NATIONAL
CONVERGENCE
TECHNOLOGY CENTER

"A Very Quick Introduction to Cryptocurrencies, Blockchains, and Smart Contracts"

Dr. Debasis Bhattacharya
University of Hawaii Maui College

September 22, 2021

This material is based upon work supported by the National Science Foundation under grant number 1700530. Any opinions, findings and conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

UNIVERSITY of HAWAI'I®
MAUI COLLEGE

Collin College Webinar

September 21, 2021

- Debasis Bhattacharya, JD, DBA – UH Maui College, HI
- Mario Canul – former student, UH Maui College, HI
- Saxon Knight – former student, UH Maui College, HI

- http://maui.hawaii.edu/cybersecurity
- debasisb@hawaii.edu
- University of Hawaii Maui College

- Partially supported by NSF ATE Award # 1700562

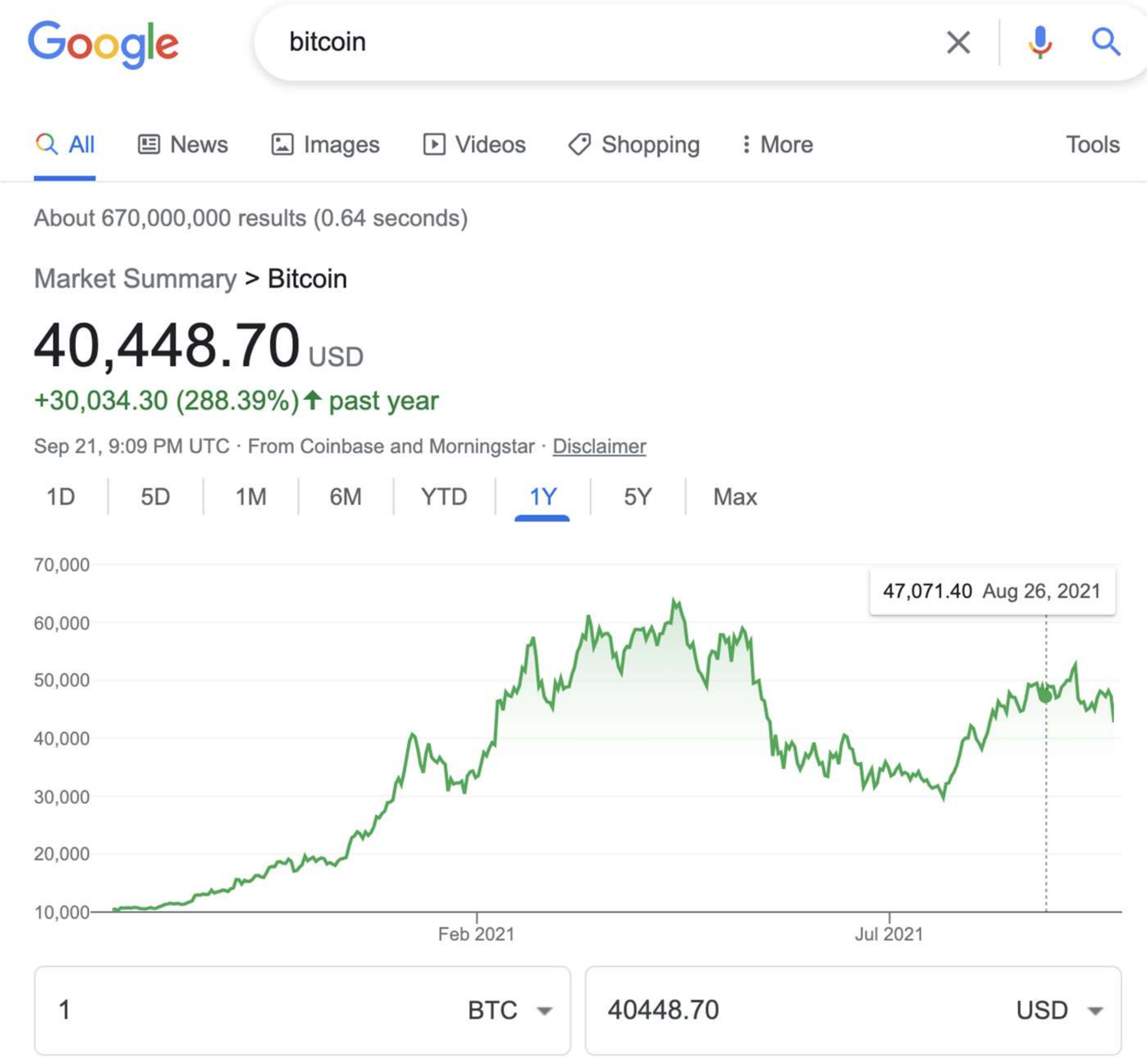
Webinar Objectives

At the completion of this webinar, the participants will be able to…

Describe the basics of the underlying technology behind cryptocurrencies, blockchains, and smart contracts

Prerequisites

A basic understanding of computers, programming, Internet and cryptography.



About 670,000,000 results (0.64 seconds)

