



TON 跨链桥架构思考

Speaker: Kojh Liang (Head of Research at Kenetic Capital)



1.跨链桥

跨链桥是一种链间的连接，允许资产从一个链转移到另一个链或兑换成另一个链的某个资产。

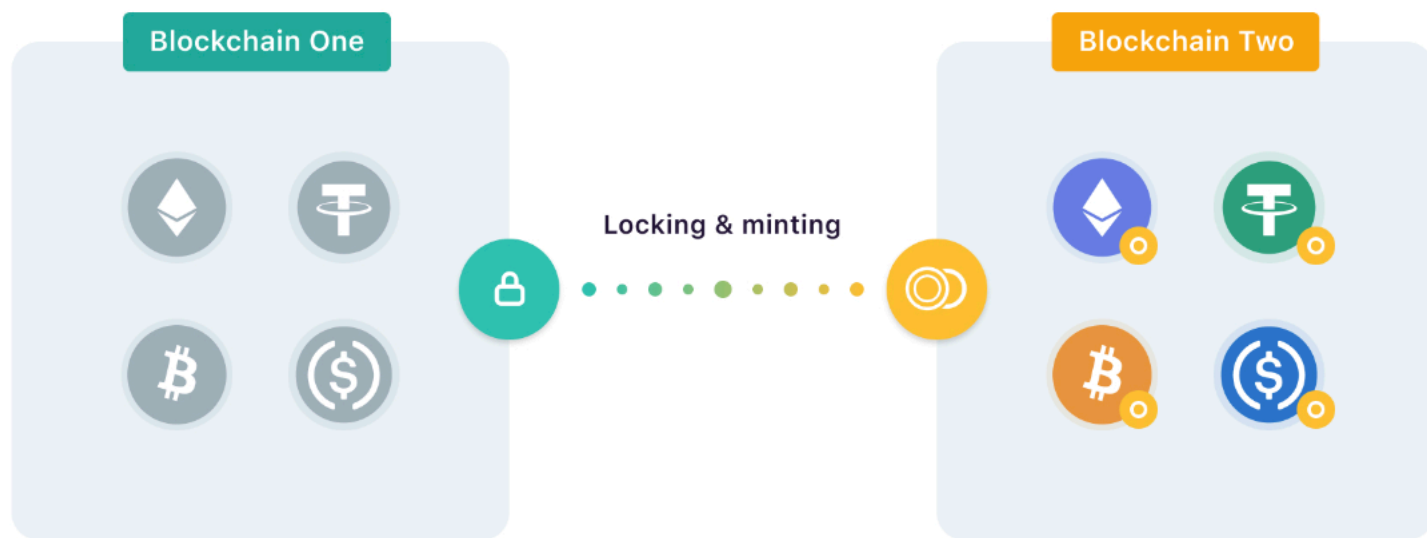
跨链桥的类别：

1.官方跨链桥（Layer2/Layer1）：比如[Optimism bridge](#)、[Arbitrum bridge](#)、[zkSync bridge](#)、[TON bridge](#)等

2.第三方跨链桥/协议：为不同的链并充当中间人网络/验证者以支持更多链的跨链。


比如基于[Wormhole](#)协议的[allbridge](#)、基于[LayerZero](#) 协议的[stargate.finance](#)等

3.企业级跨链桥/协议：为用户提供更完善的跨链转移资产， DEX跨链Swap等功能， 比如 [Li.Fi](#)等



2.目前TON的跨链桥应用


官方跨链桥：<https://bridge.ton.org> 支持Ethereum、BNB chain和TON的Token转移


 **TON App**

Jettons NEW

Categories

Use ▼

 Log In




En

Home > Bridges

Bridges 7


Transfer crypto assets between chains. Connect TON to other blockchains effortlessly with bridge apps. Explore interoperability solutions that allow you to move assets between different blockchains, expanding your options and enabling smoother interactions across ecosystems.



TON ↔ BSC

BSC exchanging bridge


1



TON ↔ ETH

TON - WTON exchanging bridge


2



Cede.store

Access and transfer your assets fro...


3



Orbit Bridge

Orbit Bridge: Fast and secure way for...


