

2502064303 - Betrand Gabrialdi L
2540123403 - Bertrand Redondo M
2540123100 - Victor Benaya
2540125024 - Felysia Meytri

Crypto Forensic

Short Definition

Crypto forensic merupakan sebuah metode investigasi dimana berfokus pada menganalisis transaksi berbasis blockchain. Transaksi yang dilakukan pada blockchain tidak seperti transaksi bank pada umumnya yang dimana setiap transaksi terbagi menjadi blok-blok unik yang sudah dihash sebelumnya.

Information

Dari proses crypto forensic bisa didapatkan beberapa informasi antara lain:

1. Transaction Mapping: Setiap data yang digunakan dalam bertransaksi dibuat alurnya menjadi sebuah flowchart. Alur dapat berupa endpoint penerima dan pengirim dan pola transaksi antar kedua pelaku seperti peel chains. Hal inilah yang memudahkan para investigator untuk mengungkap kasus pencucian uang.
2. Total Transactions: Jumlah transaksi yang dilakukan pelaku tentunya menjadi hal yang penting dalam proses investigasi dimana semakin banyak transaksi yang dilakukan, maka kemungkinan ia melakukan pencucian uang juga semakin besar.
3. Attribution Data: Dengan menggunakan alat blockchain intelligence, investigator dapat mengumpulkan bukti atau informasi dari berbagai entitas dan address dari pelaku. Informasi yang didapatkan bukan data pribadi, melainkan kelompok kriminal yang ada kaitannya dengan pelaku sehingga memudahkan para investigator untuk mencari pelaku-pelaku lainnya.
4. IP Address: Setiap transaksi yang dilakukan bakal meninggalkan jejak alamat IP pada penerima maupun pengirim. Disini, investigator bisa melacak alamat IP mereka untuk mengetahui lokasi terjadinya transaksi tersebut.

BLOCKCHAIN

Pengertian

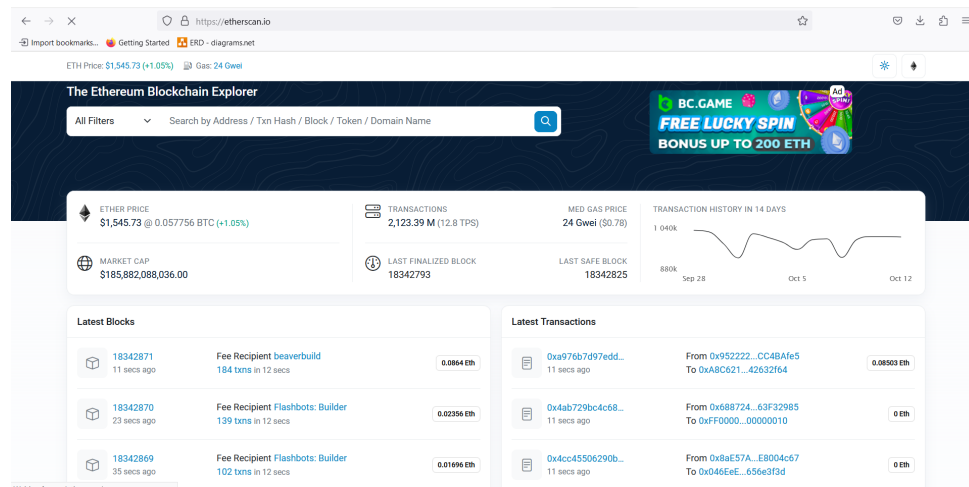
Blockchain merupakan sistem penyimpanan data digital yang berisi catatan yang terhubung melalui kriptografi. Blockchain pada umumnya sering dimanfaatkan oleh berbagai sektor, salah satunya adalah untuk transaksi cryptocurrency atau mata uang kripto seperti Bitcoin.