Market Summary > Bitcoin

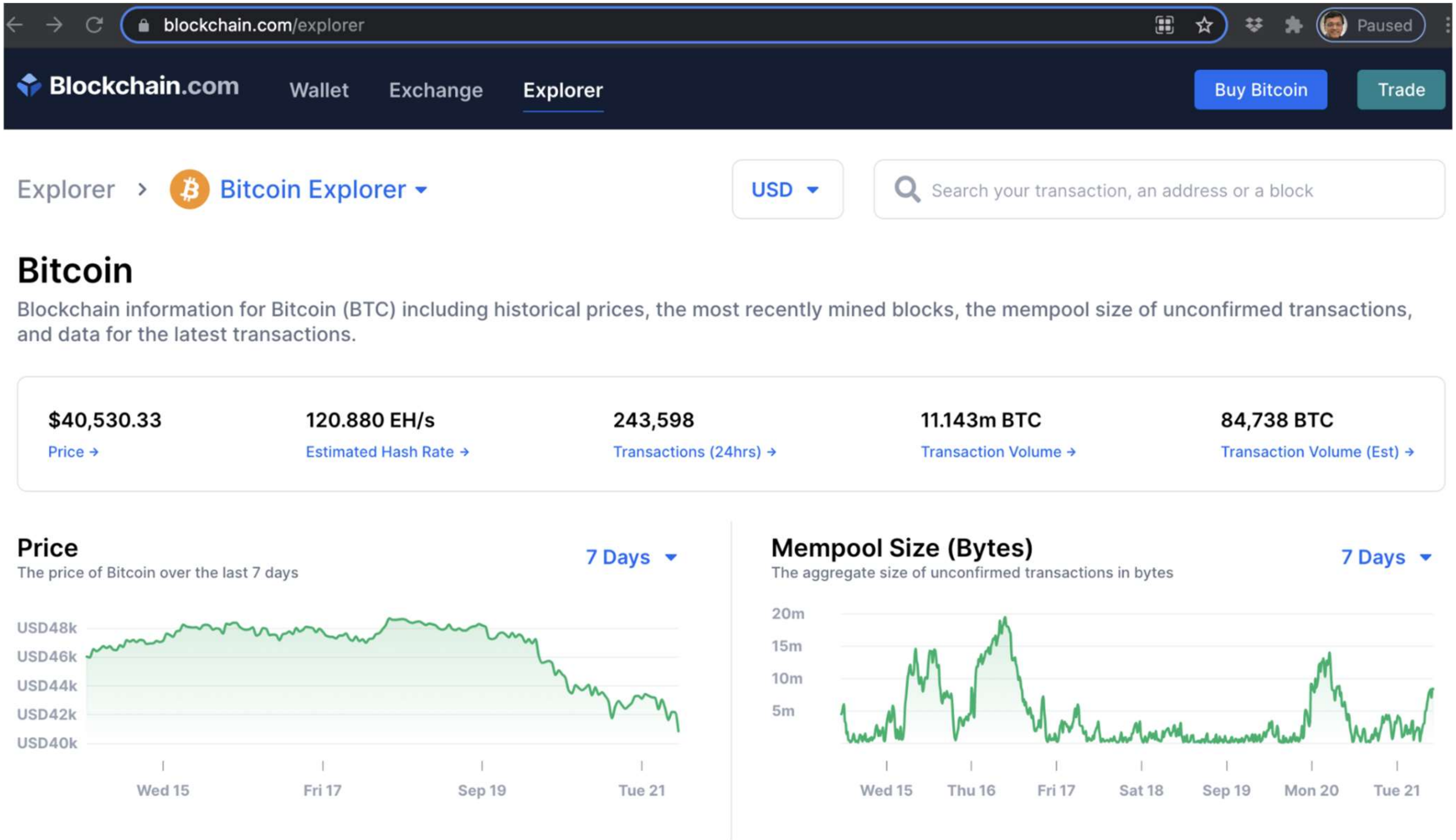
40,448.70 USD

+30,034.30 (288.39%) ↑ past year

Sep 21, 9:09 PM UTC · From Coinbase and Morningstar · Disclaimer

1 BTC

40448.70 USD



Bitcoin

Blockchain information for Bitcoin (BTC) including historical prices, the most recently mined blocks, the mempool size of unconfirmed transactions, and data for the latest transactions.

$40,530.33	120.880 EH/s	243,598	11.143m BTC	84,738 BTC
Price →	Estimated Hash Rate →	Transactions (24hrs) →	Transaction Volume →	Transaction Volume (Est) →

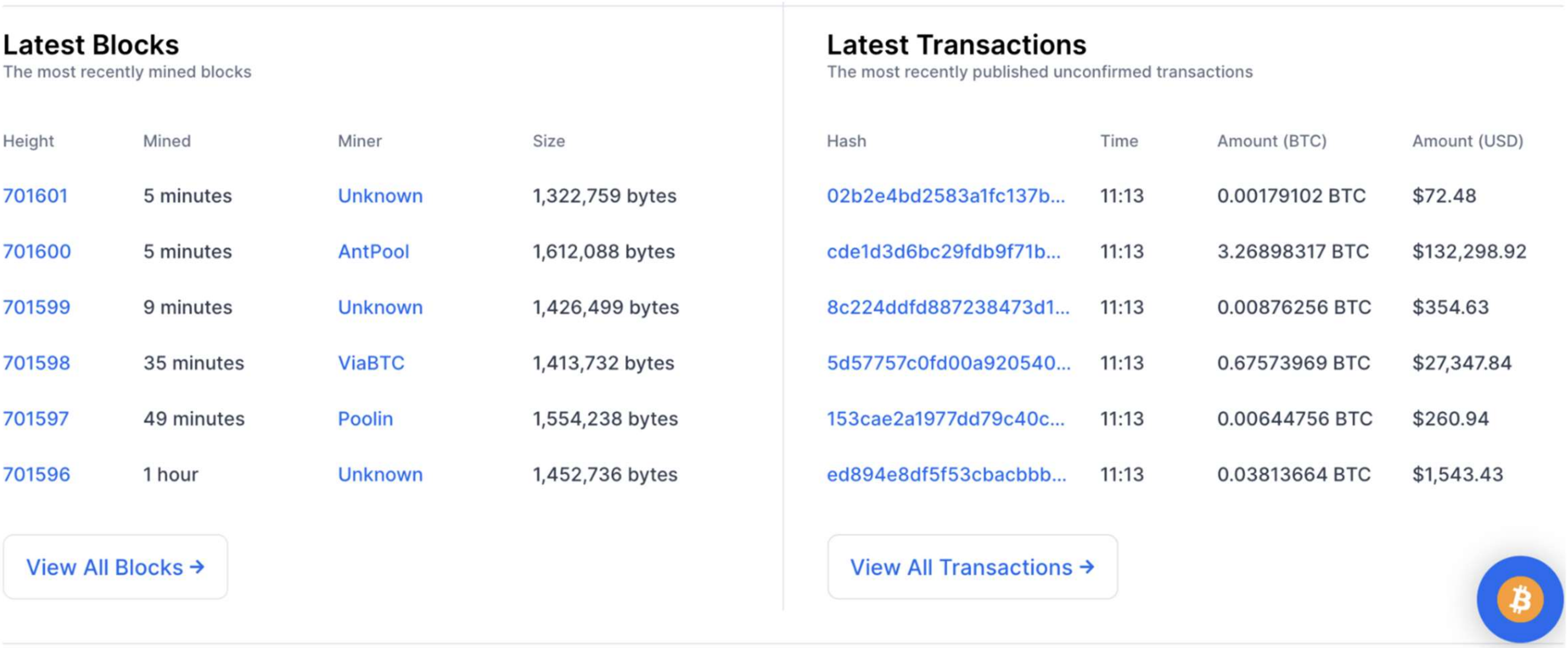
Price

The price of Bitcoin over the last 7 days

Mempool Size (Bytes)

The aggregate size of unconfirmed transactions in bytes

https://www.blockchain.com/explorer



Latest Blocks

The most recently mined blocks

Height	Mined	Miner	Size
701601	5 minutes	Unknown	1,322,759 bytes
701600	5 minutes	AntPool	1,612,088 bytes
701599	9 minutes	Unknown	1,426,499 bytes
701598	35 minutes	ViaBTC	1,413,732 bytes
701597	49 minutes	Poolin	1,554,238 bytes
701596	1 hour	Unknown	1,452,736 bytes

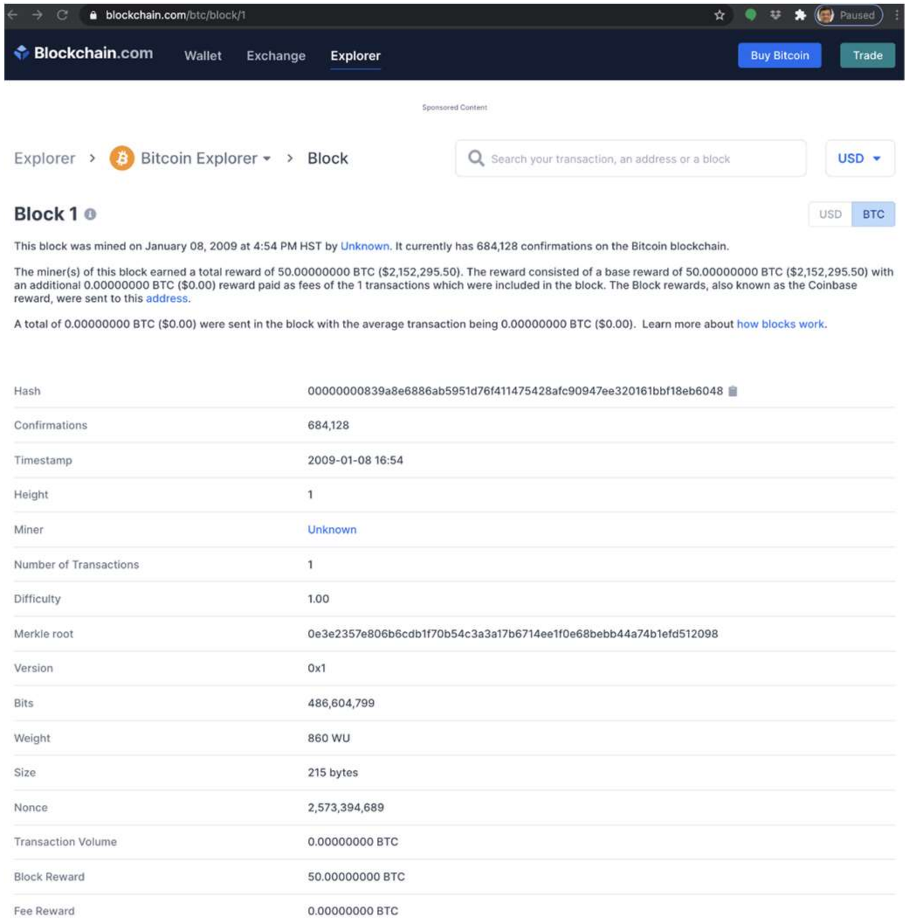
Latest Transactions

The most recently published unconfirmed transactions

Hash	Time	Amount (BTC)	Amount (USD)
02b2e4bd2583a1fc137b...	11:13	0.00179102 BTC	$72.48
cde1d3d6bc29fdb9f71b...	11:13	3.26898317 BTC	$132,298.92
8c224ddfd887238473d1...	11:13	0.00876256 BTC	$354.63
5d57757c0fd00a920540...	11:13	0.67573969 BTC	$27,347.84
153cae2a1977dd79c40c...	11:13	0.00644756 BTC	$260.94
ed894e8df5f53cbacbbb...	11:13	0.03813664 BTC	$1,543.43

https://www.blockchain.com/explorer

Bitcoin Block #1 - 1/8/2009 by Satoshi Nakamoto


blockchain.com/btc/block/1
Paused
Blockchain.com
Wallet
Exchange
Explorer
Buy Bitcoin
Trade
Sponsored Content
Explorer › Bitcoin Explorer › Block
Search your transaction, an address or a block
USD
USD
BTC