4



XP.NETWORK

Multichain NFT Bridge


5



Rubic

Rubic is a Cross-Chain Tech...

6



Tonbridge

Tonsbridge , best aggregator of...

7

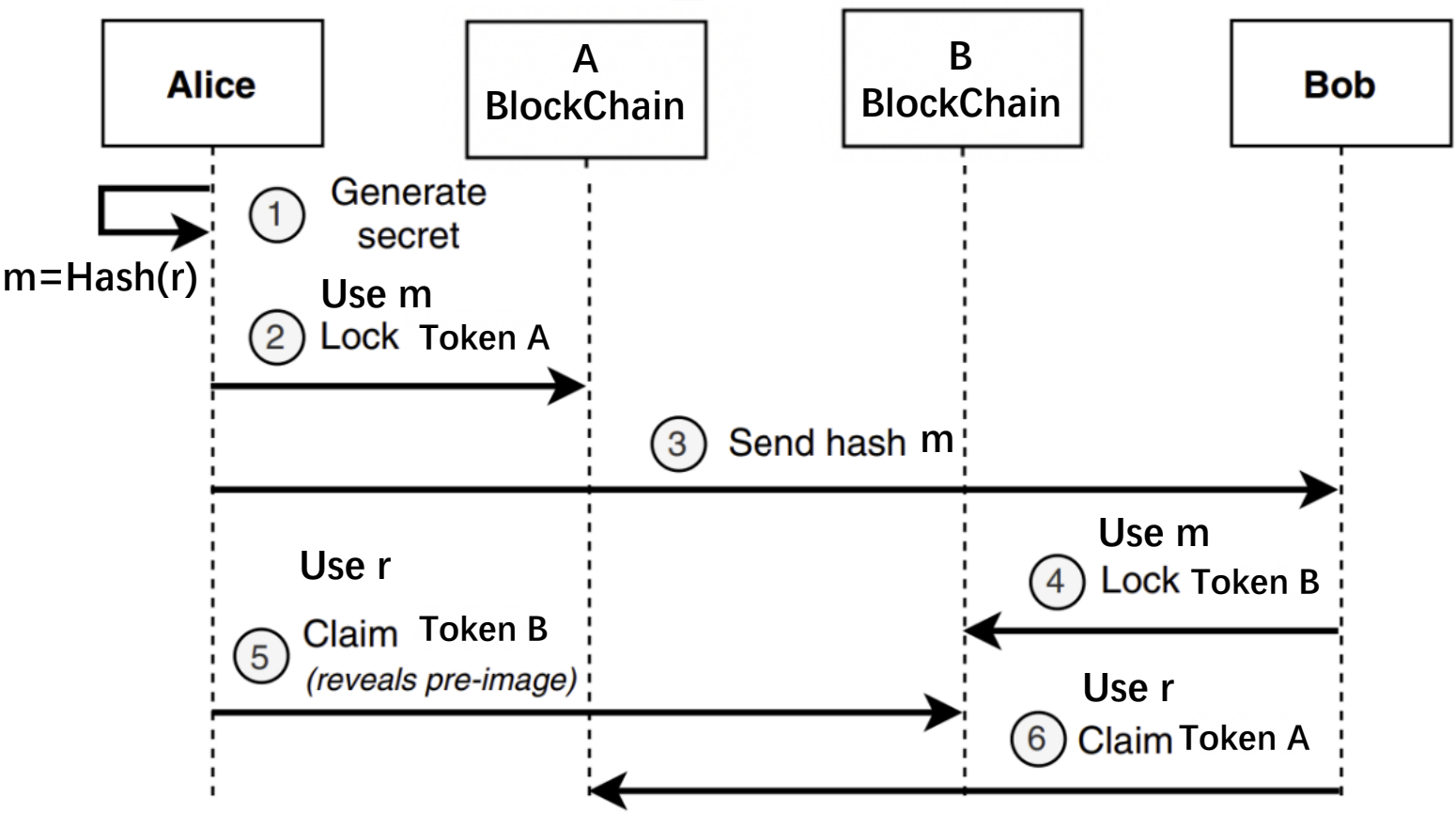
2.跨链桥的实现方案

方案1：原子交换 Atomic swaps

当用户 A 有跨链需求，跨链桥会在目标链上撮合/ 寻找另一个用户 B 的对应相反的需求，双方进行点对点匹配，以及资产的交换，当中用了哈希时间锁（HTLC）的方法实现，同时保障资金的安全性。

