

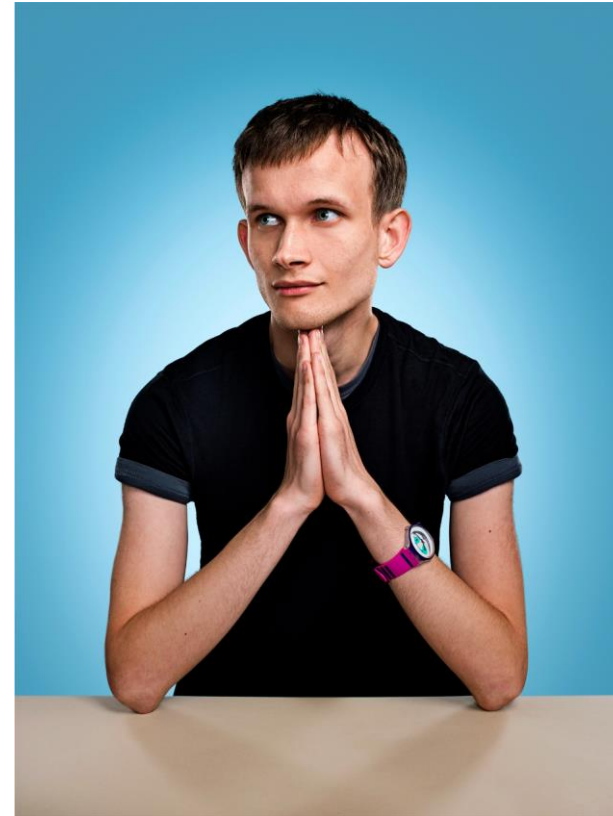
Web3 Security

Anindya Maiti

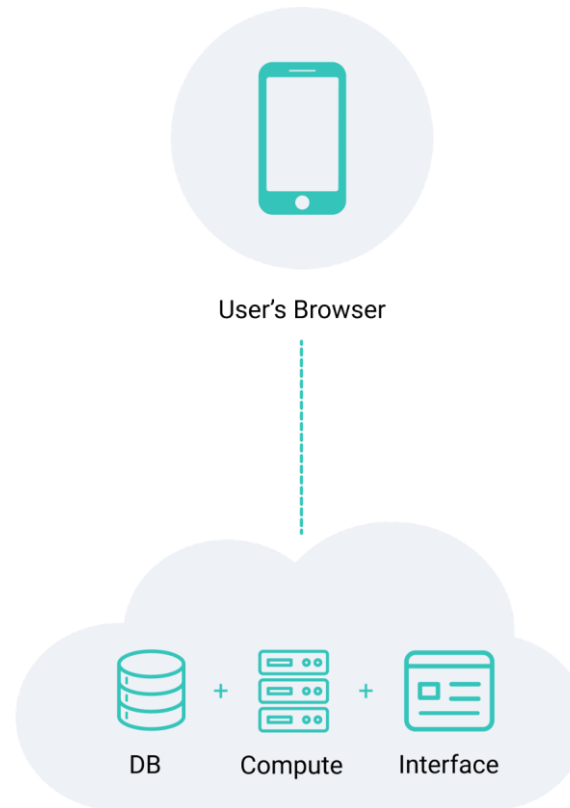
Ethereum and Web3

“ I happily played World of Warcraft during 2007-2010, but one day Blizzard removed the damage component from my beloved warlock’s Siphon Life spell. I cried myself to sleep, and on that day I realized what horrors centralized services can bring.

–Vitalik Buterin



Web2



Web3: Moving (web) apps to the blockchain!