Block 1

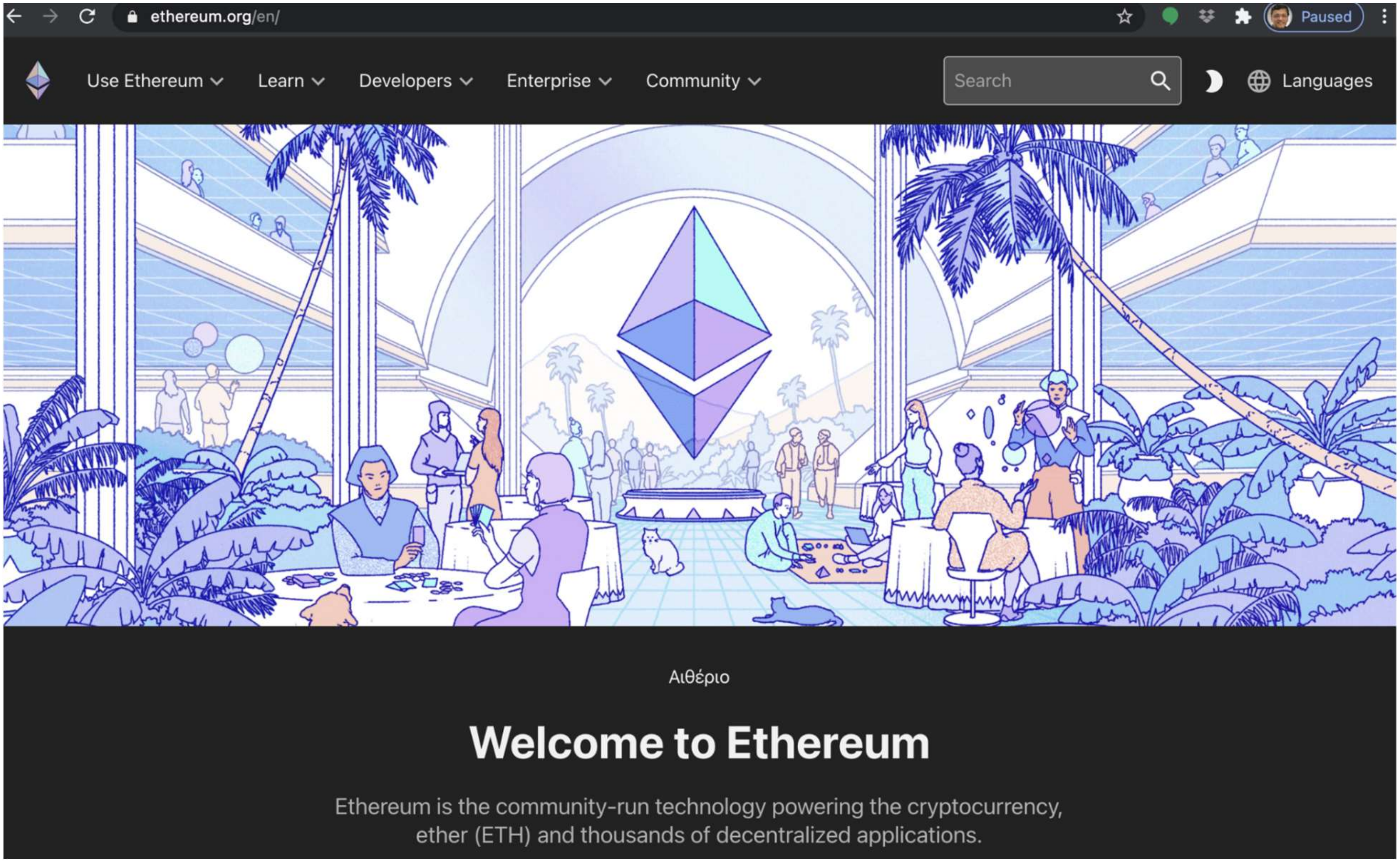
This block was mined on January 08, 2009 at 4:54 PM HST by Unknown. It currently has 684,128 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 50.00000000 BTC ($2,152,295.50). The reward consisted of a base reward of 50.00000000 BTC ($2,152,295.50) with an additional 0.00000000 BTC ($0.00) reward paid as fees of the 1 transactions which were included in the block. The Block rewards, also known as the Coinbase reward, were sent to this address.

A total of 0.00000000 BTC ($0.00) were sent in the block with the average transaction being 0.00000000 BTC ($0.00). Learn more about how blocks work.

Hash	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Confirmations	684,128
Timestamp	2009-01-08 16:54
Height	1
Miner	Unknown
Number of Transactions	1
Difficulty	1.00
Merkle root	0e3e2357e806b6cdb1f70b54c3a3a17b6714ee1f0e68bebb44a74b1efd512098
Version	0x1
Bits	486,604,799
Weight	860 WU
Size	215 bytes
Nonce	2,573,394,689
Transaction Volume	0.00000000 BTC
Block Reward	50.00000000 BTC
Fee Reward	0.00000000 BTC

https://www.blockchain.com/btc/block/1

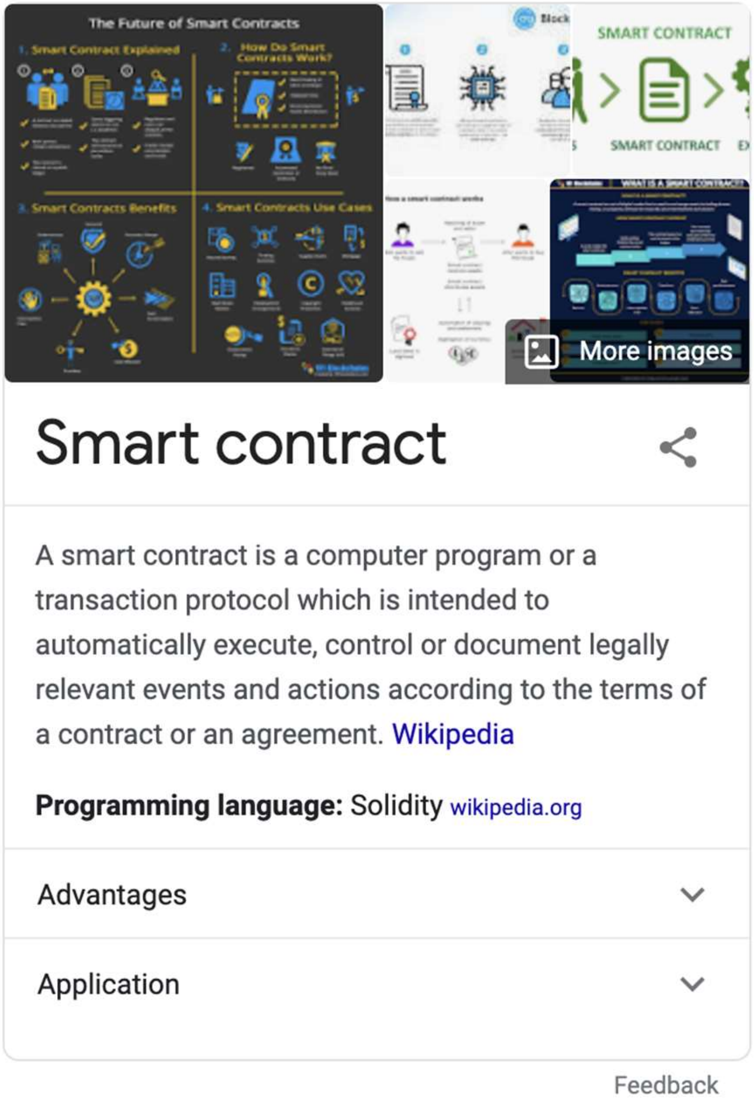


Αιθέριο

Welcome to Ethereum

Ethereum is the community-run technology powering the cryptocurrency, ether (ETH) and thousands of decentralized applications.