优点：无需第三方中介，安全性高。

缺点：成本高，每次交易需部署一个合约；难以撮合，未必可以很快找到足够流动性的对手方



交换流程：

- 1.用户 Alice 生成随机密码 r ，并计算出 r 的哈希值 $m = \text{hash}(r)$ ，将 m 值发给用户 Bob
- 2.用户 Alice 发起一笔有条件的交易，向用户 Bob 转 1 token A，须用户 B 在预设的时间出示密码 r 才能成功，否则交易自动失败
- 3.用户 Bob发起一笔有条件的交易，向用户 Alice转 1 token B，须用户 Alice 在预设的时间出示密码 r 才能成功，否则交易自动失败（
4. Alice出示密码 r 接收 1 token B，同时 Bob获得Alice出示的密码 r ，可以获取 1 token A

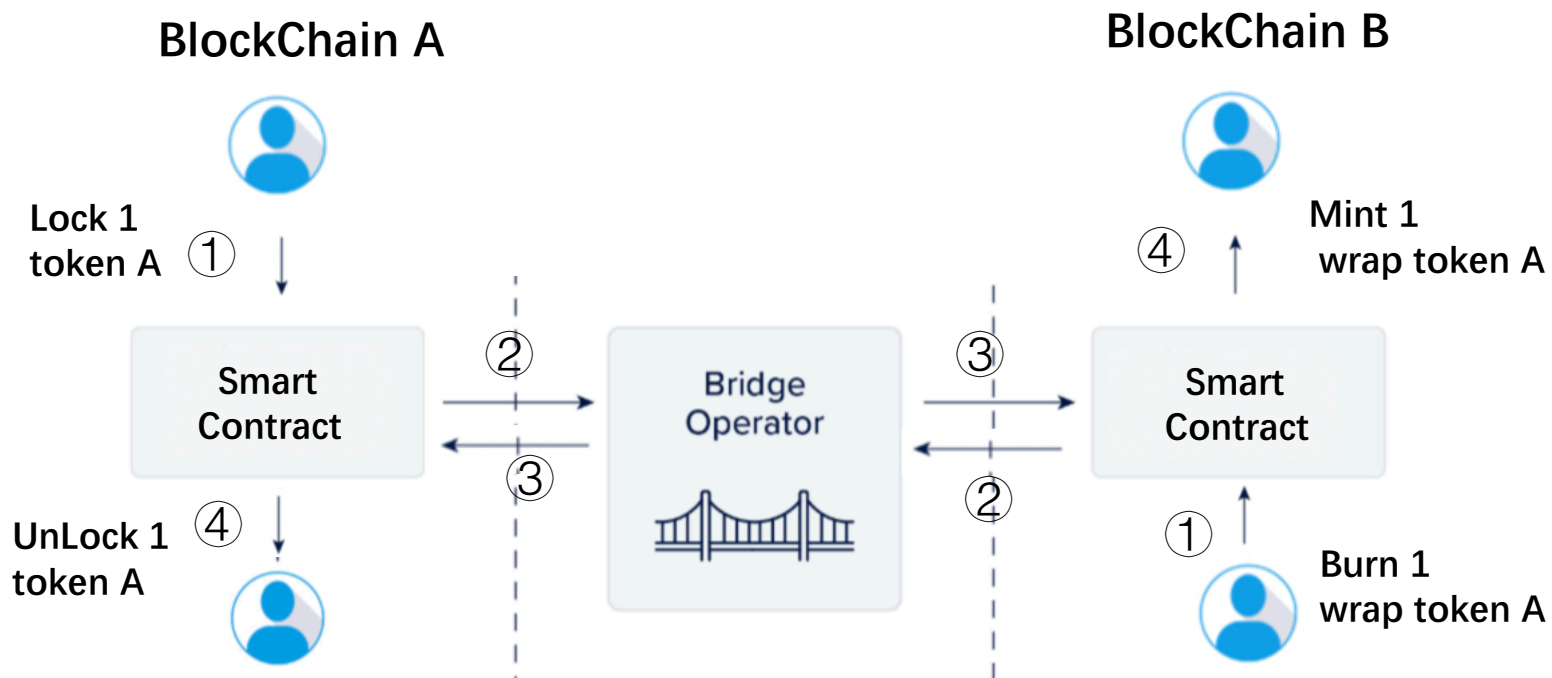
2.跨链桥的实现方案

方案2：锁定/解锁 + 铸造/销毁 Lock/unlock + Mint/ Burn

