Introduction to Crypto Wallet and Transaction

Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

Outline

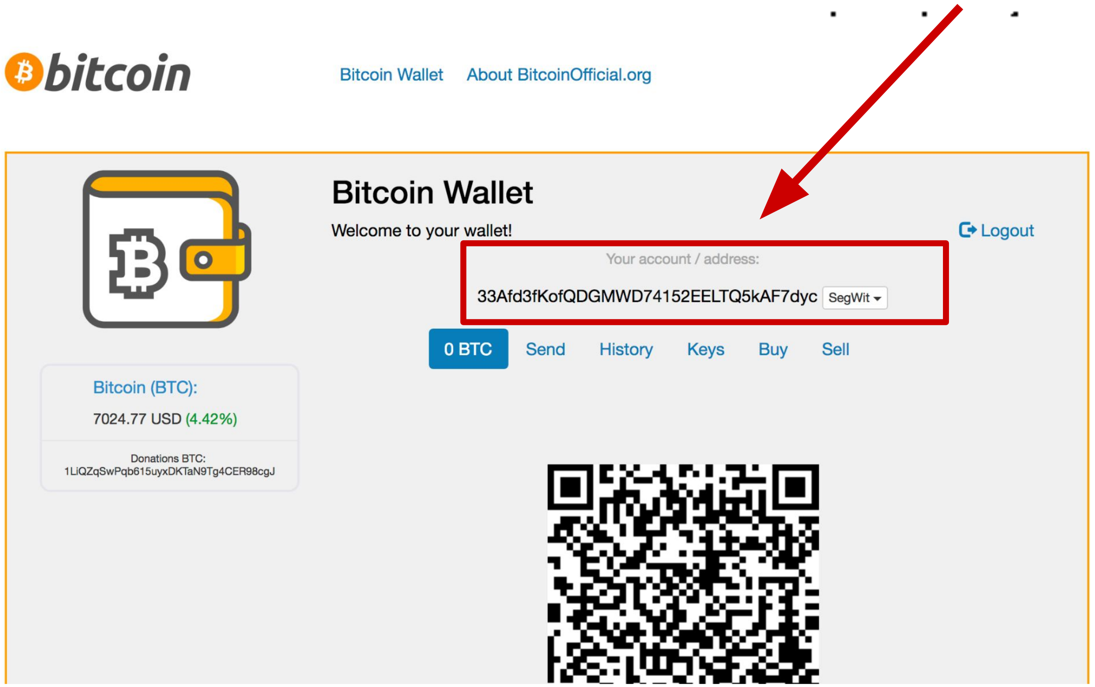
- Crypto wallets
- Security Concerns
- Understand Blockchain Transaction Data

Crypto Wallets

SWINBURNE UNIVERSITY OF TECHNOLOGY

What is a Crypto Wallet?

A crypto wallet is a digital tool that allows users to store, manage, and interact with their cryptocurrencies. A crypto wallet doesn't store actual coins but rather the keys needed to access and manage them on the blockchain.



bitcoin

Bitcoin Wallet About BitcoinOfficial.org

Bitcoin Wallet

Welcome to your wallet!

Logout

Your account / address:

33Afd3fKofQDGMWD74152EELTQ5kAF7dyc SegWit

0 BTC Send History Keys Buy Sell

Bitcoin (BTC):

7024.77 USD (4.42%)

Donations BTC:
1LiQZqSwPqb615uyxDKTaN9Tg4CER98cgJ

Public and Private Keys:

Every wallet has a pair of keys. The public key is an address where others can send cryptocurrencies. The private key is a secret code known only to the owner, allowing access to the wallet.

Types of Crypto Wallets:

- Software Wallets: Applications or online services.
- Hardware Wallets: Physical devices for offline storage.
- Paper Wallets: Physical documents with key information.