https://ethereum.org/en/what-is-ethereum/


The Future of Smart Contracts
1. Smart Contract Explained
2. How Do Smart Contracts Work?
3. Smart Contracts Benefits
4. Smart Contracts Use Cases
SMART CONTRACT
SMART CONTRACT
WHAT IS A SMART CONTRACT?
More images

Smart contract

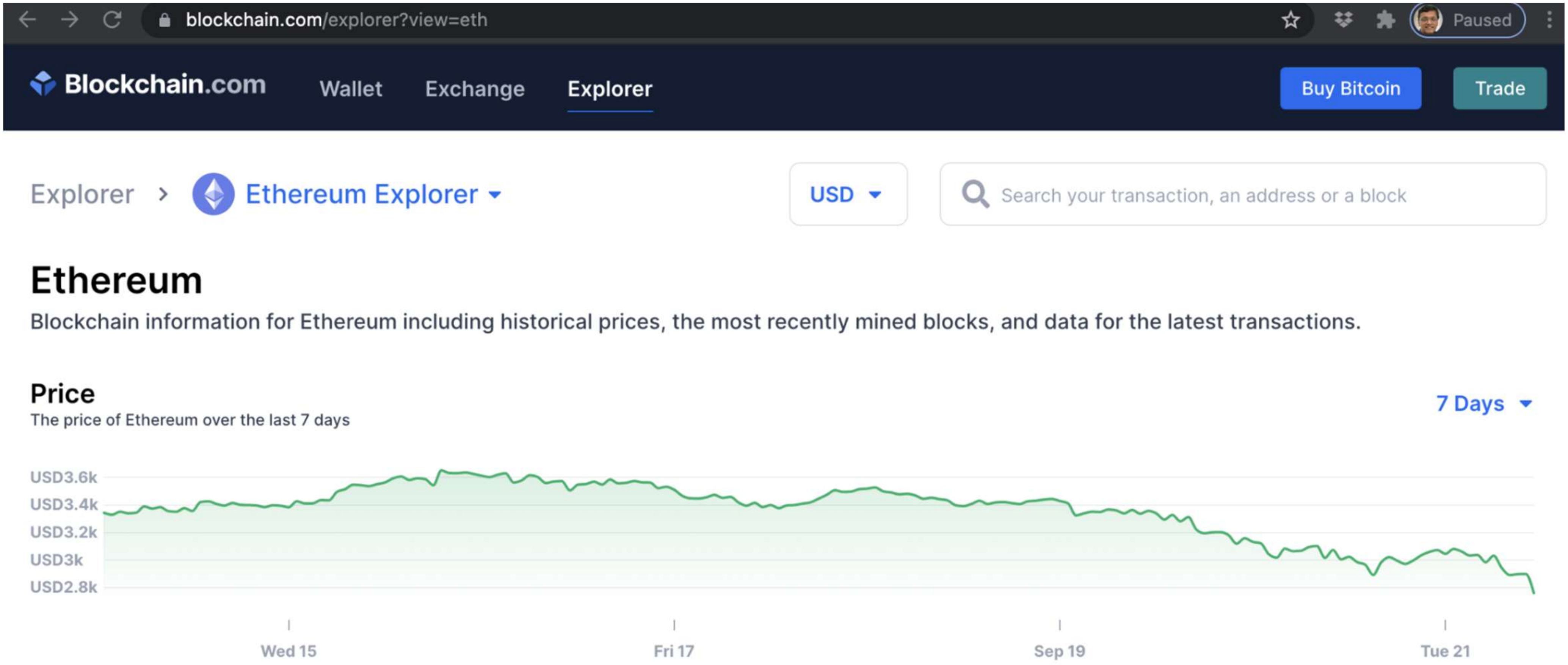
A smart contract is a computer program or a transaction protocol which is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement. Wikipedia

Programming language: Solidity wikipedia.org

Advantages

Application

Feedback



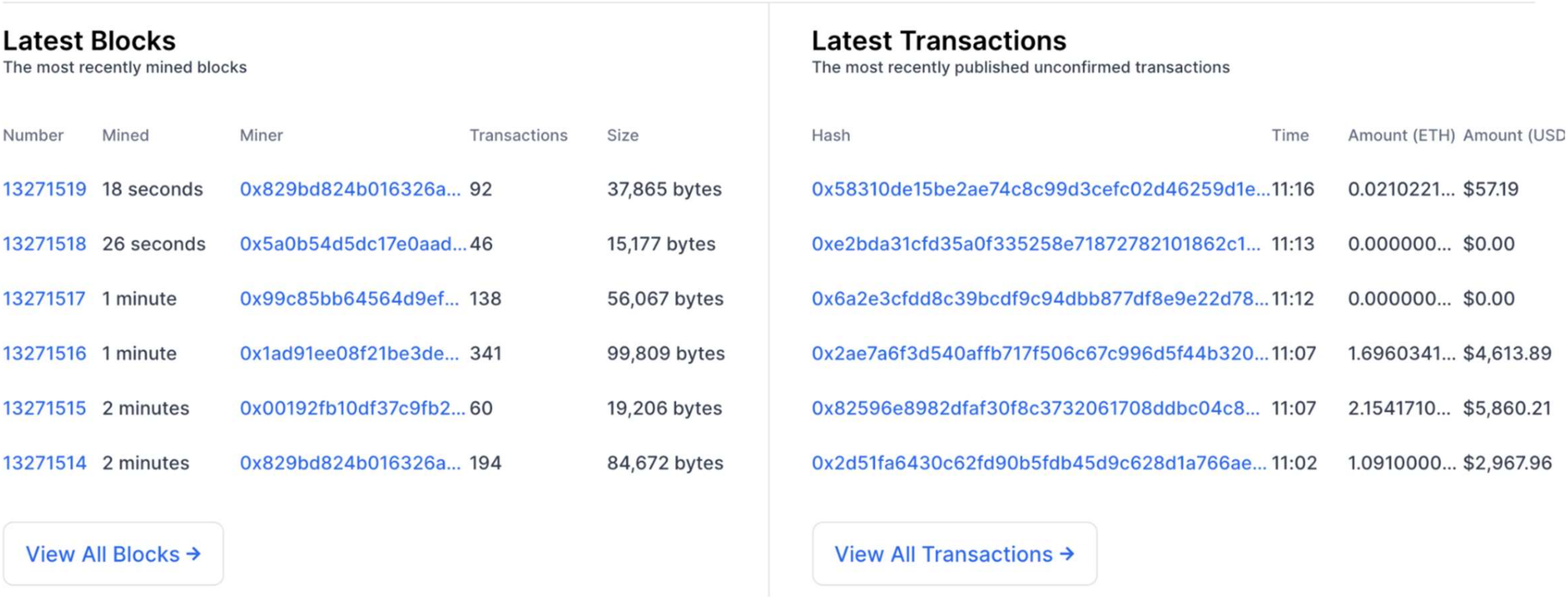
Ethereum

Blockchain information for Ethereum including historical prices, the most recently mined blocks, and data for the latest transactions.