Blockchains

- “Just” a distributed database
 - Reaching a consensus on conflicts is not trivial!
- Messages are authenticated
 - User address corresponds to a public key
 - User signs messages with a private key
 - Private key stored in a wallet
- Very useful for money transfer!
- Bitcoin (2009) is doing that:
 - “1 built-in program”: “Send(source,dest,amount)”
 - Check authenticity by verifying the user’s signature on the transaction
 - Add amount to dest, subtract amount from source
 - Results are saved in the blockchain



Classic Blockchain (like Bitcoin)

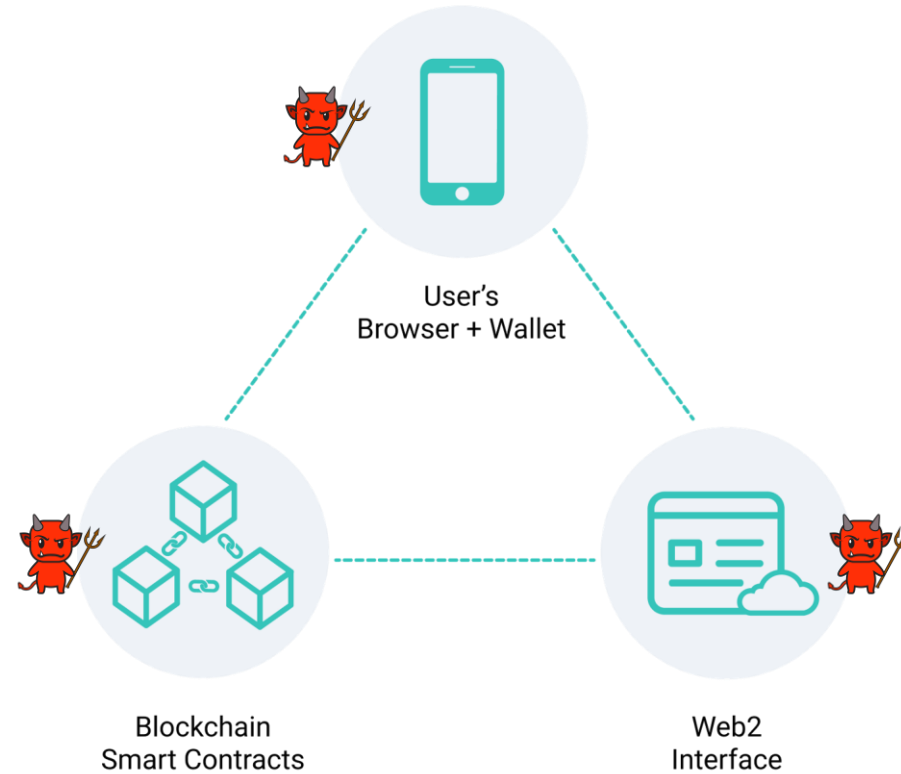


User's Wallet



Blockchain

Web3 Echosphere: Web + Blockchain (like Ethereum)

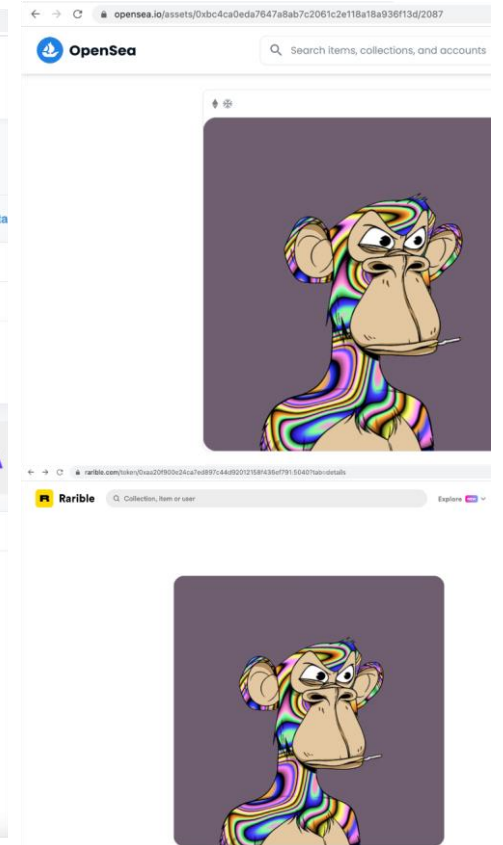
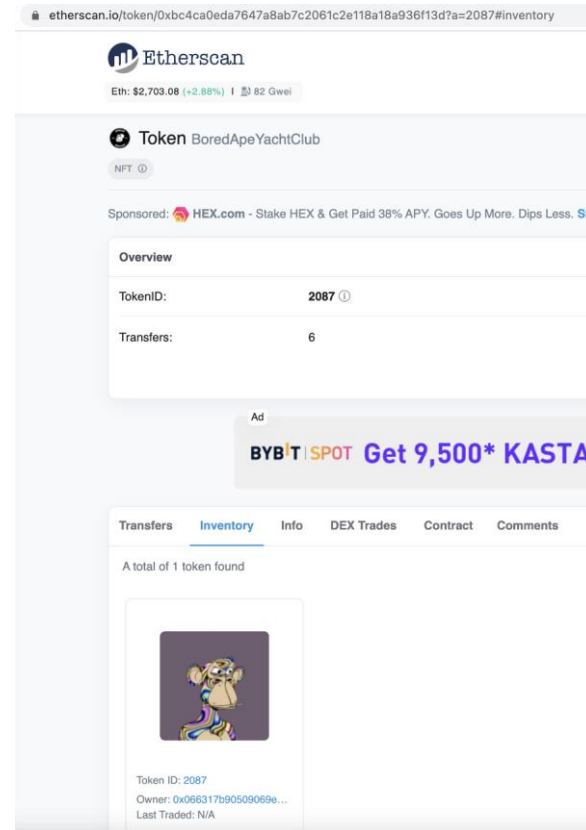