Custodial VS Non-Custodial Wallets

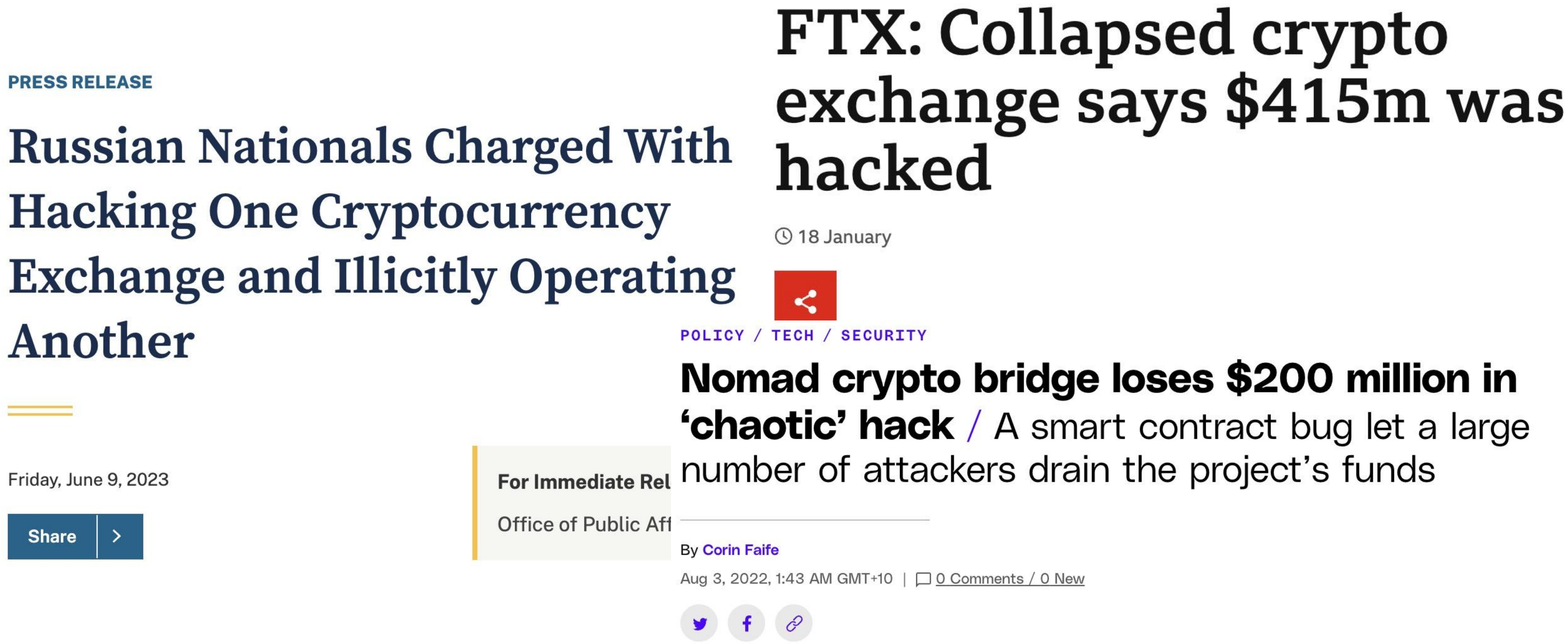
Wallet Type	**Custodial Wallet**	**Non-Custodial Wallet**
Definition	Custodial wallets are managed by third-party service providers, such as exchanges or wallet platforms.	Non-custodial wallets give users full control over their private keys and are not managed by third parties.
Pros	- User-friendly, especially for beginners. - Service providers often offer customer support. - Ideal for users who prefer a hands-off approach to security.	- Users have complete control over their funds. - Higher security, as private keys are not stored on external servers. - Supports a wide range of cryptocurrencies.
Cons	- Users do not have direct control over their private keys. - Vulnerable to security breaches on the custodian's side. - May involve additional fees or restrictions.	- Requires users to take responsibility for their security. - Potential loss of funds if private keys are lost or compromised. - Less beginner-friendly compared to custodial options.

Security Concerns

SWINBURNE UNIVERSITY OF TECHNOLOGY

Common Incidents

Hacking: Unauthorized access to a crypto wallet, often through exploiting vulnerabilities in the wallet software or hacking into the user's account.



PRESS RELEASE

Russian Nationals Charged With Hacking One Cryptocurrency Exchange and Illicitly Operating Another

Friday, June 9, 2023

Share >

For Immediate Rel

Office of Public Aff

FTX: Collapsed crypto exchange says $415m was hacked

18 January

POLICY / TECH / SECURITY

Nomad crypto bridge loses $200 million in 'chaotic' hack / A smart contract bug let a large number of attackers drain the project's funds

By Corin Faife

Aug 3, 2022, 1:43 AM GMT+10 | 0 Comments / 0 New

https://www.justice.gov/opa/pr/russian-nationals-charged-hacking-one-cryptocurrency-exchange-and-illicitly-operating-another

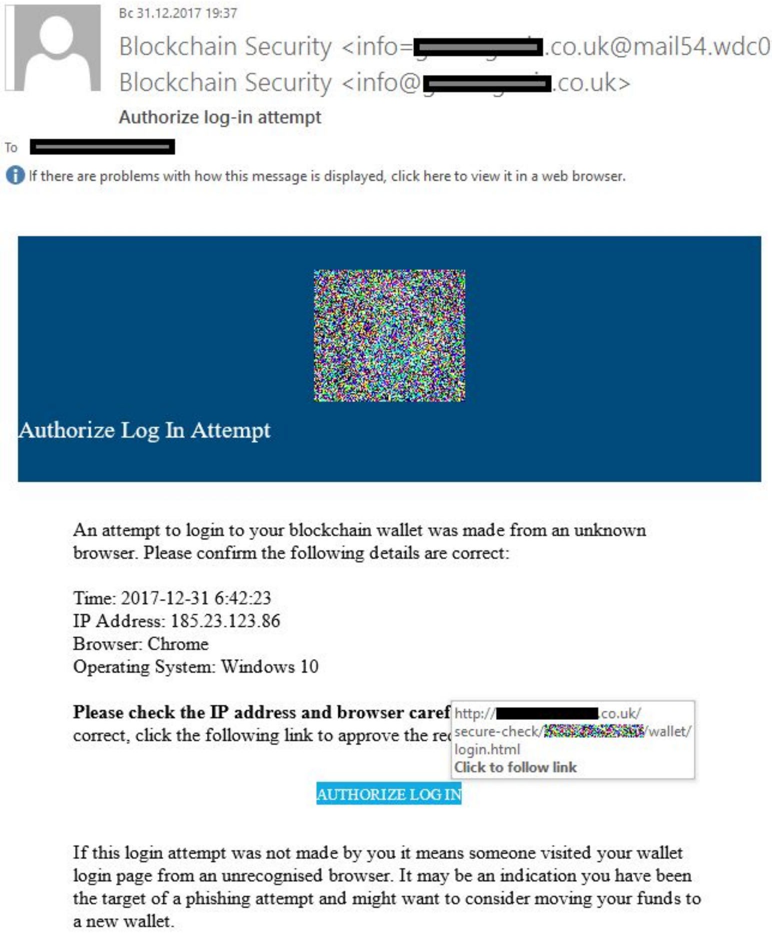
Common Incidents

Phishing: Deceptive attempts to obtain sensitive information, such as private keys or login credentials, by posing as a trustworthy entity.

Scams: Fraudulent schemes where individuals are deceived into sending funds to malicious actors under false pretenses.