Price

The price of Ethereum over the last 7 days

https://www.blockchain.com/explorer?view=eth



Latest Blocks

The most recently mined blocks

Number	Mined	Miner	Transactions	Size
13271519	18 seconds	0x829bd824b016326a...	92	37,865 bytes
13271518	26 seconds	0x5a0b54d5dc17e0aad...	46	15,177 bytes
13271517	1 minute	0x99c85bb64564d9ef...	138	56,067 bytes
13271516	1 minute	0x1ad91ee08f21be3de...	341	99,809 bytes
13271515	2 minutes	0x00192fb10df37c9fb2...	60	19,206 bytes
13271514	2 minutes	0x829bd824b016326a...	194	84,672 bytes

Latest Transactions

The most recently published unconfirmed transactions

Hash	Time	Amount (ETH)	Amount (USD
0x58310de15be2ae74c8c99d3cefc02d46259d1e...	11:16	0.0210221...	$57.19
0xe2bda31cfd35a0f335258e71872782101862c1...	11:13	0.000000...	$0.00
0x6a2e3cfdd8c39bcdf9c94dbb877df8e9e22d78...	11:12	0.000000...	$0.00
0x2ae7a6f3d540affb717f506c67c996d5f44b320...	11:07	1.6960341...	$4,613.89
0x82596e8982dfaf30f8c3732061708ddbc04c8...	11:07	2.1541710...	$5,860.21
0x2d51fa6430c62fd90b5fdb45d9c628d1a766ae...	11:02	1.0910000...	$2,967.96

https://www.blockchain.com/explorer?view=eth

Currencies - Online Transactions

- Physical cash
  - Non-traceable (well, mostly!)
  - Secure (mostly)
  - Low inflation
- Fiat Currency – legal tender whose value is backed by a government
  - Note that since 1971, the US$ has no backing with gold!
  - Cryptocurrencies are not fiat currencies!
- Physical currencies can’t be used online directly

➢Electronic credit or debit transactions

  ◆Bank sees all transactions

  ◆Merchants can track/profile customers

  ◆Cryptocurrencies are not associated with any bank or regulatory agency!

Bitcoin

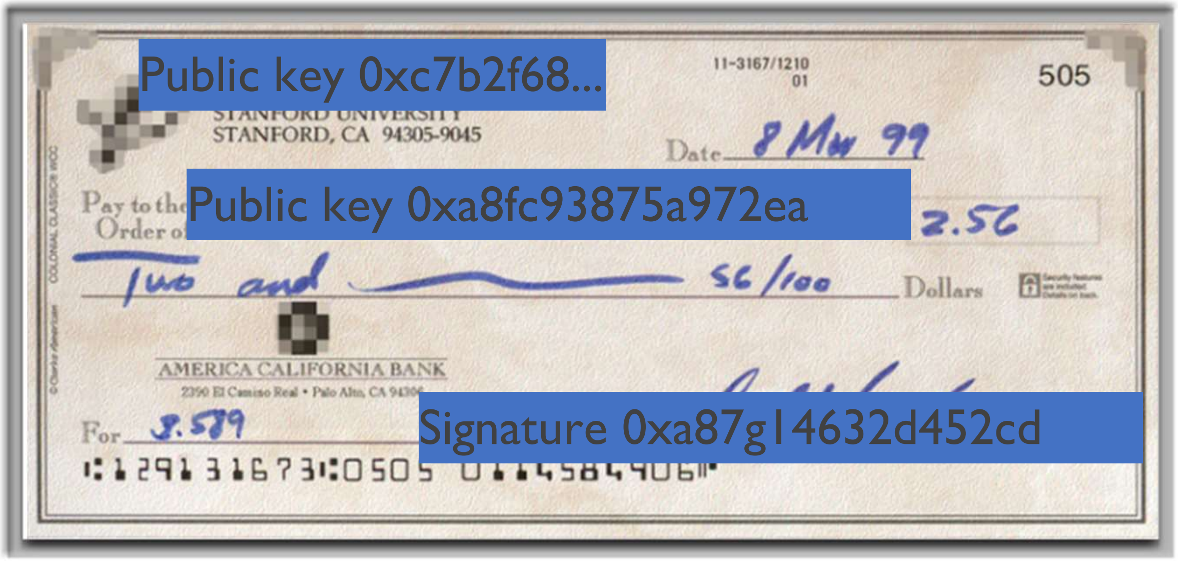
- A distributed, decentralized digital currency system
- Released by Satoshi Nakamoto 2008
- Effectively a bank run by an ad hoc network
  - Digital checks
  - A distributed transaction log

Size of the BitCoin Economy

- Number of BitCoins in circulation ~18.82 million (September 2021)
- Total number of BitCoins generated cannot exceed 21 million.
  - New blocks created every 10 minutes.
  - Currently, each block adds 6.25 bitcoins into circulation
  - Mining will end in the year 2140…
- Average price of a Bitcoin:
  - $43,819.54 on September 21, 2021
  - $43,045.91 on May 18, 2021
  - $10,360.45 on July 1, 2019
  - $4,110 on February 23, 2019
  - $3,729 on Dec 29, 2018
  - $8,522 on May 15, 2018
  - $18,000 on December, 2017
  - $3,867 on September 25, 2017
  - $2,350 on June 27, 2017

  □ Price has been very unstable and speculative.
- Currently, 244,157 tx/day or ~170 tx/minute.
  (In contrast, Visa transaction 200,000 per minute!)

Bitcoin Transactions



Public key 0xc7b2f68...