Jenis Blockchain:

1. Public Blockchain: blockchain yang dapat dibuka dan dapat diakses siapa saja tanpa ada otorisasi khusus
2. Private Blockchain: blockchain yang dibangun dengan tujuan terbatas untuk sekelompok orang atau organisasi yang telah diberi izin khusus.
3. Hybrid Blockchain: gabungan antara public & private blockchain, untuk fleksibilitas kebutuhan bisnis
4. Consortium Blockchain: perantara antara public dan private blockchain.

Tools

<https://etherscan.io/>



Etherscan.io merupakan sebuah website dan tool yang digunakan untuk melakukan analisis blockchain Ethereum.

Dari etherscan, kita dapat melihat detail dari sebuah transaksi

<https://etherscan.io/tx/0x606eb566551e248a5c782b726747977cec779eb872d0dfe85dd28050277060ba>

ETH Price: \$1,546.61 (+0.03%) Gas: 5 Gwei

Search by Address / Txn Hash / Block / Token / Domain Name


Transaction Hash: 0x606eb566551e248a5c782b726747977cec779eb872d0fe85dd28050277060ba

Status: Success

Block: 18348447 1 Block Confirmation

Timestamp: 14 secs ago (Oct-14-2023 11:52:59 AM +UTC)

Transaction Action: Transfer 0.018260029648630082 ETH To 0x068B65...AF3b5195

Sponsored: 

From: 0x95222290DD7278Aa3Ddd389Cc1E1d165CC4BAfe5 (beaverbuild)

To: 0x068B65394EBB0e19DFF45880729C77fAAF3b5195

Value: 0.018260029648630082 ETH (\$28.24)

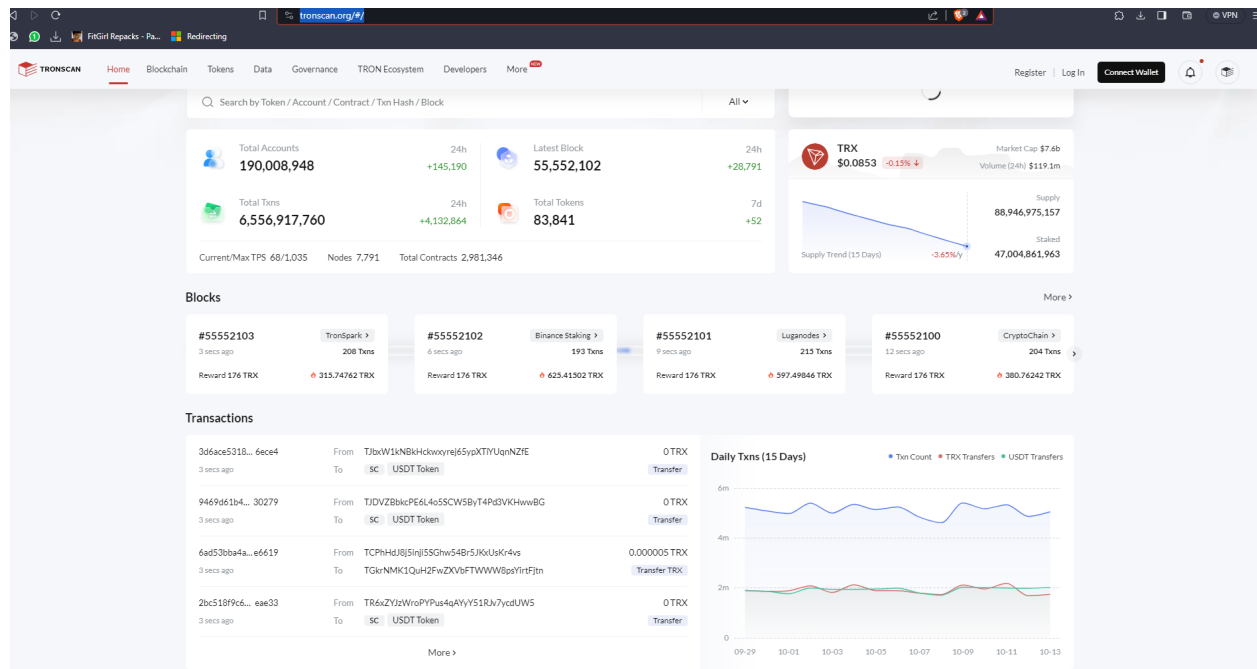
Transaction Fee: 0.000115994184327 ETH (\$0.18)