Examples:

- Blackmail and extortion
- "Business opportunity"
- Fake job listing
- Giveaway
- Impersonation
- Investment
- ...



Bc 31.12.2017 19:37

Blockchain Security <info=[redacted].co.uk@mail54.wdc01.[redacted]> on behalf of Blockchain Security <info@[redacted].co.uk>

Authorize log-in attempt

To [redacted]

If there are problems with how this message is displayed, click here to view it in a web browser.

Authorize Log In Attempt

An attempt to login to your blockchain wallet was made from an unknown browser. Please confirm the following details are correct:

Time: 2017-12-31 6:42:23
IP Address: 185.23.123.86
Browser: Chrome
Operating System: Windows 10

Please check the IP address and browser caref correct, click the following link to approve the rec

http://[redacted].co.uk/secure-check/[redacted]/wallet/login.html
Click to follow link

AUTHORIZE LOG IN

If this login attempt was not made by you it means someone visited your wallet login page from an unrecognised browser. It may be an indication you have been the target of a phishing attempt and might want to consider moving your funds to a new wallet.

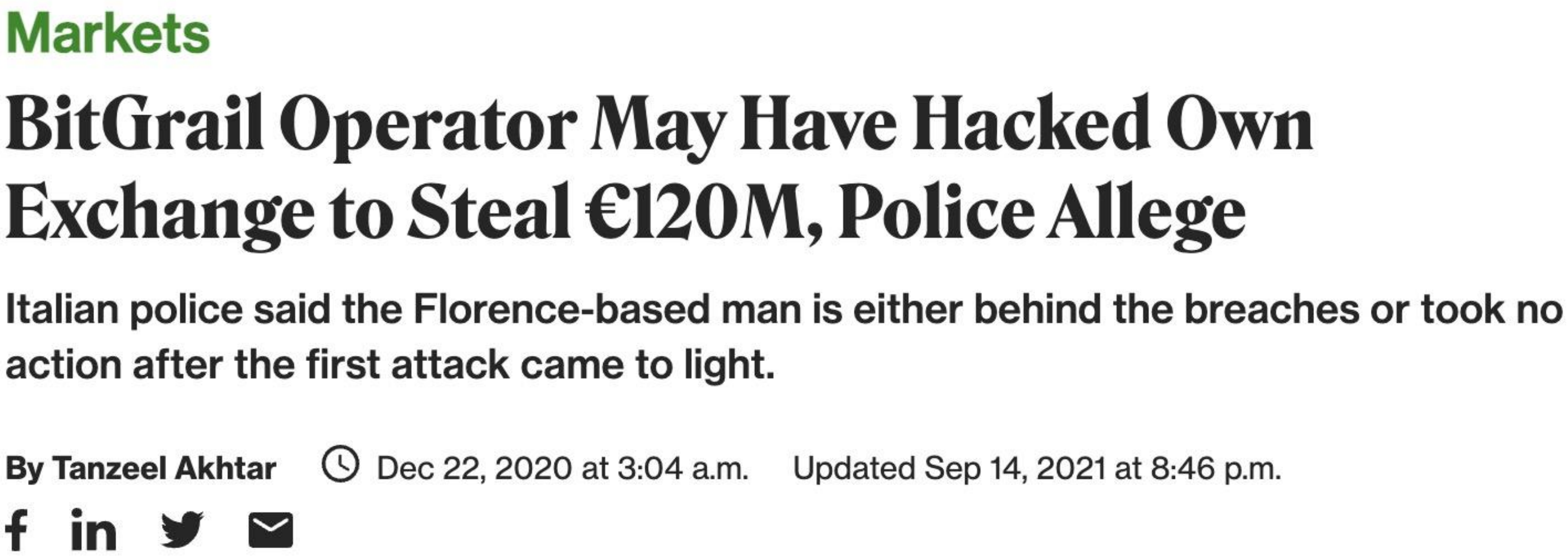
https://www.kaspersky.com/blog/crypto-phishing/20765/
https://time.com/personal-finance/article/popular-crypto-scams/

Common Incidents

Malware Attacks: Malicious software designed to compromise the security of a user's device and gain access to crypto wallet information.

Insider Threats: Misuse of access privileges by individuals within a trusted organization or service.

Unsecured Private Keys: Exposure of private keys due to poor security practices or storage methods.



Markets

BitGrail Operator May Have Hacked Own Exchange to Steal €120M, Police Allege

Italian police said the Florence-based man is either behind the breaches or took no action after the first attack came to light.

By Tanzeel Akhtar Dec 22, 2020 at 3:04 a.m. Updated Sep 14, 2021 at 8:46 p.m.

https://www.coindesk.com/markets/2020/12/21/bitgrail-operator-may-have-hacked-own-exchange-to-steal-120m-police-allege/

Security Features - User Wallet

Encryption: Most crypto wallets use advanced encryption algorithms to protect private keys and sensitive information.

Protection: Encryption ensures that even if unauthorized access occurs, the data is unreadable without the proper decryption keys, providing a strong layer of defense against theft.

Two-Factor Authentication (2FA): Users are required to provide two forms of identification before accessing their wallets. This typically involves a combination of a password and a secondary authentication method (e.g., SMS code, authenticator app).

Protection: 2FA adds an extra layer of security, making it more challenging for attackers to gain unauthorized access, even if they have obtained login credentials.

Other security features:

- Hierarchical Deterministic (HD) Wallets
- Multi-Signature (Multisig) Wallets
- Biometric Authentication
- Offline Storage (Cold Wallets)
- Timed Logouts and Session Management
- Regular Software Updates

Security Features - Exchange Companies

Two-Factor Authentication (2FA): Similar to crypto wallets, exchanges often enforce two-factor authentication to add an extra layer of security to user accounts.