STANFORD UNIVERSITY
STANFORD, CA 94305-9045

11-3167/1210
01

505

Date 8 Mar 99

Pay to the Order of Public key 0xa8fc93875a972ea

2.56

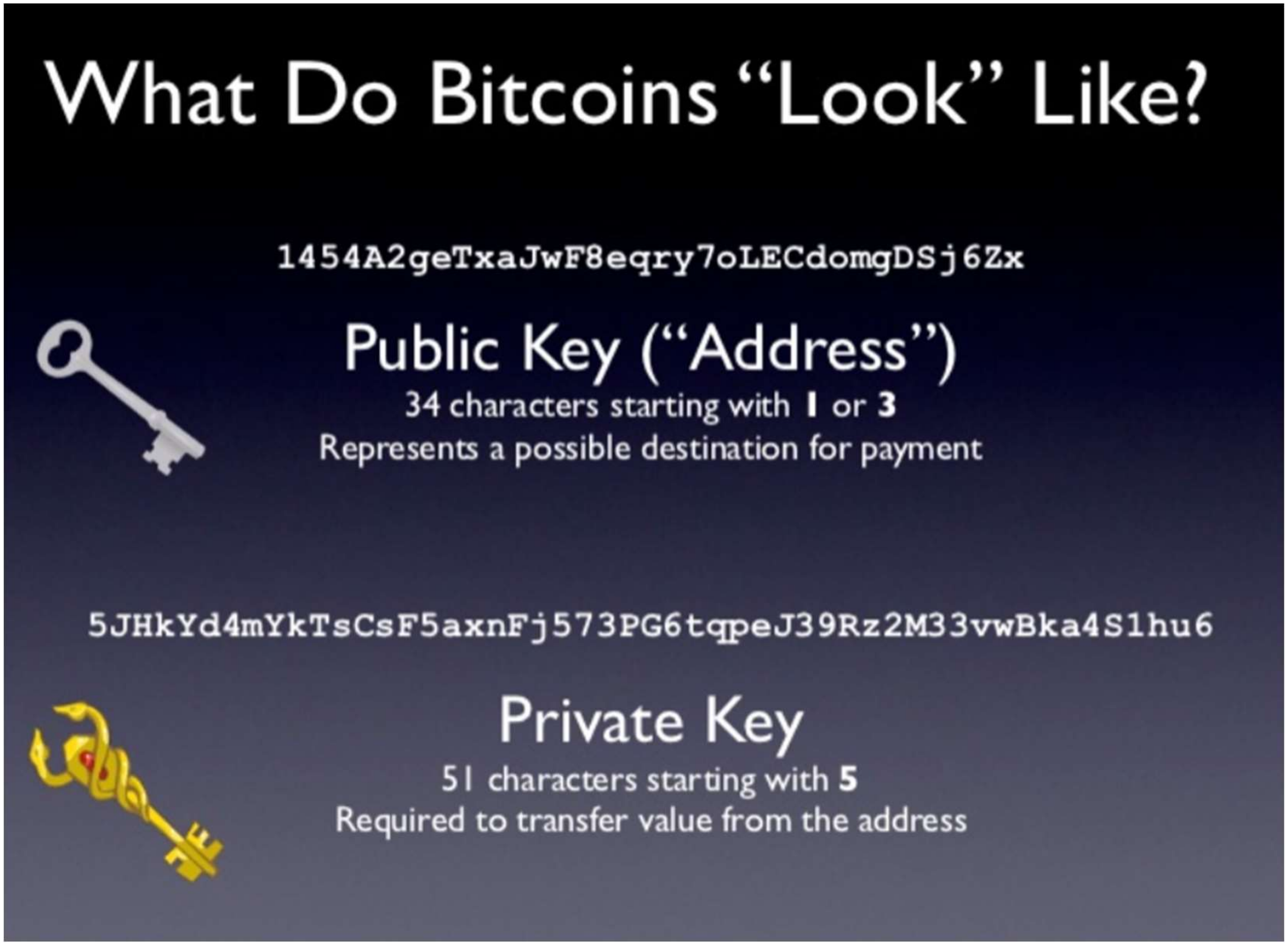
Two and ——— 56/100 Dollars

AMERICA CALIFORNIA BANK
2350 El Camino Real • Palo Alto, CA 94306

For 8.589

Signature 0xa87g14632d452cd

⑆1291 31673⑆0505 0114584406⑈



What Do Bitcoins "Look" Like?

1454A2geTxaJwF8eqry7oLECdomgDSj6Zx

Public Key ("Address")

34 characters starting with **1** or **3**

Represents a possible destination for payment

5JHkYd4mYkTsCsF5axnFj573PG6tqpeJ39Rz2M33vwBka4S1hu6

Private Key

51 characters starting with **5**

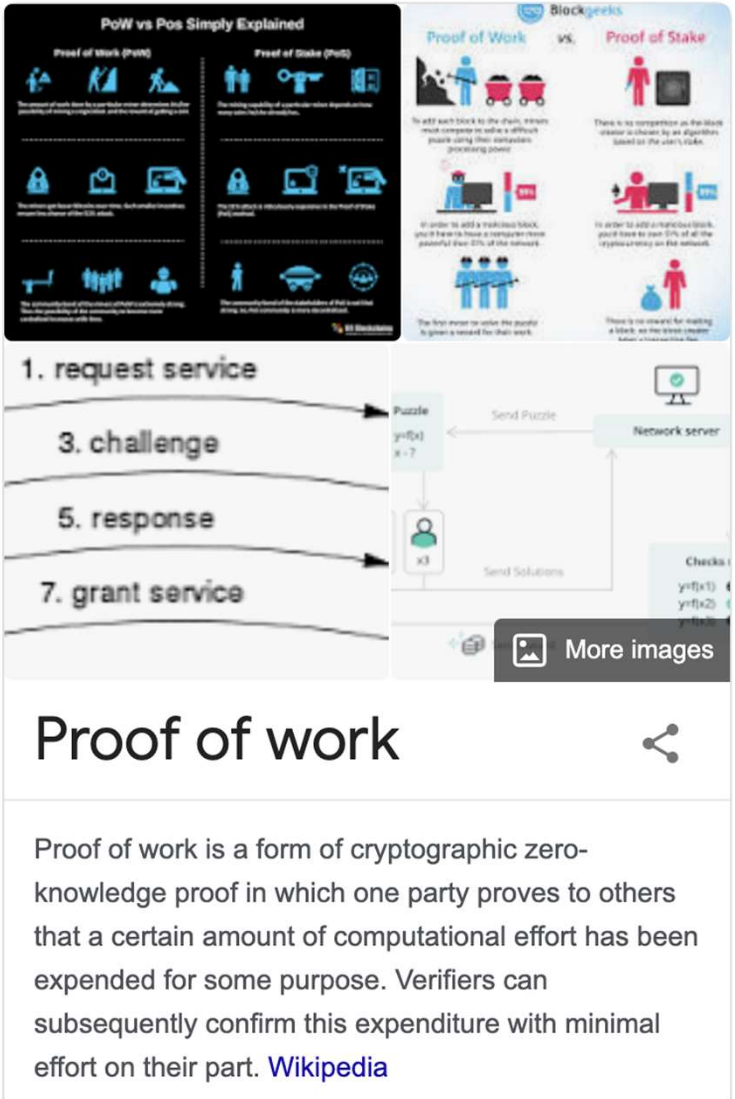
Required to transfer value from the address

Bitcoin Network

- Each P2P node runs the following algorithm:
  - New transactions are broadcast to all nodes.
  - Each node (miners) collects new transactions into a block.
  - Each node works on finding a proof-of-work for its block. (Hard to do. Probabilistic. The one to finish early will probably win.)
  - When a node finds a proof-of-work, it broadcasts the block to all nodes.
  - Nodes accept the block only if all transactions in it are valid (digital signature checking) and not already spent (check all the transactions).
  - Nodes express their acceptance by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

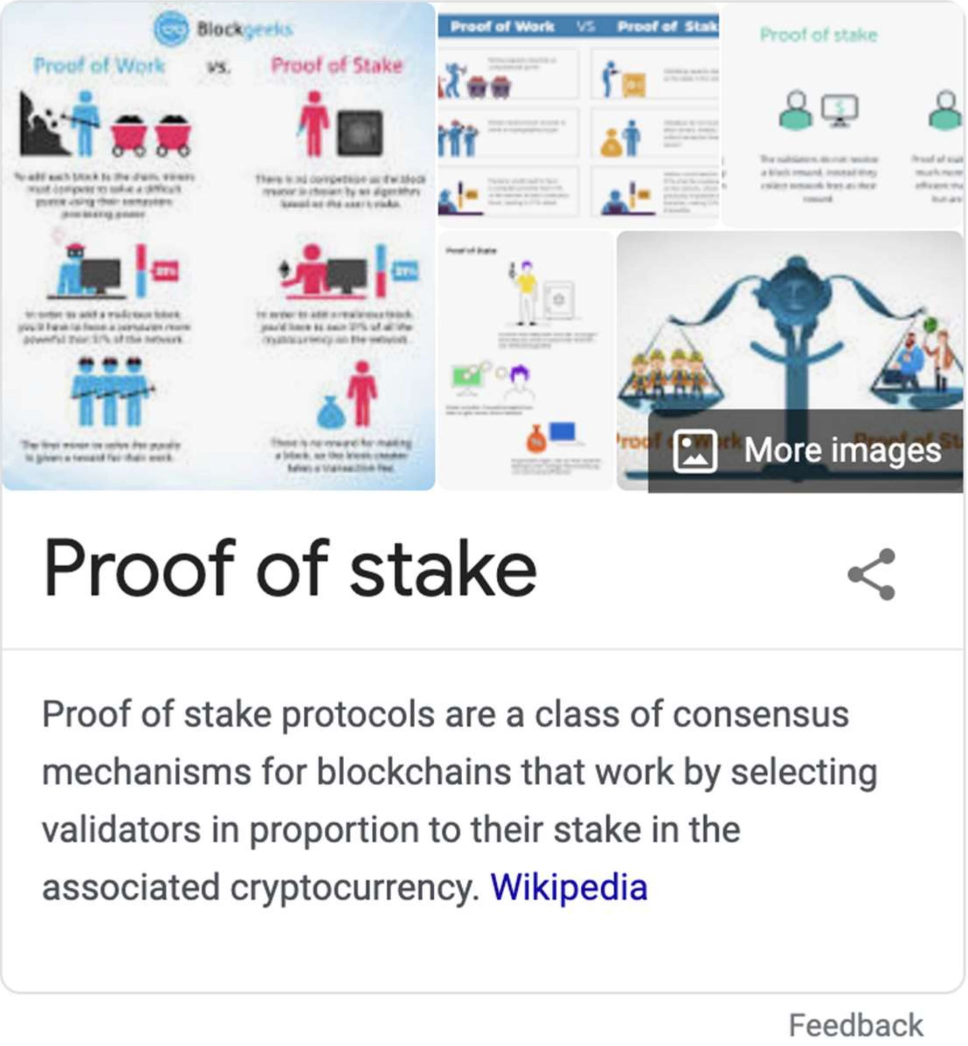
BitCoin: Challenges

- Creation of a virtual coin/note
  - How is it created in the first place?
  - How do you prevent inflation? (What prevents anyone from creating lots of coins?)
- Validation
  - Is the coin legit? (proof-of-work)
  - How do you prevent a coin from double-spending?
- Buyer and Seller protection in online transactions
  - Buyer pays, but the seller doesn’t deliver
  - Seller delivers, buyer pays, but the buyer makes a claim.
- Trust on third-parties
  - Rely on “proof of work” instead of trust
  - Verifiable by everyone – blockchain is visible to all
  - No central bank or clearing house