Gas Price: 5.523532587 Gwei (0.000000005523532587 ETH)

- Transaction Hash: hash unik yang mengidentifikasi transaksi ini di blockchain Ethereum.
- Status: Success, artinya dana telah sukses ditransfer.
- Block: Transaksi ini tercatat di dalam blok nomor 18348447.
- Timestamp: Transaksi ini terjadi pada tanggal 14 Oktober 2023, pukul 11:52:59 AM UTC.
- Transaction Action: Tindakan Transaksi "Transfer" sejumlah 0.018260029648630082 ETH.
- Sponsored: menunjukkan apakah transaksi ini merupakan transaksi yang disponsori atau tidak. Dalam kasus ini, tidak ada sponsor
- From: Address Pengirim 0x95222290DD7278Aa3Ddd389Cc1E1d165CC4BAfe5.
- To: Address Penerima: 0x068B65394EBB0e19DFF45880729C77fAAF3b5195.
- Value: Jumlah ETH yang ditransfer, yaitu 0.018260029648630082 ETH dengan nilai sekitar \$28.24.
- Transaction Fee: Biaya transaksi yang dikenakan, sebesar 0.000115994184327 ETH atau sekitar \$0.18.
- Gas Price: Harga gas yang digunakan dalam transaksi, yaitu 5.523532587 Gwei (0.000000005523532587 ETH).
- Gas Limit & Usage by Txn: Batas gas yang ditetapkan untuk transaksi adalah 32,000, dan penggunaan gas sebesar 21,000 (sekitar 65.63% dari gas yang dialokasikan).
- Gas Fees: Biaya gas yang digunakan dalam transaksi, dengan harga gas dasar sebesar 5.523532587 Gwei.
- Burnt & Txn Savings Fees: Menunjukkan jumlah gas yang dihancurkan selama transaksi dan penghematan biaya transaksi. Dalam kasus ini, 0.000115994184327 ETH terbakar dan tidak ada penghematan biaya transaksi.
- Other Attributes: Jenis transaksi (Txn Type) adalah 2, yang mengacu pada EIP-1559, yang adalah standar perbaikan Ethereum. Nonce adalah 433863, dan transaksi ini berada pada posisi ke-126 dalam blok.
- Input Data: data tambahan yang dapat dimasukkan dalam transaksi, tetapi dalam kasus ini, tidak ada data tambahan yang dimasukkan.