跨链桥在原链锁定/解锁用户资产，并在在目标链铸造/销毁等量的代币并转移到用户在目标链的账户中，进而完成资产价值的跨链转移。（常见于Layer2项目的跨链桥）

优点：无需提供流动性的对手方

缺点：安全性依赖网络验证节点，如验证节点作恶或被黑客控制，容易造成资产损失；
存在超发超过锁定资产的Token的风险；存在管理员提现所有跨链桥锁定资产的风险



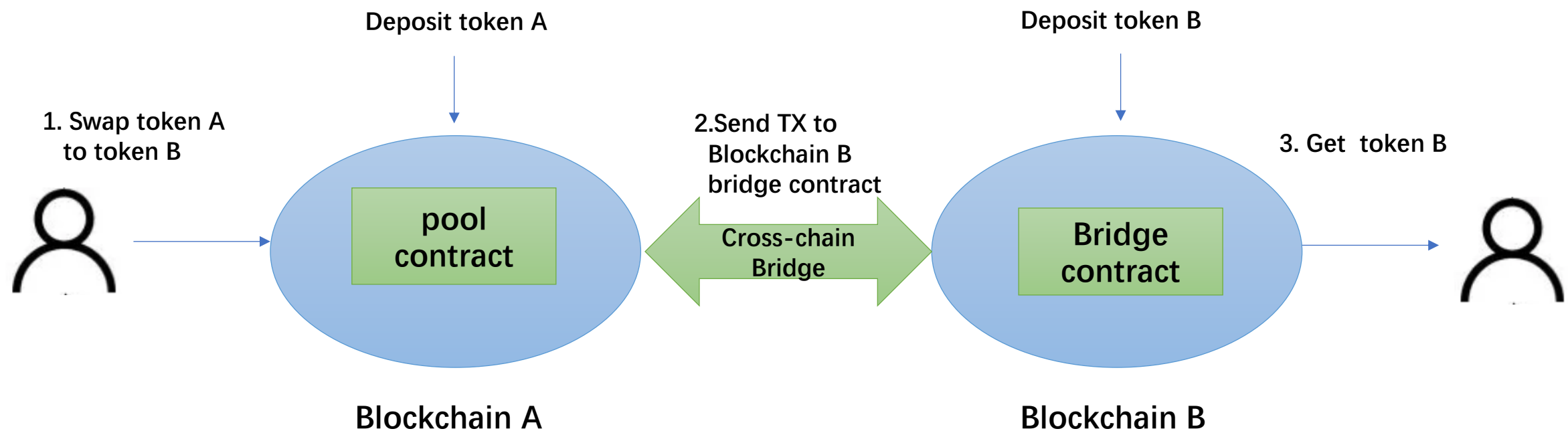
2.跨链桥的实现方案

方案3：流动性置换 *Liquidity pool*

项目方在源链和目标链部署跨链桥合约，建立流动性资金池，支持用户Swap源链的token A到目标链的token B。

优点：项目方和用户共同提供流动性资金池

缺点：安全性依赖项目方的跨链桥合约，如果合约存在漏洞，有损失资产风险；另外流动性池可能存在深度不足的问题



3.跨链桥实现例子 – TON/EVM 跨链桥 (Lock/unlock + Mint/ Burn)