Protection: 2FA mitigates the risk of unauthorized access by requiring users to provide a second form of verification in addition to their passwords.

Cold Wallet Storage: Reputable exchanges often store a significant portion of user funds in cold wallets, which are not connected to the internet.

Protection: This practice minimizes the risk of online hacking attempts, as the majority of funds are kept in offline storage that is less vulnerable to cyber threats.

Encrypted Communication: Exchanges use secure sockets layer (SSL) and other encryption protocols to ensure that communication between users and the exchange platform is encrypted and secure.

Protection: Encryption protects sensitive information, such as login credentials and transaction details, from interception by malicious actors.

Security Features - Exchange Companies

Regular Security Audits: Reputable exchanges conduct regular security audits and assessments to identify and address vulnerabilities in their systems.

Protection: Ongoing security audits help ensure that the exchange's infrastructure is robust and resilient against potential threats.

Withdrawal Whitelists: Users can set withdrawal whitelist addresses, meaning that funds can only be withdrawn to specified addresses.

Protection: This feature adds an extra layer of security by preventing unauthorized withdrawals to unknown addresses, even if an account is compromised.

Insurance Funds: Some exchanges maintain insurance funds to compensate users in the event of a security breach or unexpected losses.

Protection: Insurance funds provide an additional layer of financial protection for users, demonstrating the exchange's commitment to covering losses due to security incidents.

Security Features - Exchange Companies

User Education and Alerts: Exchanges often provide educational resources to users about security best practices and potential risks. They may also send alerts for suspicious activities.

Protection: Informed users are better equipped to recognize and respond to potential security threats, reducing the likelihood of falling victim to scams or phishing attempts.

Distributed Architecture: Some exchanges employ distributed and redundant architecture to ensure continuous operation even in the face of hardware failures or DDoS attacks.

Protection: Distributed architecture enhances the resilience of the exchange platform, making it more difficult for attackers to disrupt services or compromise user data.

Understand Blockchain Transactions

SWINBURNE UNIVERSITY OF TECHNOLOGY

ETH Transactions ERC-20 & ERC -721

ERC-20	ERC-721
Fungible tokens. Each token is interchangeable and has the same value as any other token of the same type.	Non-fungible tokens (NFTs). Each token is unique and cannot be replaced or exchanged on a one-to-one basis with another token.
Transferring ERC-20 tokens between addresses is straightforward and follows the same process as sending any other cryptocurrency.	Transferring ERC-721 tokens involves transferring ownership of a specific item from one address to another. Each token has a designated owner, and ownership can only be transferred, not duplicated.
Crowdfund through Initial Coin Offerings (ICOs), create stablecoins, and as a medium of exchange in decentralized applications (dApps)	Gained popularity in the art, gaming, and collectibles space, where unique ownership and provenance of digital assets are essential.

Top ERC-20 token list: https://etherscan.io/tokens

Top ERC-721 NFT list: https://etherscan.io/nft-top-contracts

ETH Transactions ERC-20 & ERC -721

ERC-20 token: Fungible, identical and interchangeable

ERC-721 token: Non-fungible tokens (NFTs) , unique and cannot be replaced or exchanged

ETH Transactions (ERC-20)

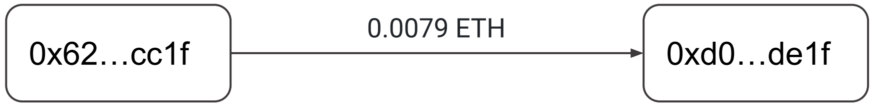
Transactions

Transactions triggered by **external addresses**. External addresses can generally be thought of as user wallets.

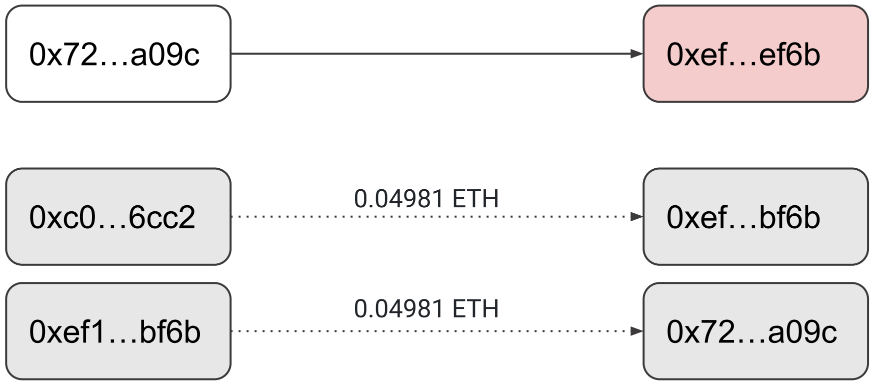
Internal Transactions

Internal transactions are transactions triggered by **smart contracts**.