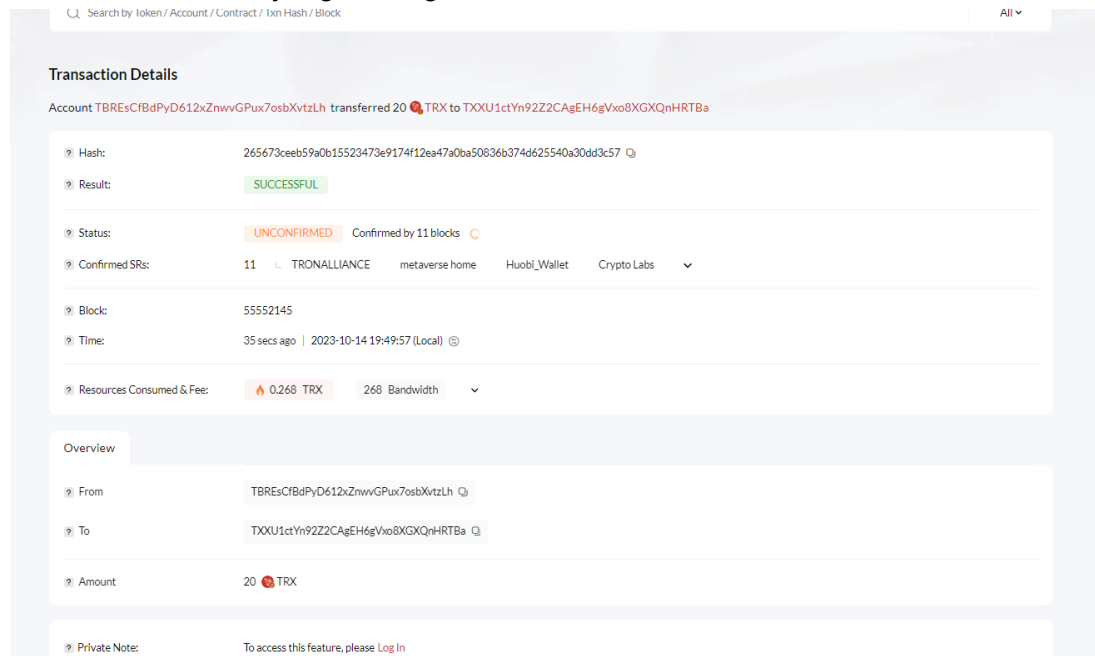
Tools

<https://tronscan.org/#/>



TronScan adalah blockchain explorer untuk jaringan TRON, memungkinkan menganalisis blockchain transaksi TRX, Smart Contracts, dan token activity.

Detail dari transaksi yang sedang kita analisa

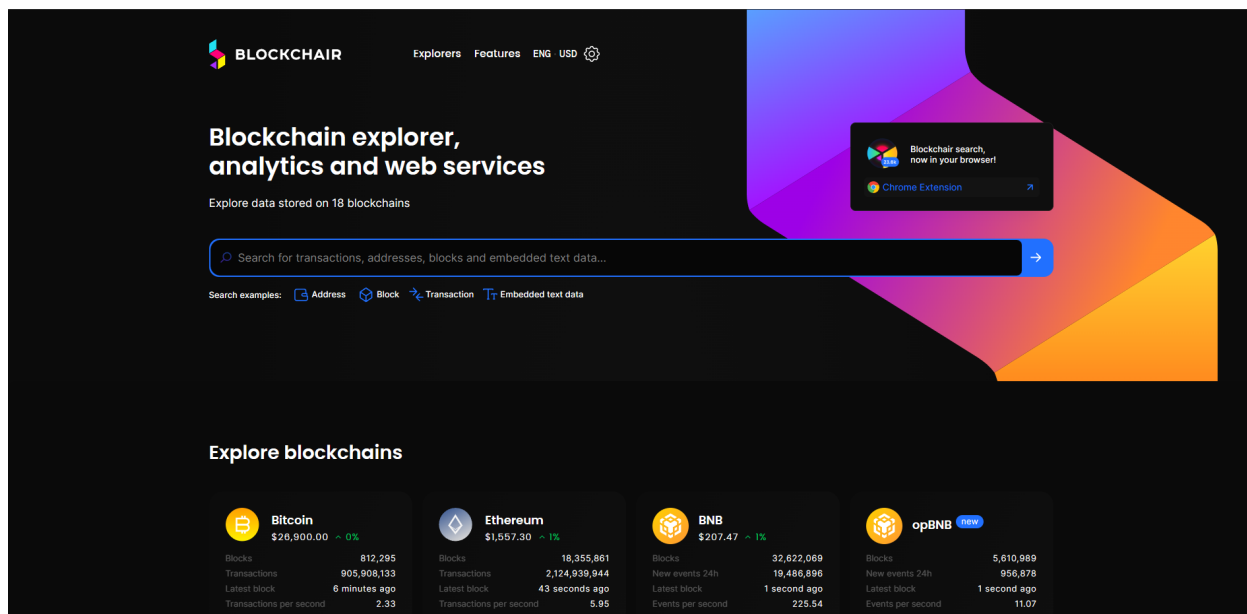


<https://tronscan.org/#/transaction/265673ceeb59a0b15523473e9174f12ea47a0ba50836b374d625540a30dd3c57>