功能： swap TON to WTON(ERC20) token /Swap WTON(ERC20) token to TON

需要考虑的兼容性问题：

1.地址格式： TON地址 和EVM地址

2.签名方案： TON： ED25519 EVM： ECDSA

3.智能合约语言： TON： FunC/Tact EVM： solidity

4.资产标准： TON： Jetton(TEP74)、 NFT(TEP62) EVM： ERC20 、 ERC721

5.Gas fee： TON 、 ETH

核心模块：

1.TON侧 bridge合约： ton_bridge.fc

2.EVM侧bridge合约： evm_bridge.sol

3.Bridge service:

监听TON区块链bridge合约的交易消息，根据不同的操作，发送相应的交易到EVM侧bridge合约

监听EVM区块链bridge合约的交易事件，根据不同的事件，发送相应的交易到TON侧bridge合约

3.跨链桥实现例子 – TON/EVM 跨链桥 (ton_bridge 合约示例代码)

```
() recv_internal(int msg_value, cell in_msg_cell, slice in_msg) impure {
    int op = in_msg~load_uint(32);
    if (op == op::lock_ton()) {
        int destination_address = in_msg~load_uint(160); ;;ETH address
        int amount = in_msg~load_coins();
        lock_ton(sender_address, destination_address, amount);
        return ();
    }
}

() recv_external(slice in_msg) impure {
    var signature = in_msg~load_bits(512);
    var in_msg_body_cell = in_msg~load_ref();

    throw_unless(35, check_signature(cell_hash(in_msg_body_cell), signature, public_key));
    accept_message();
    var msg_body = in_msg_body_cell.begin_parse();
    int op = msg_body~load_uint(32);

    if (op == op::unlock_ton()) {
        slice destination_address = in_msg~load_msg_addr(); ;;TON address
        int amount = in_msg~load_coins();
        unlock_ton(sender_address, destination_address, amount);
        return ();
    }
}
```


3.跨链桥实现例子 – TON/EVM 跨链桥 (evm_bridge 合约示例代码)

```
contract Evm_Bridge is ERC20, Ownable {
    constructor(address initialOwner)
    |   ERC20("wTON", "wTON")
    |   Ownable(initialOwner)
    {}

    function mint(address to, uint256 amount) public onlyOwner {
    |   _mint(to, amount);
    }

    function burn(uint256 value) public {
    |   _burn(msg.sender, value);
    }
}
```

3.跨链桥实现例子 – TON/EVM 跨链桥 (Lock/unlock + Mint/ Burn)