Hash:0xf7bacf4c744919ce021cc46205df0b6a8ddf177e5c6b7a177d31e075d3895380



Hash:0x9deeb84ba43ce1d6174d16330047dbb8ace0068108ea62f5f17a17b980487372

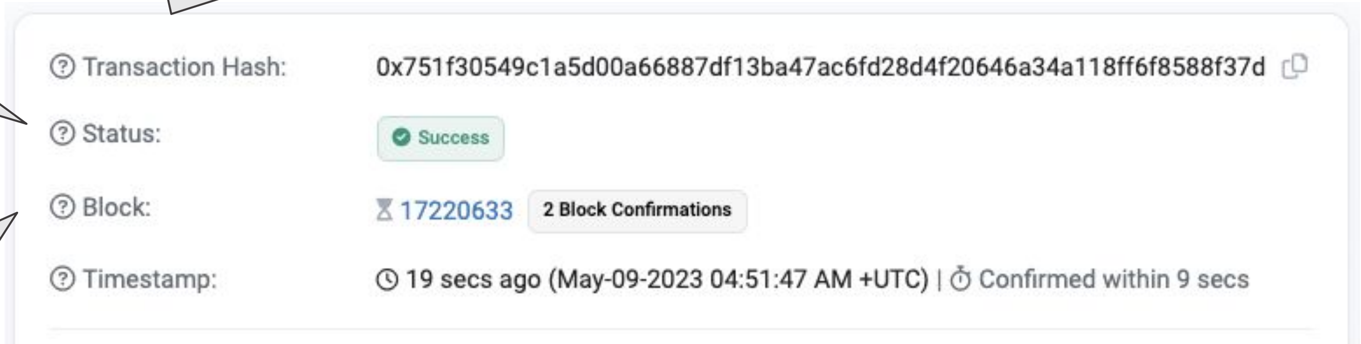


https://etherscan.io/tx/0x9deeb84ba43ce1d6174d16330047dbb8ace0068108ea62f5f17a17b980487372

Understand ETH Transactions (ERC-20)

The string of numbers and letters (TXID) associated with a particular transaction.

Whether the transaction has failed, is in progress, or was successful.



Transaction Hash: 0x751f30549c1a5d00a66887df13ba47ac6fd28d4f20646a34a118ff6f8588f37d

Status: Success

Block: 17220633 2 Block Confirmations

Timestamp: 19 secs ago (May-09-2023 04:51:47 AM +UTC) | Confirmed within 9 secs

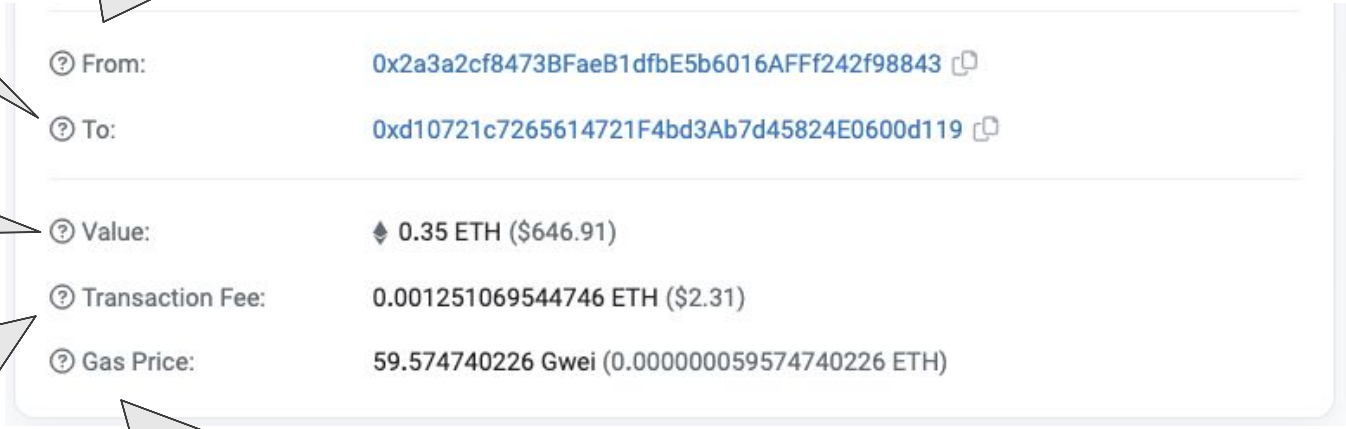
The block number the transaction was included in. You can also see how many times your transaction has been confirmed. This is the number of blocks added to the chain after the transaction's block.

The timestamp of the block the transaction was added to.

Understand ETH Transactions (ERC-20)

The wallet address that made the transaction.

The receiving address or smart contract.



From: 0x2a3a2cf8473BFaeB1dfbE5b6016AFFf242f98843

To: 0xd10721c7265614721F4bd3Ab7d45824E0600d119

Value: 0.35 ETH ($646.91)

Transaction Fee: 0.001251069544746 ETH ($2.31)

Gas Price: 59.574740226 Gwei (0.000000059574740226 ETH)

The amount sent in the transaction.

The fee paid for making the transaction.