The Web3 Triangle

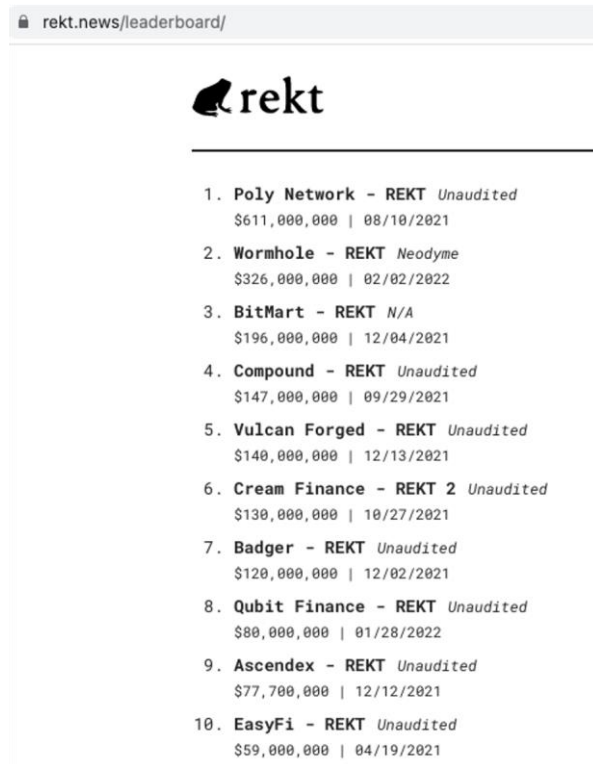
- Web2 app interface: App UX, suggests transactions to the user.
- Wallet: key management, transaction signing and blockchain interaction.
- Blockchain smart contracts (“contracts”): implements the app’s logic.

Example: NFT

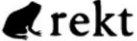
- The user owns NFTs
 - Ownership is public on blockchain
 - User can transfer via wallet
- Multiple marketplaces
 - For example: Opensea, rarible



Web3 Security: The Problem



rekt.news/leaderboard/

 rekt

1. Poly Network - REKT Unaudited
\$611,000,000 08/10/2021
2. Wormhole - REKT Neodyme
\$326,000,000 02/02/2022
3. BitMart - REKT N/A
\$196,000,000 12/04/2021
4. Compound - REKT Unaudited
\$147,000,000 09/29/2021
5. Vulcan Forged - REKT Unaudited
\$140,000,000 12/13/2021
6. Cream Finance - REKT 2 Unaudited
\$130,000,000 10/27/2021
7. Badger - REKT Unaudited
\$120,000,000 12/02/2021
8. Qubit Finance - REKT Unaudited
\$80,000,000 01/28/2022
9. Ascendex - REKT Unaudited
\$77,700,000 12/12/2021
10. EasyFi - REKT Unaudited
\$59,000,000 04/19/2021

