한 번에 끝내는
블록체인 개발 A to Z

Chapter 3

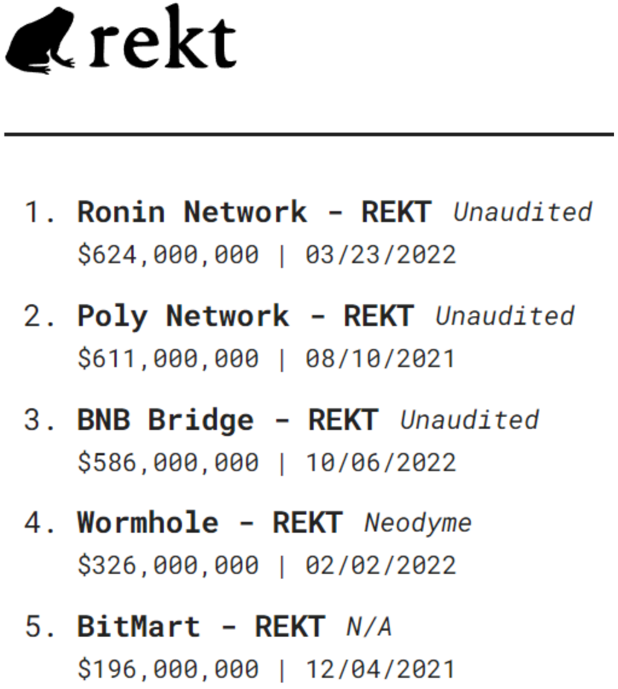
이종 블록체인간 연결하기

Chapter 3 이종 블록체인간 연결하기

Bridge 보안

Crypto Exploit

- 이종 블록체인간 자산 이동 중 발생
  - Bridge
  - Layer2
  - ...



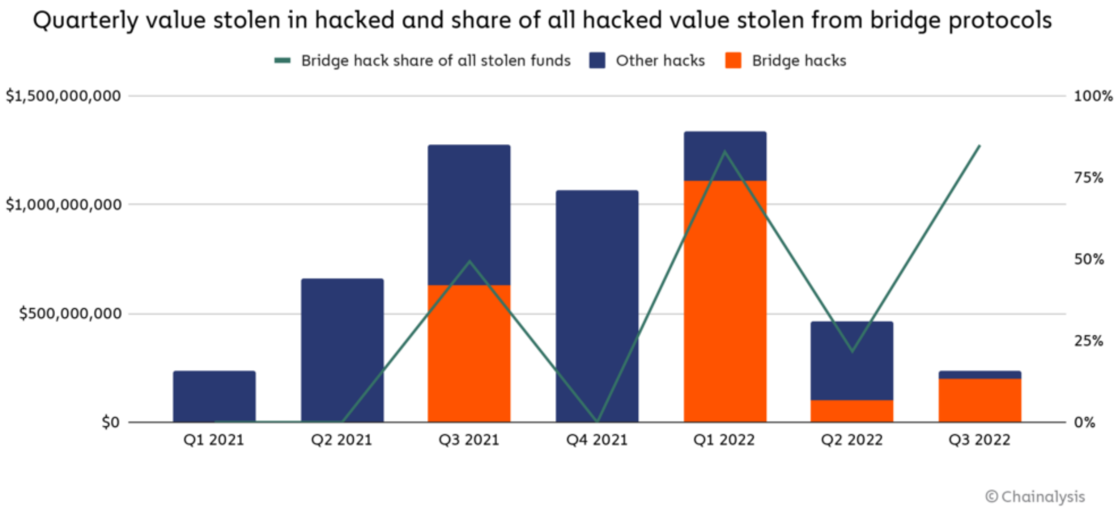
rekt

1. **Ronin Network - REKT** *Unaudited*
   $624,000,000 | 03/23/2022
2. **Poly Network - REKT** *Unaudited*
   $611,000,000 | 08/10/2021
3. **BNB Bridge - REKT** *Unaudited*
   $586,000,000 | 10/06/2022
4. **Wormhole - REKT** *Neodyme*
   $326,000,000 | 02/02/2022
5. **BitMart - REKT** *N/A*
   $196,000,000 | 12/04/2021