Proof of work

Proof of work is a form of cryptographic zero-knowledge proof in which one party proves to others that a certain amount of computational effort has been expended for some purpose. Verifiers can subsequently confirm this expenditure with minimal effort on their part. Wikipedia



Proof of stake

Proof of stake protocols are a class of consensus mechanisms for blockchains that work by selecting validators in proportion to their stake in the associated cryptocurrency. Wikipedia

Back to BitCoin

- Validation
  - Is the coin legit? (proof-of-work) → Use of Cryptographic Hashes
  - How do you prevent a coin from double-spending? → Broadcast to all nodes
- Creation of a virtual coin/note
  - How is it created in the first place? → Provide incentives for miners, earn bitcoins after work!
  - How do you prevent inflation? (What prevents anyone from creating lots of coins?) → Limit the creation rate of the BitCoins. Right now, 6.25 coins to miners as of June 2020

Security in Bitcoin

- Authentication
  - Am I paying the right person? Not some other impersonator?
- Integrity
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- Availability
  - Can I make a transaction anytime I want?
- Confidentiality
  - Are my transactions private? Anonymous?

Security in Bitcoin

- Authentication → Public Key Crypto: Digital Signatures
  - Am I paying the right person? Not some other impersonator?
- Integrity → Digital Signatures and Cryptographic Hash
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- Availability→ Broadcast messages to the P2P network
  - Can I make a transaction anytime I want?
- Confidentiality→ Pseudonymity
  - Are my transactions private? Anonymous?

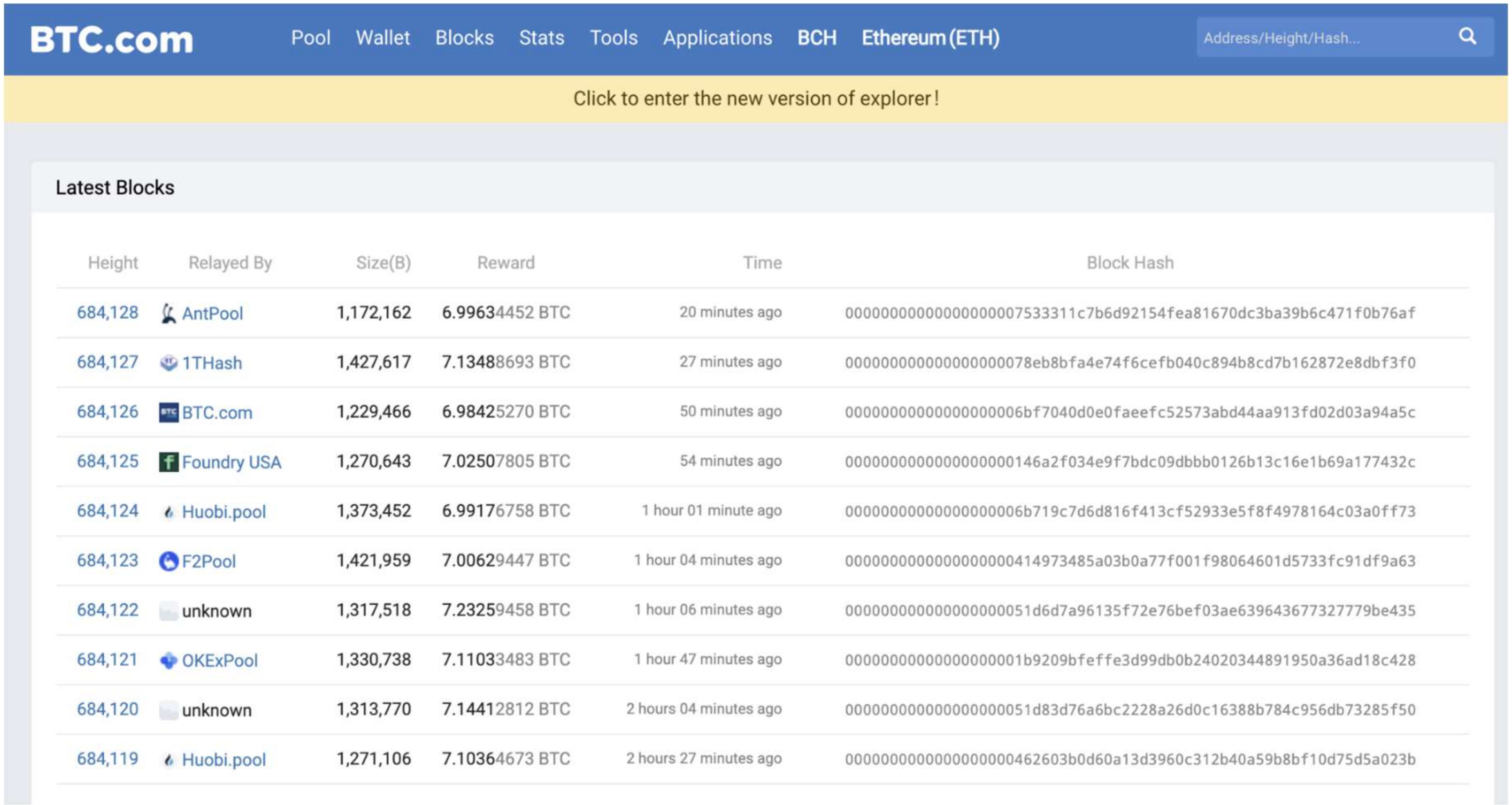
Practical Limitation

- At least 10 minutes to verify a transaction.
  - Agree to pay
  - Wait for one block (10 mins) for the transaction to go through.
  - But, for a large transaction ($$$) wait longer, around 60 minutes. Because if you wait longer it becomes more secure.
  - For large $$$, you wait for six blocks (1 hour).

Bitcoin Economics

- Rate limiting on the creation of a new block
  - Adapt to the "network's capacity"
  - A block created every 10 mins (six blocks every hour)
    - How? Difficulty is adjusted every two weeks to keep the rate fixed as capacity/computing power increases
- N new Bitcoins per each new block: credited to the miner → incentives for miners
  - N was 50 initially. In 2013, N=25
  - Since 2016 N = 12.5, next half is June 2020 for N = 6.25.
  - Halved every 210,000 blocks (every four years) till 2140 when all mining will end
  - Thus, the total number of BitCoins will not exceed 21 million. (After this miner takes a fee)

Mining Pools - www.btc.com



Click to enter the new version of explorer!

