TON</b> <span>More ▾</span>

Event overview **Transactions tree** Value flow

Action	Route	Payload	Value
Transfer token	<a href="#">0QDz...L5DK</a> → <a href="#">kQAV...Dwwe</a>	-	<b>0.05 NNOT</b>
Contract deploy	<a href="#">kQctfylZ...0Hj-LIGL</a>	Interfaces: <code>[jetton_wallet_v2]</code>	-

```
graph LR; A((A)) -- "0.05 TON  
Jetton Transfer" --> B((B)); B -- "0.04533 TON  
Jetton Internal Tr..." --> C((C)); C -- "0.000000001 TON  
Jetton Notify" --> D((D)); C -- "0.034190386 TON  
Excess" --> A;
```

Contract deploy & deposit on TON testnet

2025

# TON

Event overview	Transactions tree	Value flow	
</> Call Contract	0QBe...gSKL → kQAV...Dwwe	0x013a3ca6	0.02 TON
☰ Transfer token	kQAV...Dwwe → 0QBe...gSKL	-	0.05 NNOT
</> Contract deploy	kQB5c7ce...5UWK7M5v	Interfaces: [jetton_wallet_v2]	-

```
graph LR; A((A)) -- "0.02 TON  
0x013a3ca6" --> B((B)); B -- "0.066665167 TON  
Jetton Transfer" --> C((C)); C -- "0.061998367 TON  
Jetton Internal Tr..." --> D((D)); D -- "0.052347954 TON  
Excess" --> A2((A))
```

Event overview	Transactions tree	Value flow	
Account		Balance change	NNOT
(A) 0QBeRNWx...Zv5fgSKL		+0.028563072 TON	0.05 NNOT
(B) kQAVdN7T...eKwtDwwe		-0.04971358 TON	-0.05 NNOT

Withdraw on TON testnet

2025

# Conclusion

- Traditional methods often of cross-chain escrow often rely on trusted intermediaries or complex bridging mechanisms, introducing points of failure and security vulnerabilities.
- This work addressed this challenge by focusing on the design, development, and evaluation of an atomic cross-chain escrow system.
- As a result, the system was implemented to support specifically EVM, Solana and TON.
- This work successfully demonstrated the technical feasibility of such a system, providing a functional and evaluated solution.

**Thanks for your attention**