As for this hack? Here's what MetaMask support has to say about it:

If you were hacked, this would most likely be due to a few possible reasons:

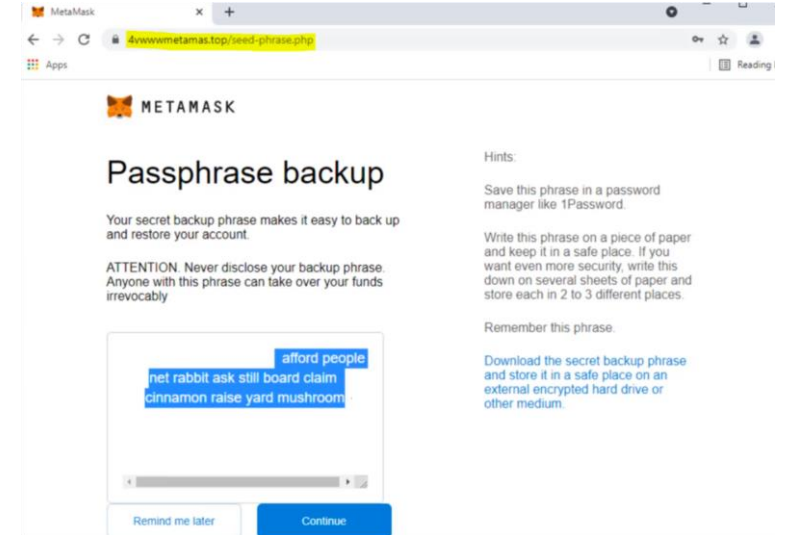
- *Your computer has been compromised with (malware/spyware) and you stored your private information on your computer.*
- *You have visited a malicious phishing website that stole your information.*
- *You gave your private key or Seed Phrase / Secret Recovery Phrase to someone or a site.*
- *You gave a web3 site / smart contract unlimited access to your funds (check who you gave access to and revoke here: <https://tac.dappstar.io/#/>)*
- *You installed a fake MetaMask extension that stole your funds.*