- Hash: Memiliki fungsi untuk memverifikasi transaksi, Data Integrity, Block Identification dan Search & Exploration
- Result: Untuk menunjukan transaksi sukses atau gagal
- Status dan Confirmed SR (Super Representative): 2 ini berkaitan karena SR itu entity yang mengamankan jaringan dan mengelola jaringan, butuh minimal 19 SR untuk konfirmasi agar status suatu transaksi bisa dinyatakan Confirmed.
- Block: Transaksi ini tercatat di dalam blok nomor 55552145
- Time: menunjukan waktu transaksi sudah berlalu dan kapan dimulainya
- Resources Consumed & Fee : Menunjukan berapa banyak resource dan biaya yang dikeluarkan
- From: dikirim dari siapa
- To: dikirim untuk siapa
- Amount : total transaksi atau coin yang dikirim

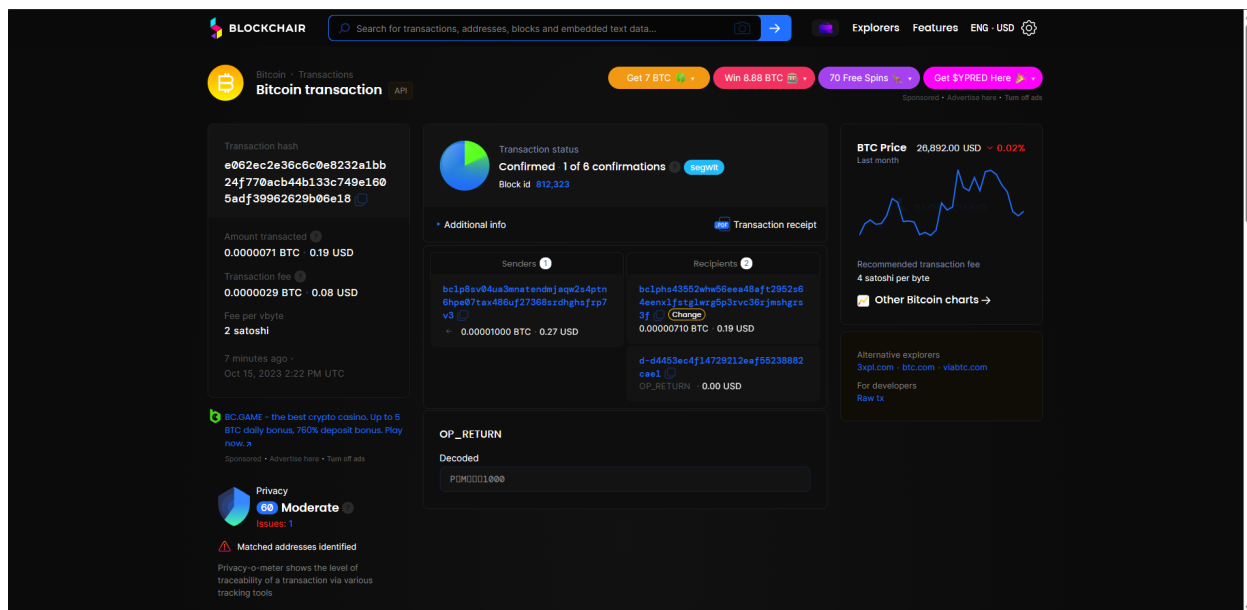
Tools

<https://blockchair.com/>




Blockchair adalah sebuah blockchain search engine dan analytic engine yang dapat digunakan untuk berbagai macam Blockchain seperti bitcoin, ethereum dan lainnya. Engine ini dapat digunakan untuk melakukan analisis detail transaksi dari sebuah cryptocurrency.