调用流程：

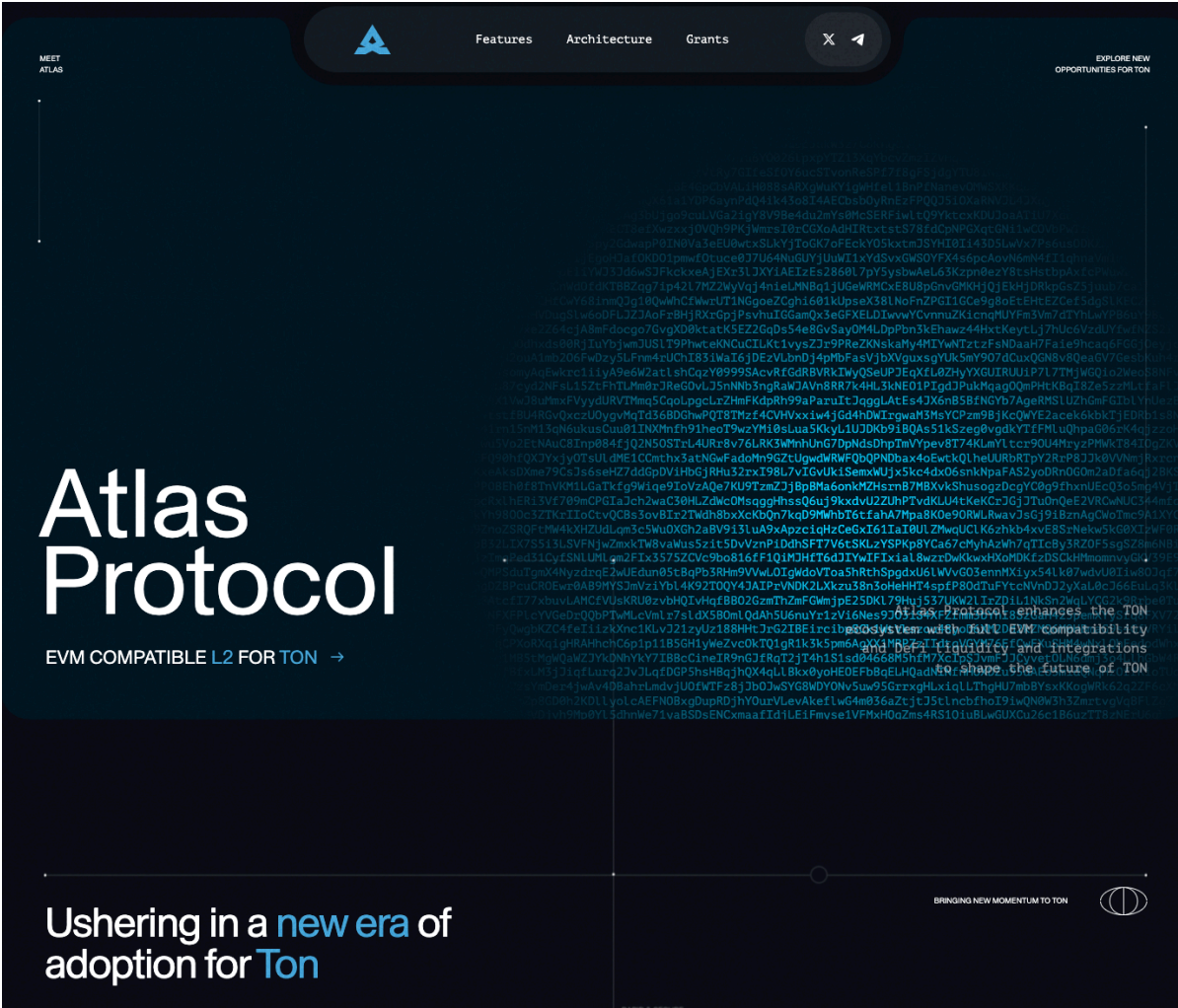
1.Swap TON to WTON

- (1) 用户把TON发送到ton_bridge合约 (InternalMessage)
- (2) 跨链桥监听到Ton_bridge合约的lock_ton消息
- (3) 跨链桥使用管理员地址调用evm_bridge合约的mint方法
- (4) evm_bridge合约mint相应数量的WTON到用户的EVM钱包地址

2.Swap WTON to TON

- (1) 用户调用evm_bridge合约的burn方法， burn掉一定数量的WTON
- (2) 跨链桥监听到evm_bridge合约发出的burn wTON事件
- (3) 由跨链桥使用管理员私钥签名消息， 发送unlock_ton消息到ton_bridge合约 (ExternalMessage)
- (4) ton_bridge合约unlock相应数量的TON到用户的TON钱包地址

Atlas Protocol



<https://www.atl.network>

Network name

Atlas Testnet

New RPC URL

<https://rpc.testnet.atl.network/>

Chain ID ⓘ

622463

Currency symbol

TON

Ticker symbol verification data is currently unavailable, make sure that the symbol you have entered is correct. It will impact the conversion rates that you see for this network


Block explorer URL (Optional)

<https://explorer.testnet.atl.network/>

Atlas Testnet network config

Atlas Protocol

<https://faucet.testnet.atl.network>




Connect Wallet

TON Atlas faucet:
fast & reliable.


Simply sign into use any wallet, enter your wallet address, and hit «Send me TON».

Enter Wallet Address

 0.01
\$TON per hour

Connect wallet

<https://bridge.testnet.atl.network>




Connect Wallet

Bridge


History

From



Connect your wallet

To

 Atlas Network

☐ Receive TON to another wallet

Connect EVM Wallet



TON Layer2 交流群(微信)



Thanks!

TRC404 Twitter

https://x.com/ton_trc404



(Use



to scan)