# 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





# 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)



## 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

â etherscan.	io/token/0xbc4ca0eda7647a	8ab7c2061c2e118a18a936f1	3d?a=2087#inventory	← → C a opensea.io/assets/0xbc4ca	0eda7647a8ab7c2061c2e118a18a936f13d/2087	
	D Etherscan			🕗 OpenSea	Q Search items, collections, and accord	
	Eth: \$2,703.08 (+2.68%) 1 🔝 82 Gwei			\$ B		
	<b>Token</b> BoredApeYa	chtClub				
	Sponsored: <mark>জ</mark> HEX.com - Sta	ake HEX & Get Paid 38% APY.	Goes Up More. Dips Less. Sta			
	Overview					
	TokenID:	2087 ①				
	Transfers: Ad	6				
	BY	BIT SPOT Get 9,	,500* KASTA	← → C a ratible.com/tukery0vaz201900c24ca1ro1897c44d	820121584356479150407tab-details	
	Transfers Inventory	Info DEX Trades C	ontract Comments			
	A total of 1 token found	e				

#### Web3 Security: The Problem



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

👹 MetaMask	× +	0			
← → C	Avwwwmetamas.top/seed-phrase.php	07	\$	-	
Apps				Reading	
	🗮 METAMASK				
	Passphrase backup	Hints:			
		Save this phrase in a password manager like 1Password.			
	Your secret backup phrase makes it easy to back up and restore your account.	Write this phrase on a piece of paper and keep it in a safe place. If you			
	ATTENTION. Never disclose your backup phrase. Anyone with this phrase can take over your funds irrevocably	want even more security, write this down on several sheets of paper and store each in 2 to 3 different places.			
		Remember this phrase.			
	afford people net rabbit ask still board claim cinnamon raise yard mushroom	Download the secret backup phrase and store it in a safe place on an external encrypted hard drive or other medium.			
	• 2				
	Remind me later Continue				

#### 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

Vw.dris       Cuarcidor Vivuils       Povertifications statuling revended.       USD •         Dega       ALL SET IS       VALABLE APR       VL         Boost       ALL SET IS       S277% - 74.52%       DEPOSIT       WTHDRAWY         Arcade <ul> <li></li></ul>	😲 BADGER	Ethereu	m TVL:	Badger Price:	• CONNECT
Guarded Wattle       Sett Valitle       Power Hall Blichein stradesgies. Automatie takking reveards.       Mark Alle LARR       Tut         Beet       ALL SETTS       Start Stradesgies. Automatie takking reveards.       Start Stradesgies. Automatie takking reveards.       Start Stradesgies. Automatie takking reveards.       Start Star	Vaults				
Digit Reverted Blaccin strategies. Automatic strating reveards.     BitC   Bidge   Boost   Arcade     Arcade     Convex     Convex	Guarded Vaults	Sett V	/aults		
herc   Bridge   Boot   Acade   Acade   Corres   Corres <th>Digg</th> <th></th> <th>Il Bitcoin strategies. Automatic staking rewards.</th> <th></th> <th></th>	Digg		Il Bitcoin strategies. Automatic staking rewards.		
Bridge   Boost   Arcade   Connect	ibBTC	ALL S	SETTS	VARIABLE APR TV	
Boot       Image: Convect Current Curr	Bridge				
Arcado       COMAR       28.90%       DEPOSIT       WITHDRAW         Image: Comar	Boost 🗸	<u></u>	ibBTC / crvsBTC LP	25.77% - 74.52%	DEPOSIT
<p< td=""><th>Arcade 🗸</th><th></th><td>Convex</td><td></td><td></td></p<>	Arcade 🗸		Convex		
Curve 28.90% DEPOSIT   WITHDRAW   Image: Curve			CVX / Vote Locked CVX	<b>60 00</b> 0/	
Vote Locked CVX 39.60%   Convex 39.60%   DEPOSIT WITHDRAW   Image: Sublive Deposit Strike   Image: Strike   Image: Strike   Image: Strike   Image: Strike   Image: Strike			Curve	28.90%	DEPOSIT
Vote Locked CVX 39.60%   Convex 39.60%   DEPOSIT WITHDRAW   Image: Sublisher Proped BTC/Badger 0.72%   DEPOSIT WITHDRAW   Image: Sublisher Proped BTC/Badger 33.57%   DEPOSIT WITHDRAW					
Digg Digg   Badger 8.22%   DEPOSIT   WTHDRAW   Composition   Sushiswap Wrapped BTC/Badger		C	Vote Locked CVX Convex	39.60%	DEPOSIT
Image: Pigg Badger     8.22%       Image: Pigg Badger     8.22%       Image: Pigg Badger     0.72%       Image: Pigg Badger     0.72% <th></th> <th></th> <th></th> <th></th> <th></th>					
Badger       Eadger       Image: Badger		<u>68</u>	Digg	8.22%	DEPOSIT
Wrapped BTC/ibBTC     0.72%     DEPOSIT     WITHDRAW       Sushiswap Wrapped BTC/Badger     33.57%     DEPOSIT     WITHDRAW			Badger		
Sushiswap     O.72%     DEPOSIT     WITHDRAW       Image: Sushiswap Wrapped BTC/Badger     33.57%     DEPOSIT     WITHDRAW			Wrapped BTC/ibBTC		
Sushiswap Wrapped BTC/Badger 33.57% DEPOSIT WITHDRAW			Sushiswap	0.72%	DEPOSIT
Sushiswap Wrapped BTC/Badger 33.57% DEPOSIT WITHDRAW					
			Sushiswap Wrapped BTC/Badger Sushiswap	33.57%	DEPOSIT

### 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!



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
- <u>https://medium.com/zengo/without-permit-multichains-exploit-explained-8417e8c1639b</u>

### 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.

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); 3

### Web3 Security: Conclusion

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