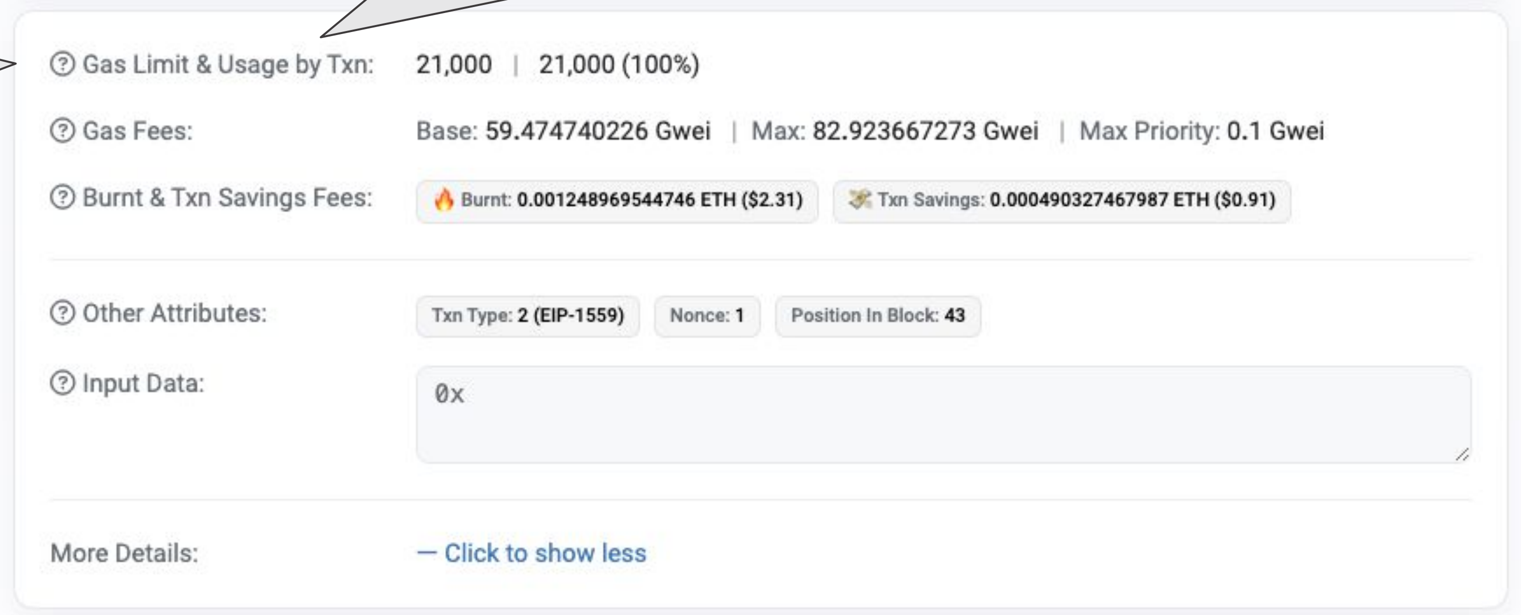
Gas Limit * Gas Price per Unit

The cost per unit of gas for the transaction.

Understand ETH Transactions (ERC-20)

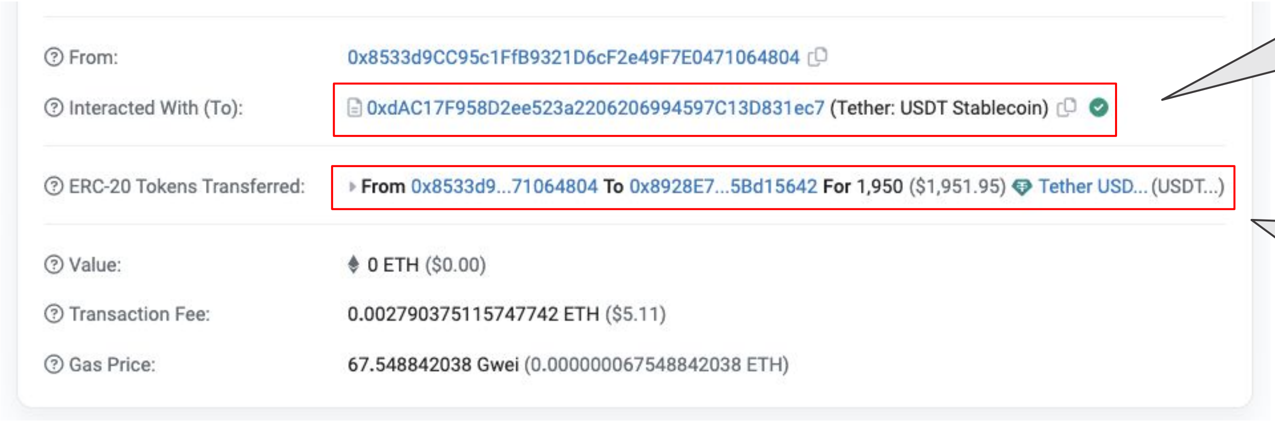
The maximum amount of gas allowed for the transaction. It represents the computational resources required to execute the transaction.

The actual amount of gas consumed during the execution of the transaction. This value determines the total transaction fee (gas cost) paid by the sender.



ⓘ Gas Limit & Usage by Txn:	21,000 | 21,000 (100%)
ⓘ Gas Fees:	Base: 59.474740226 Gwei | Max: 82.923667273 Gwei | Max Priority: 0.1 Gwei
ⓘ Burnt & Txn Savings Fees:	🔥 Burnt: 0.001248969544746 ETH ($2.31) Txn Savings: 0.000490327467987 ETH ($0.91)
ⓘ Other Attributes:	Txn Type: 2 (EIP-1559) Nonce: 1 Position In Block: 43
ⓘ Input Data:	0x
More Details:	— Click to show less

Understand ETH Transactions (ERC-20:Interacted with a contract)



From: 0x8533d9CC95c1FfB9321D6cF2e49F7E0471064804

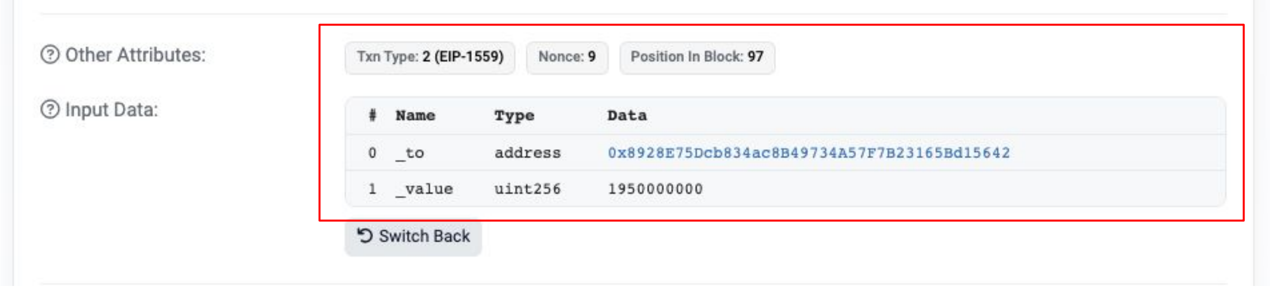
Interacted With (To): 0xdAC17F958D2ee523a2206206994597C13D831ec7 (Tether: USDT Stablecoin)

ERC-20 Tokens Transferred: From 0x8533d9...71064804 To 0x8928E7...5Bd15642 For 1,950 ($1,951.95) Tether USD... (USDT...)