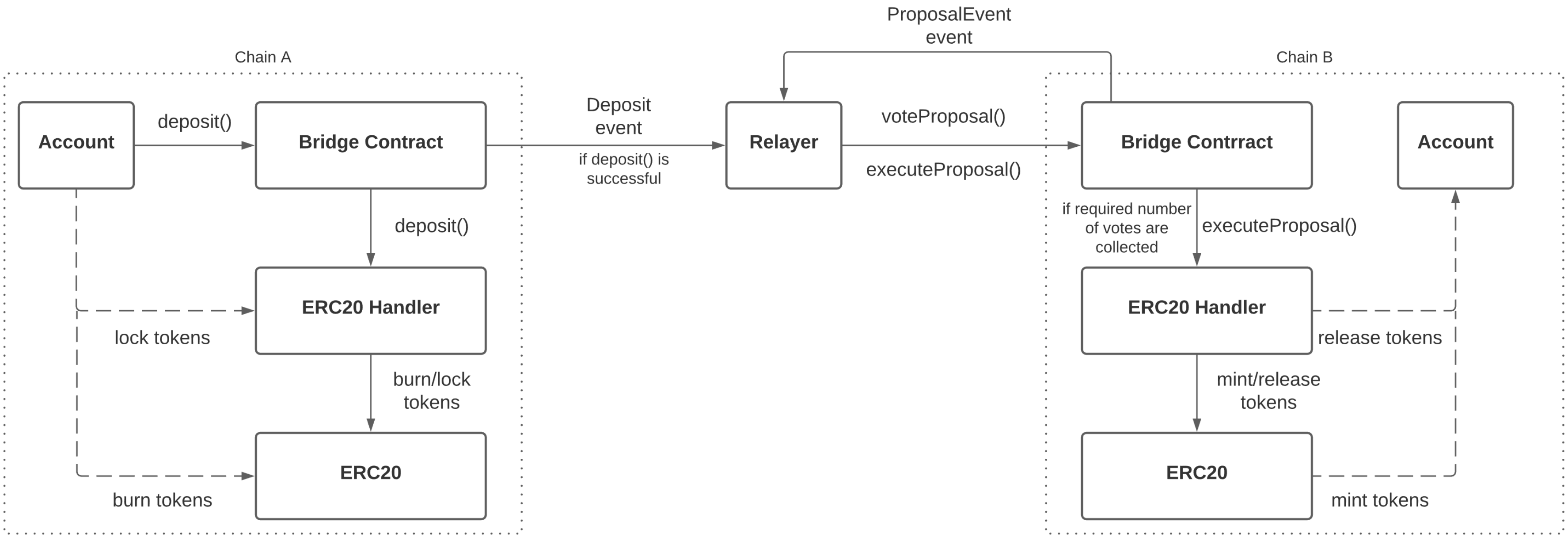
https://rekt.news/leaderboard/

Bridge Risk

- Smart Contract Risk
- Network Risk
- Intermediary Risk



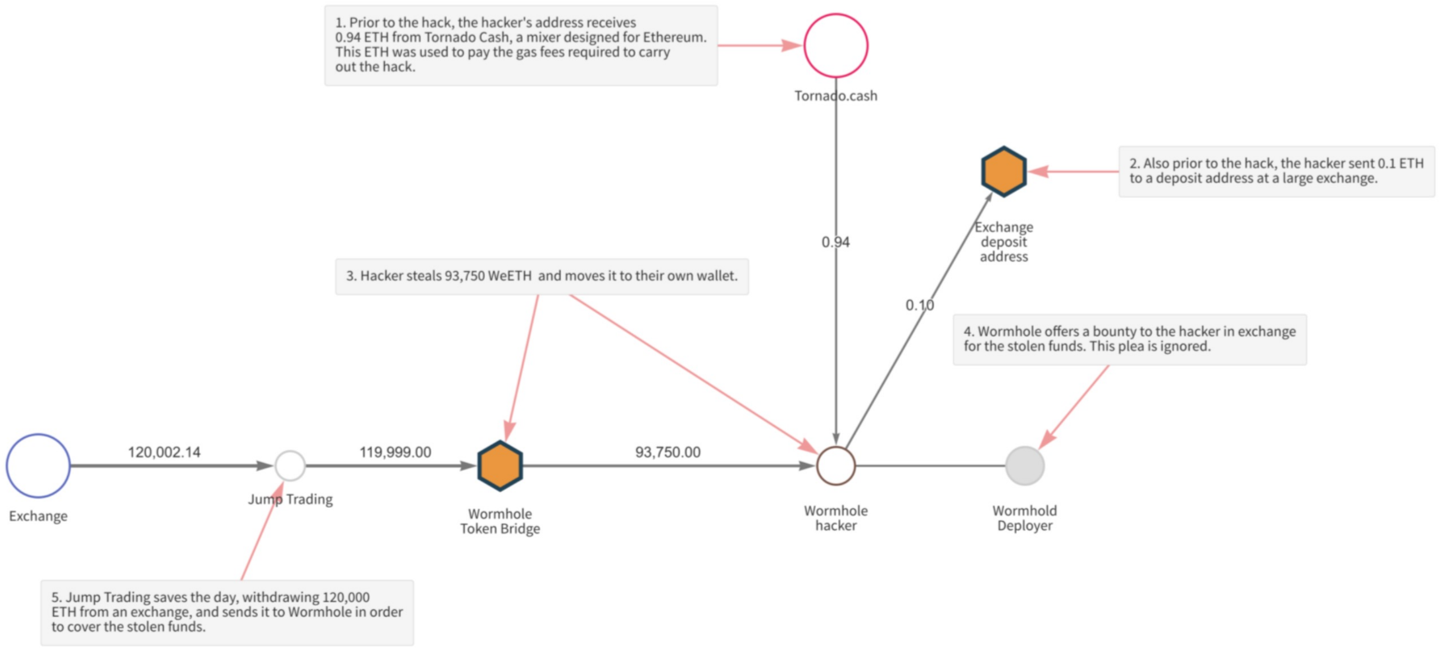
Bridge 보안


ProposalEvent
event
Chain A
Chain B
Account
deposit()
Bridge Contract
Deposit
event
if deposit() is
successful
Relayer
voteProposal()
executeProposal()
Bridge Contrract
Account
deposit()
if required number
of votes are
collected
executeProposal()
ERC20 Handler
lock tokens
ERC20 Handler
release tokens
burn/lock
tokens
mint/release