<https://rekt.news/leaderboard/>

Security #1: Wallet

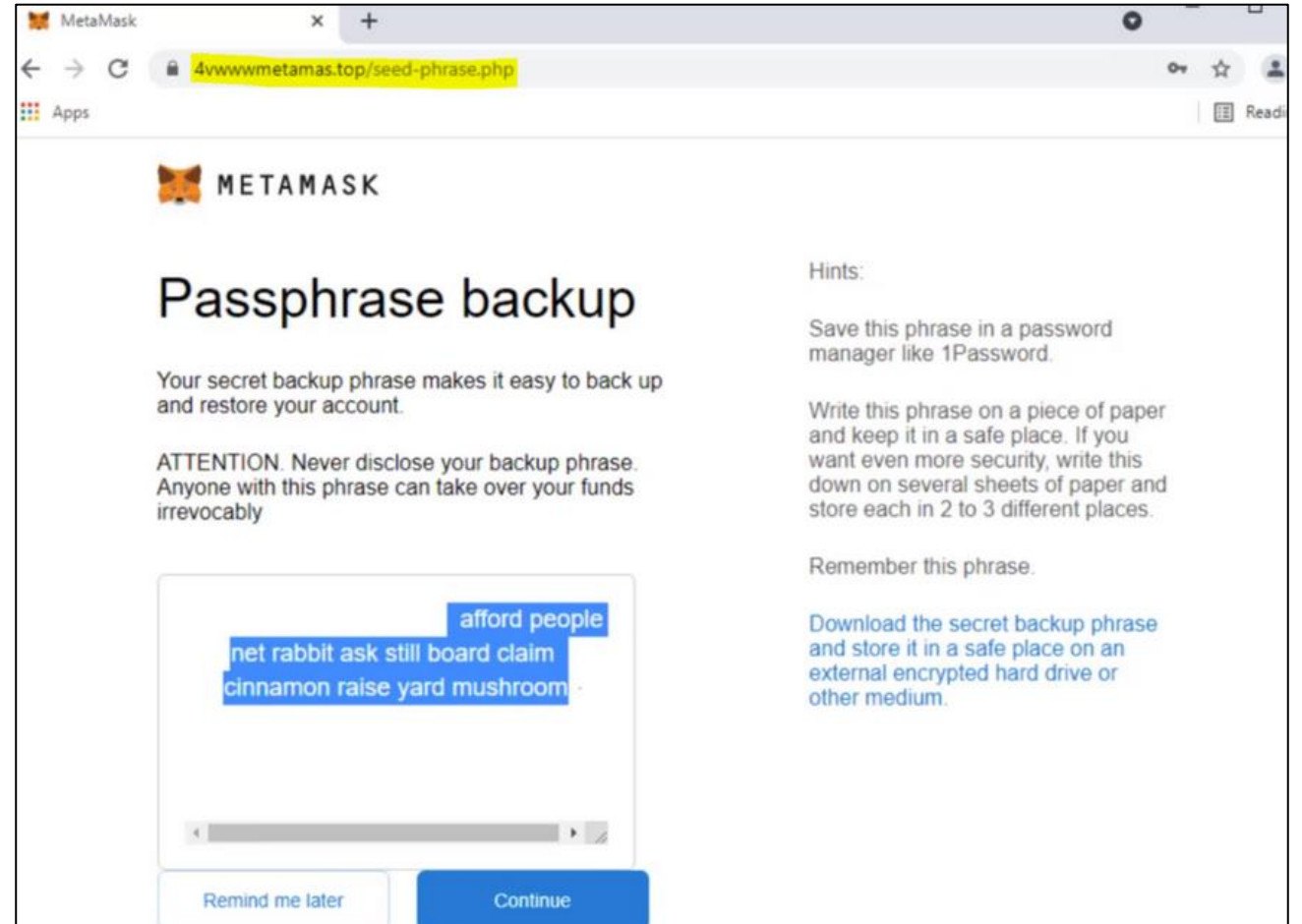
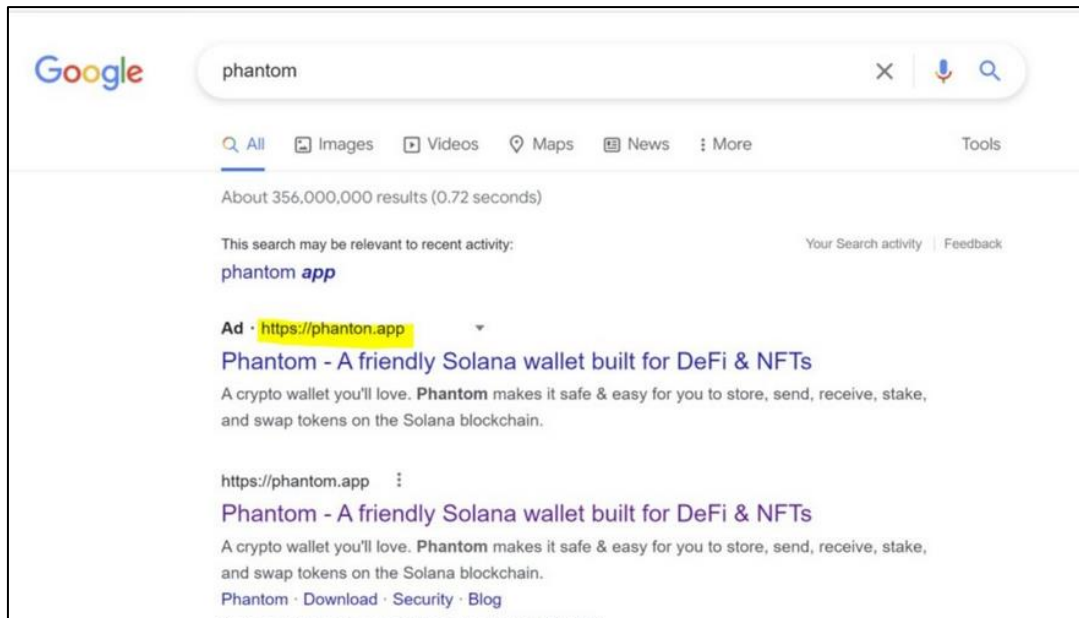
Wallet Security