Dalam page ini, transaksi sebuah cryptocurrency dapat dilihat secara cukup detail seperti gambar dibawah ini :



Gambar diatas menunjukan detail transaksi sebuah akun Bitcoin

- Transaction hash : Merupakan hash yang merepresentasikan transaksi tersebut
- Amount transacted : Merupakan nominal yang dikirimkan dalam bentuk BitCoin dan USD dengan kurs yang berlaku disaat transaksi dilakukan
- Transaction fee : Merupakan fee transaksi dalam bentuk BitCoin dan USD dengan kurs yang berlaku disaat transaksi dilakukan
- Timestamp : Merupakan tanggal dan waktu transaksi dilakukan
- Transaction Status : Merupakan status transaksi yang menentukan ke sah-an transaksi yang dilakukan. Dibutuhkan 6 konfirmasi untuk menyatakan sebuah transaksi adalah sah.
- Transaction Receipt : Merupakan fitur untuk melakukan *printout* detail transaksi dengan format PDF
- Senders : Merupakan akun pengirim dalam bentuk hash, berserta jumlah yang dikirim dalam bentuk BitCoin dan USD dengan kurs yang berlaku pada saat transaksi berlangsung.
- Recipients : Merupakan akun penerima dalam bentuk hash, berserta jumlah yang dikirim dalam bentuk BitCoin dan USD dengan kurs yang berlaku pada saat transaksi berlangsung.



BLOCKCHAIR
info@blockchair.com
https://blockchair.com

TRANSACTION RECEIPT
BITCOIN

TRANSACTION IDENTIFIER:
e802ec2a38c6b8232a1a024f770eb44b133c749a1085ef39962628b06e18

TRANSACTION TIMESTAMP:
2023-10-10 14:22 (UTC)

CONFIRMED TRANSACTION:
Included in block: #832223 on the Bitcoin blockchain

SENDERS (INPUTS):

#	SENDER	VALUE (BTC)	VALUE (USD)
0	bc1p8v84ux3ematendjgaw2uqpt8hpe87cax48uf27388vcdhghfcp7v3	0.00001000	0.27
→ TOTAL:		0.00001000 BTC	0.27 USD

RECIPIENTS (OUTPUTS):

#	RECIPIENT	VALUE (BTC)	VALUE (USD)
0	bc1phs43852wh0eeaa48a7c2902a64eeenlftglwrgp3rcvc38rjmshgrs3f	0.00000710	0.19
1	d-04403ec4f14729212eaf55238882cael	0.00000000	0.00
+ * * MINER FEE * * *		0.00000290	0.00
→ TOTAL:		0.00001000 BTC	0.19 USD

NOTE

BTC-USD RATE AT THE TIME OF TRANSACTION.
OMNI LAYER BALANCES ARE NOT INCLUDED IN THIS REPORT.

DISCLAIMER

THIS RECEIPT WAS GENERATED AUTOMATICALLY ON 2023-10-10 14:26 (UTC) AND IS BASED ON PUBLIC DATA FROM THE BITCOIN BLOCKCHAIN. BLOCKCHAIR MAKES NEITHER WARRANTY THAT THIS RECEIPT IS FREE OF ERRORS, NOR WARRANTY THAT ITS CONTENT IS ACCURATE. BLOCKCHAIR WILL NOT BE RESPONSIBLE OR LIABLE TO YOU FOR ANY LOSS OF ANY KIND, FROM ACTION TAKEN, OR TAKEN IN RELIANCE ON INFORMATION CONTAINED IN THIS RECEIPT. BLOCKCHAIR IS NEITHER A BANK, NOR A PAYMENT PROCESSOR FOR THIS PAYMENT. BLOCKCHAIR DOES NOT PROVIDE SUPPORT IN CASE OF PROBLEMS ASSOCIATED WITH THIS RECEIPT.



Scan to check the validity of the receipt at [Blockchair.com](https://blockchair.com)

Receipt transaksi