tokens
ERC20
burn tokens
ERC20
mint tokens

Axie Infinity Hack

- Ronin Bridge
  - bridge consensus를 위한 9개의 Validator 중 5개 공격

Solana-Wormhole hack



1. Prior to the hack, the hacker's address receives 0.94 ETH from Tornado Cash, a mixer designed for Ethereum. This ETH was used to pay the gas fees required to carry out the hack.

2. Also prior to the hack, the hacker sent 0.1 ETH to a deposit address at a large exchange.

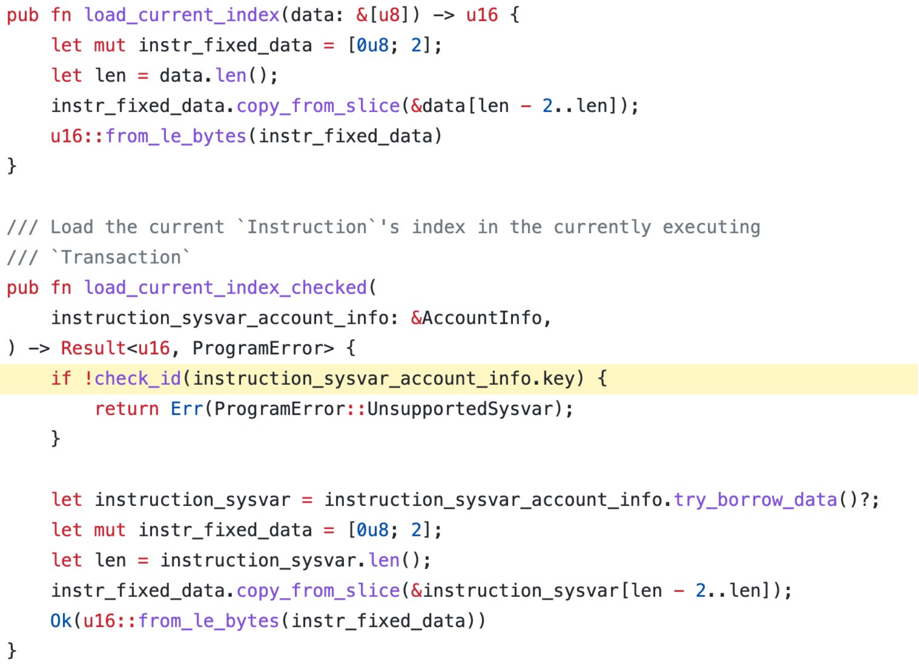
3. Hacker steals 93,750 WeETH and moves it to their own wallet.