- Attacks on private key:
 - Theft: phishing, malware, stolen backup, fake wallets
 - Loss: key is lost and backup fails
- Wallet security is key security
- Web3 is pretty much same as for “old” crypto
- Solutions: protect key with a “secure” wallet



Security #1: Wallet

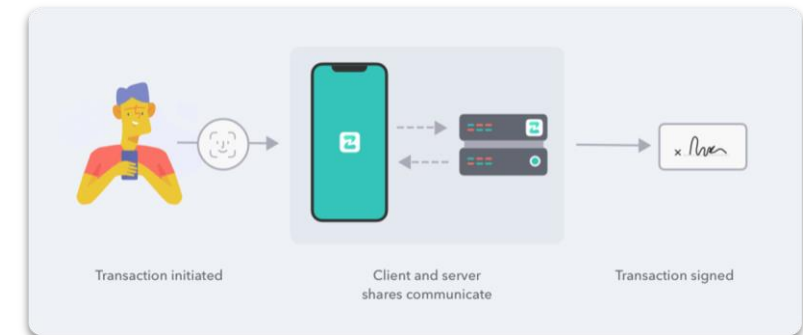
Lingering problems



Security #1: Wallet

Threshold Signatures

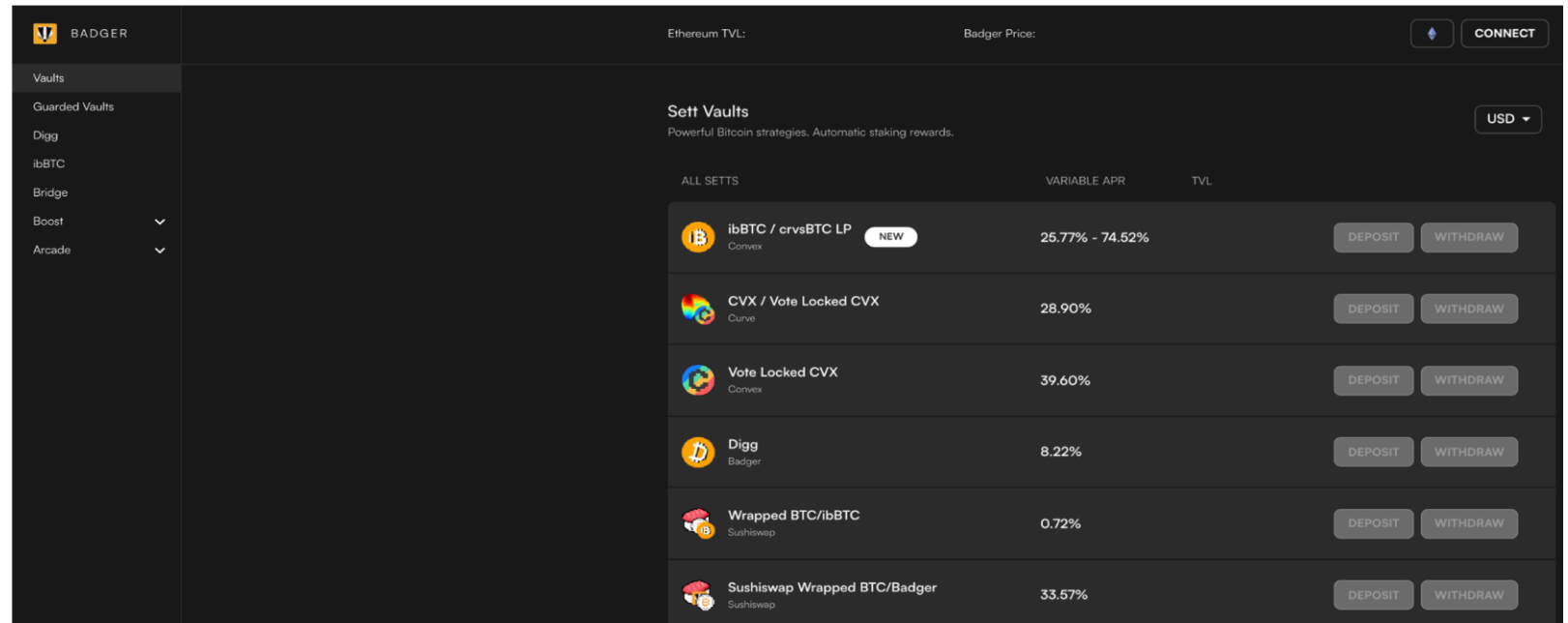
- Private key becomes distributed: no longer a Single-Point-of-Failure
- Distributed protocols: back and forth messages exchange between parties
 - Key generation: each party creates a “Share” (which is not “half of the key”)
 - Signing: using the Shares, parties sign together
- The signature looks the same!
- When 1 (private key) becomes 2 (shares):
 - Harder for attackers to steal: needs to compromise both parties
 - Easier to backup: each share is meaningless by itself