Value: 0 ETH ($0.00)

Transaction Fee: 0.002790375115747742 ETH ($5.11)

Gas Price: 67.548842038 Gwei (0.000000067548842038 ETH)



Other Attributes: Txn Type: 2 (EIP-1559) Nonce: 9 Position In Block: 97

Input Data:

#	Name	Type	Data
0	_to	address	0x8928E75Dcb834ac8B49734A57F7B23165Bd15642
1	_value	uint256	1950000000

The Ethereum address of a contract. This is the address where the token contract is deployed.

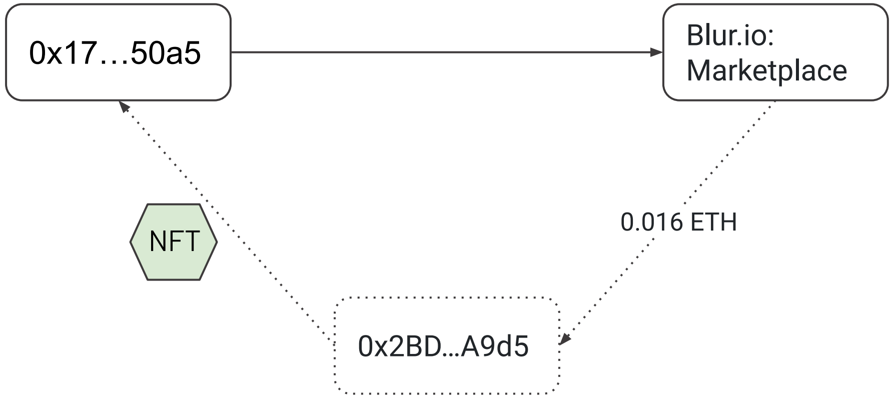
From/To Address
Token Symbol: The symbol or abbreviation of the token being transferred.
Token Name: The name of the token being transferred.
Token Contract Address: The address of the token's smart contract.

For smart contract transactions, this field contains the input data or function call encoded in hexadecimal format.

https://etherscan.io/tx/0xf12c9a0a56cffe86212b4e1d2f1ab361734bf9458c35b60112ae9a77581a9db7

ETH Transactions (ERC-721)

Hash:0x95f1bda709d9916f8a53d9c733f69235b777f8e7834357c22c4a744d37c1b74d



ERC-20 Transactions

The ERC-20 transactions table shows any transaction where an ERC-20 token was involved.

ERC-721 Transactions

Similar to the ERC-20 transaction table, ERC-721 transactions show any transactions using ERC-721 tokens. Generally, these will be NFT transactions.

ETH Transactions Features

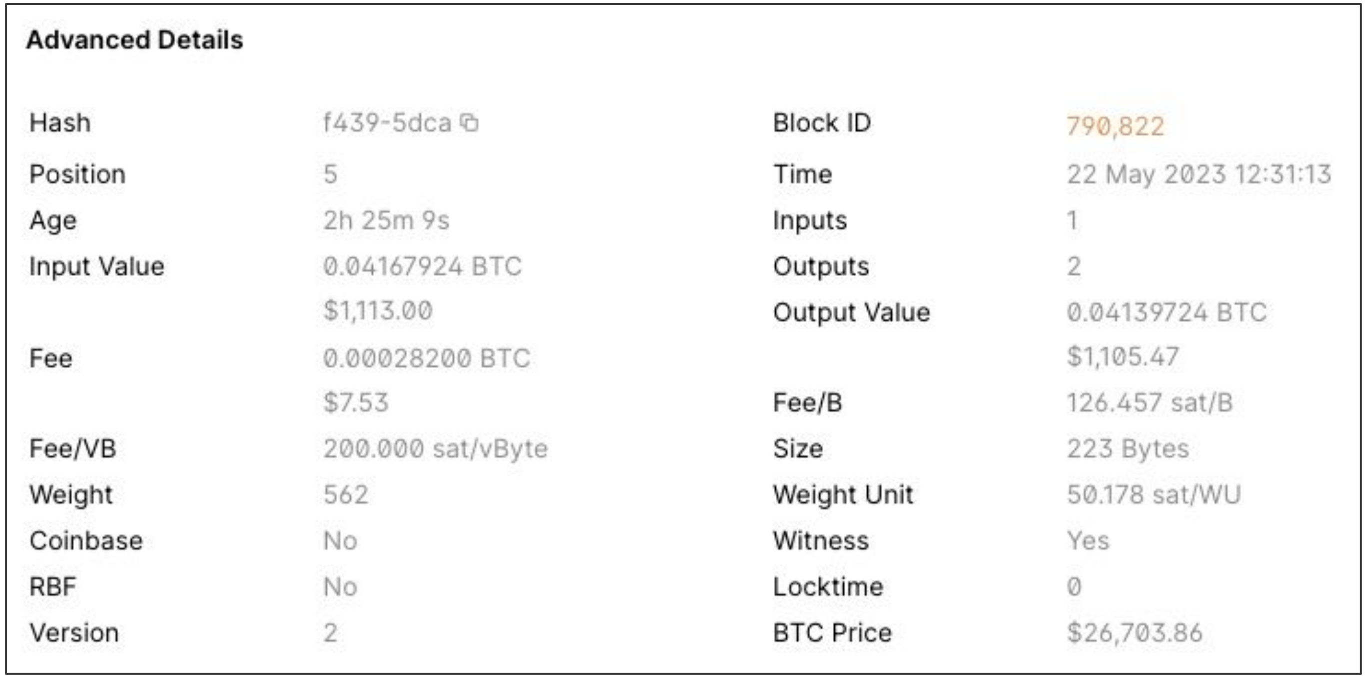
Distributed ledger technology
All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that’s typical of traditional business networks.