4. Wormhole offers a bounty to the hacker in exchange for the stolen funds. This plea is ignored.

5. Jump Trading saves the day, withdrawing 120,000 ETH from an exchange, and sends it to Wormhole in order to cover the stolen funds.

Solana-Wormhole hack

- Contract Vulnerability



```rust
pub fn load_current_index(data: &[u8]) -> u16 {
    let mut instr_fixed_data = [0u8; 2];
    let len = data.len();
    instr_fixed_data.copy_from_slice(&data[len - 2..len]);
    u16::from_le_bytes(instr_fixed_data)
}

/// Load the current `Instruction`'s index in the currently executing
/// `Transaction`
pub fn load_current_index_checked(
    instruction_sysvar_account_info: &AccountInfo,
) -> Result<u16, ProgramError> {
    if !check_id(instruction_sysvar_account_info.key) {
        return Err(ProgramError::UnsupportedSysvar);
    }

    let instruction_sysvar = instruction_sysvar_account_info.try_borrow_data()?;
    let mut instr_fixed_data = [0u8; 2];
    let len = instruction_sysvar.len();
    instr_fixed_data.copy_from_slice(&instruction_sysvar[len - 2..len]);
    Ok(u16::from_le_bytes(instr_fixed_data))
}
```

Bridge 보안

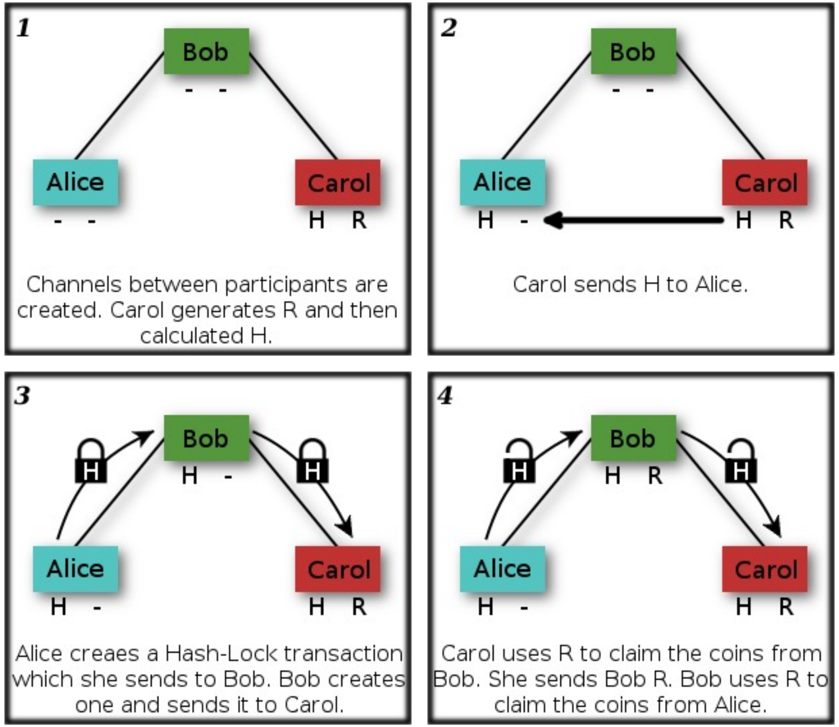
- Validation
  - Consensus, State, Validator …

- Swapping Protocol
  - Conditional Transfer
  - Trusted bridging provider

- Formatted Contract
  - Auditing
  - OpenZeppelin

Bridge 보안

- Example
  - Hash Time Lock Contract (HTLC)



Channels between participants are created. Carol generates R and then calculated H.

Carol sends H to Alice.

Alice creaes a Hash-Lock transaction which she sends to Bob. Bob creates one and sends it to Carol.

Carol uses R to claim the coins from Bob. She sends Bob R. Bob uses R to claim the coins from Alice.