Security #2: Front End

BadgerDao Hack

- “Bringing Bitcoin to DeFi” : Earn interest on your BTC
 - via ERC20



The screenshot displays the BadgerDAO interface. On the left is a navigation sidebar with options: Vaults, Guarded Vaults, Digg, ibBTC, Bridge, Boost, and Arcade. The main content area is titled 'Sett Vaults' and includes a sub-header 'Powerful Bitcoin strategies. Automatic staking rewards.' Below this is a table of vaults with columns for 'ALL SETTS', 'VARIABLE APR', and 'TVL'. Each row includes a vault name, its provider, an APY range, and 'DEPOSIT' and 'WITHDRAW' buttons.

ALL SETTS	VARIABLE APR	TVL
ibBTC / crvsBTC LP <small>Convex</small>	25.77% - 74.52%	
CVX / Vote Locked CVX <small>Curve</small>	28.90%	
Vote Locked CVX <small>Convex</small>	39.60%	
Digg <small>Badger</small>	8.22%	
Wrapped BTC/ibBTC <small>Sushiswap</small>	0.72%	
Sushiswap Wrapped BTC/Badger <small>Sushiswap</small>	33.57%	

Security #2: Front End

- CloudFlare: Hackers' entry method
- CloudFlare (CF) is a web2 proxy
 - Security, Content caching (CDN)
- BadgerDAO (BD) uses CF
 - CF has a feature to add content to website ("workers")
- [Aug 2021] Hackers used a vulnerability in CF to add API key to workers controlled by attackers
 - Required some mistakes on BD side too [Sep 2021]
- Hackers were able to inject code into BD's web2 interface!



rekt
@RektHQ



Replying to @BadgerDAO

@BadgerDAO yells at @Cloudflare



8:13 PM · Dec 11, 2021 · Twitter for iPhone

Security #2: Front End

Not just BadgerDAO!

**Celsius lost \$54 million Bitcoin by using
MetaMask for customer funds**

6:16 PM • Dec 07, 2021

Shai



Security #3: Smart Contracts

The MultiChain Hack

- Multichain Router (previously AnySwap) allows users to freely swap tokens between two blockchains.
- Exploited
 - Started January 18th 2022
 - >1900 ETH Stolen (~\$5M)
- Smart Contract logical error
- <https://medium.com/zengo/without-permit-multichains-exploit-explained-8417e8c1639b>

Security #3: Smart Contracts

The MultiChain Hack

The vulnerable code: Multichain failed here as this function should have checked if the token address is indeed of a Multichain token.

```
function anySwapOutUnderlyingWithPermit(
    address from,
    address token,
    address to,
    uint amount,
    uint deadline,
    uint8 v,
    bytes32 r,
    bytes32 s,
    uint toChainID
) external {
    address _underlying = AnyswapV1ERC20(token).underlying();
    IERC20(_underlying).permit(from, address(this), amount, deadline, v, r, s);
    TransferHelper.safeTransferFrom(_underlying, from, token, amount);
    AnyswapV1ERC20(token).depositVault(amount, from);
    _anySwapOut(from, token, to, amount, toChainID);
}
```

Web3 Security: Conclusion

- Security is important and ongoing venture is three key areas:
 - User wallets
 - Frontend: web server/service
 - Backend: smart contracts