Immutable records
No participant can change or tamper with a transaction after it’s been recorded to the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible.

Smart contracts
To speed transactions, a set of rules — called a smart contract — is stored on the blockchain and executed automatically. A smart contract can define conditions for corporate bond transfers, include terms for travel insurance to be paid and much more.

Understand BTC Transactions

Hash:f43912c4ccbb533618f42b8a66b15b03de4b3b8c49aefc40efa93f3f92735dca



Advanced Details

Hash	f439-5dca	Block ID	790,822
Position	5	Time	22 May 2023 12:31:13
Age	2h 25m 9s	Inputs	1
Input Value	0.04167924 BTC	Outputs	2
	$1,113.00	Output Value	0.04139724 BTC
Fee	0.00028200 BTC		$1,105.47
	$7.53	Fee/B	126.457 sat/B
Fee/VB	200.000 sat/vByte	Size	223 Bytes
Weight	562	Weight Unit	50.178 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	2	BTC Price	$26,703.86

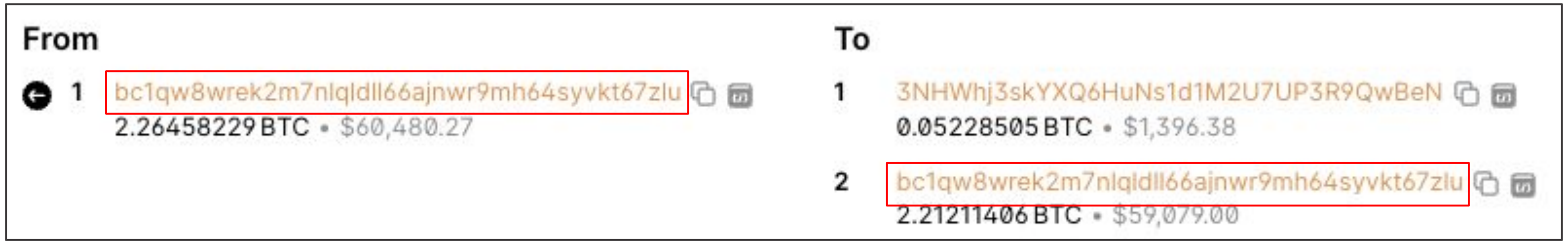
The weight of a transaction is calculated by multiplying the size (in bytes) of different parts of the transaction data by different values

A coinbase transaction is the first transaction in each block

https://www.blockchain.com/explorer/transactions/btc/f43912c4ccbb533618f42b8a66b15b03de4b3b8c49aefc40efa93f3f92735dca

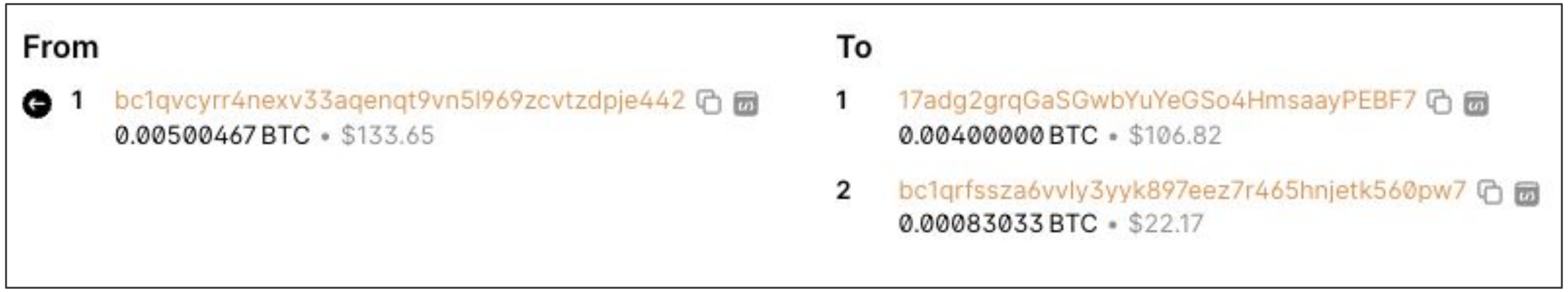
Understand BTC Transactions

Hash:f800ebdb5ebef9ce884158585491b54952efdda044b01f06a4d2b405e65b596a



From	To
1 bc1qw8wrek2m7nlqldll66ajnwr9mh64syvkt67zlu 2.26458229 BTC • $60,480.27	1 3NHWhj3skYXQ6HuNs1d1M2U7UP3R9QwBeN 0.05228505 BTC • $1,396.38
	2 bc1qw8wrek2m7nlqldll66ajnwr9mh64syvkt67zlu 2.21211406 BTC • $59,079.00

Hash: 22621b0e2e279b46206ffc172638521b81e1bb128d136b4c4ea4466346783bda



From	To
1 bc1qvcyrr4nexv33aqenqt9vn5l969zcvtzdpje442 0.00500467 BTC • $133.65	1 17adg2grqGaSGwbYuYeGSo4HmsaayPEBF7 0.00400000 BTC • $106.82
	2 bc1qrfssza6vvly3yyk897eez7r465hnjetk560pw7 0.00083033 BTC • $22.17

Change Address:

Change addresses are an aspect of cryptocurrency that allow users to transact using exact amounts, even if the transaction isn't the total amount of the output being spent.