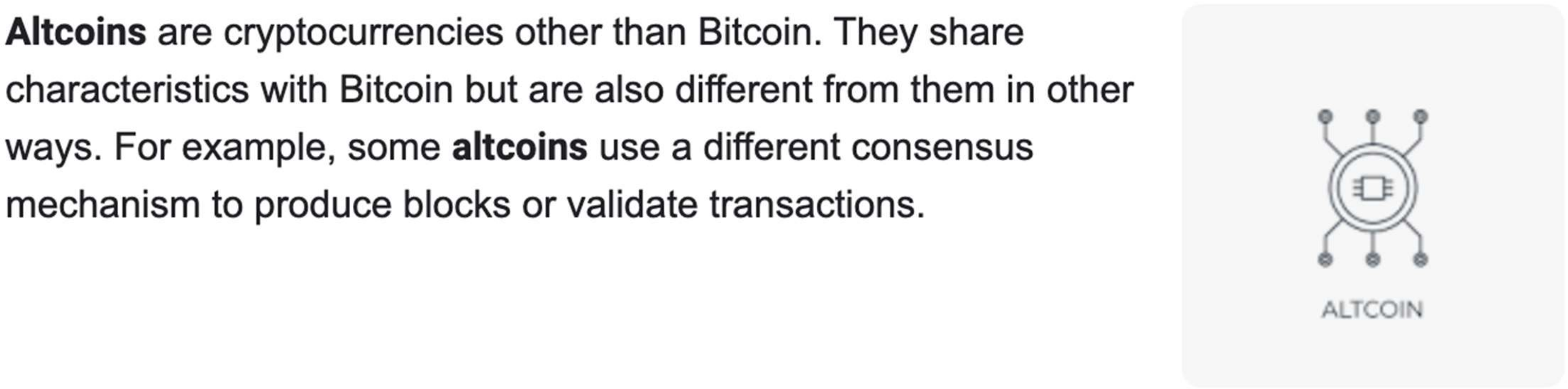
Latest Blocks

Height	Relayed By	Size(B)	Reward	Time	Block Hash
684,128	AntPool	1,172,162	6.99634452 BTC	20 minutes ago	00000000000000000007533311c7b6d92154fea81670dc3ba39b6c471f0b76af
684,127	1THash	1,427,617	7.13488693 BTC	27 minutes ago	000000000000000000078eb8bfa4e74f6cefb040c894b8cd7b162872e8dbf3f0
684,126	BTC.com	1,229,466	6.98425270 BTC	50 minutes ago	00000000000000000006bf7040d0e0faeefc52573abd44aa913fd02d03a94a5c
684,125	Foundry USA	1,270,643	7.02507805 BTC	54 minutes ago	0000000000000000000146a2f034e9f7bdc09dbbb0126b13c16e1b69a177432c
684,124	Huobi.pool	1,373,452	6.99176758 BTC	1 hour 01 minute ago	00000000000000000006b719c7d6d816f413cf52933e5f8f4978164c03a0ff73
684,123	F2Pool	1,421,959	7.00629447 BTC	1 hour 04 minutes ago	0000000000000000000414973485a03b0a77f001f98064601d5733fc91df9a63
684,122	unknown	1,317,518	7.23259458 BTC	1 hour 06 minutes ago	000000000000000000051d6d7a96135f72e76bef03ae639643677327779be435
684,121	OKExPool	1,330,738	7.11033483 BTC	1 hour 47 minutes ago	00000000000000000001b9209bfeffe3d99db0b24020344891950a36ad18c428
684,120	unknown	1,313,770	7.14412812 BTC	2 hours 04 minutes ago	000000000000000000051d83d76a6bc2228a26d0c16388b784c956db73285f50
684,119	Huobi.pool	1,271,106	7.10364673 BTC	2 hours 27 minutes ago	0000000000000000000462603b0d60a13d3960c312b40a59b8bf10d75d5a023b

Privacy Implications

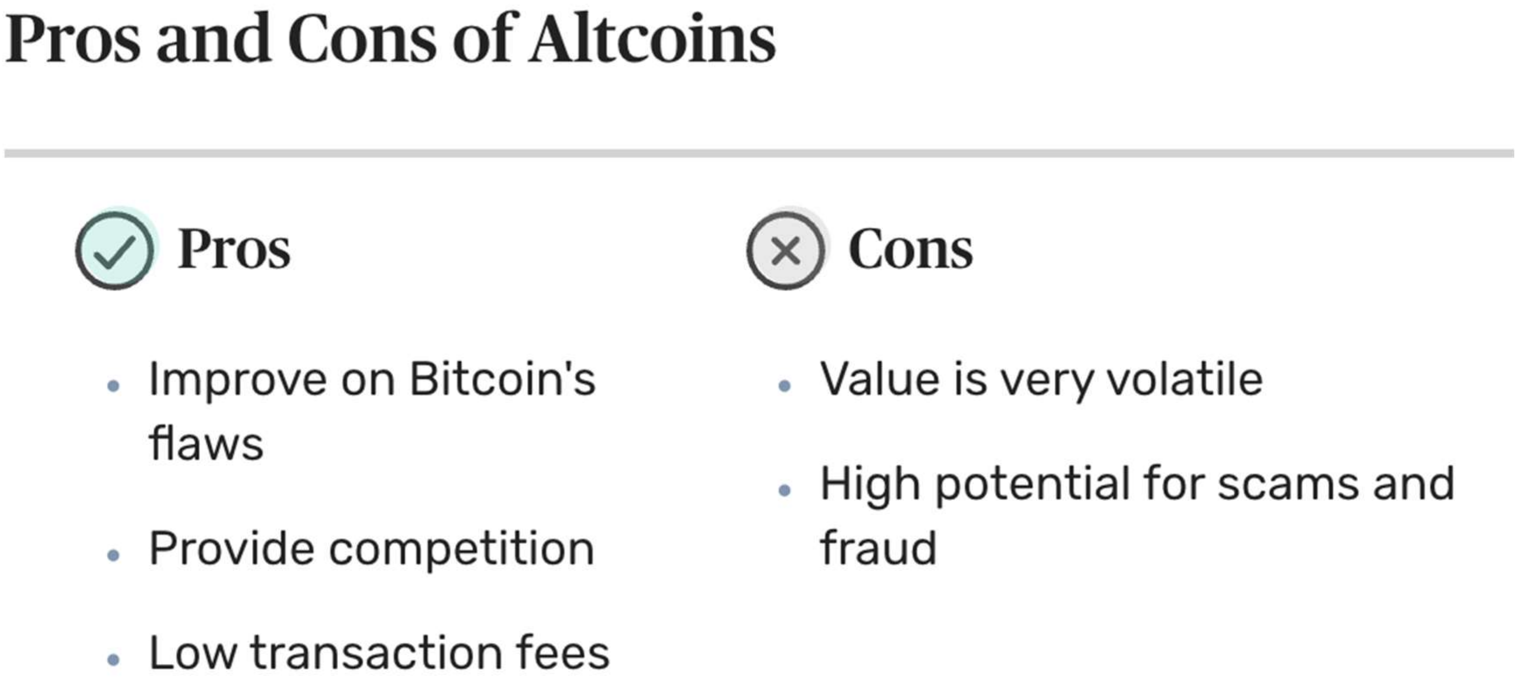
- No anonymity, only pseudonymity
- All transactions remain on the block chain– indefinitely!
- Retroactive data mining
  - Target used data mining on customer purchases to identify pregnant women and target ads at them (NYT 2012), ended up informing a woman's father that his teenage daughter was pregnant
  - Imagine what credit card companies could do with the data

Alternative Crypto Coins - Altcoins



Altcoins are cryptocurrencies other than Bitcoin. They share characteristics with Bitcoin but are also different from them in other ways. For example, some **altcoins** use a different consensus mechanism to produce blocks or validate transactions.

Altcoins



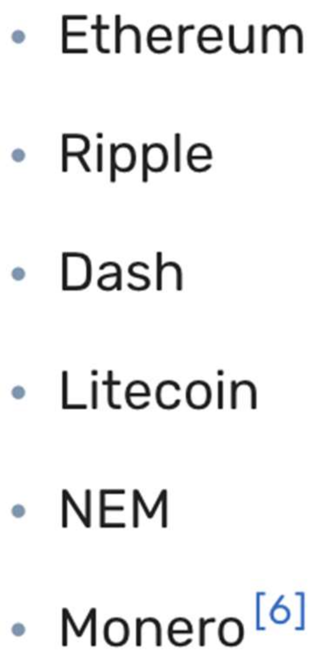
Pros and Cons of Altcoins

✓ Pros

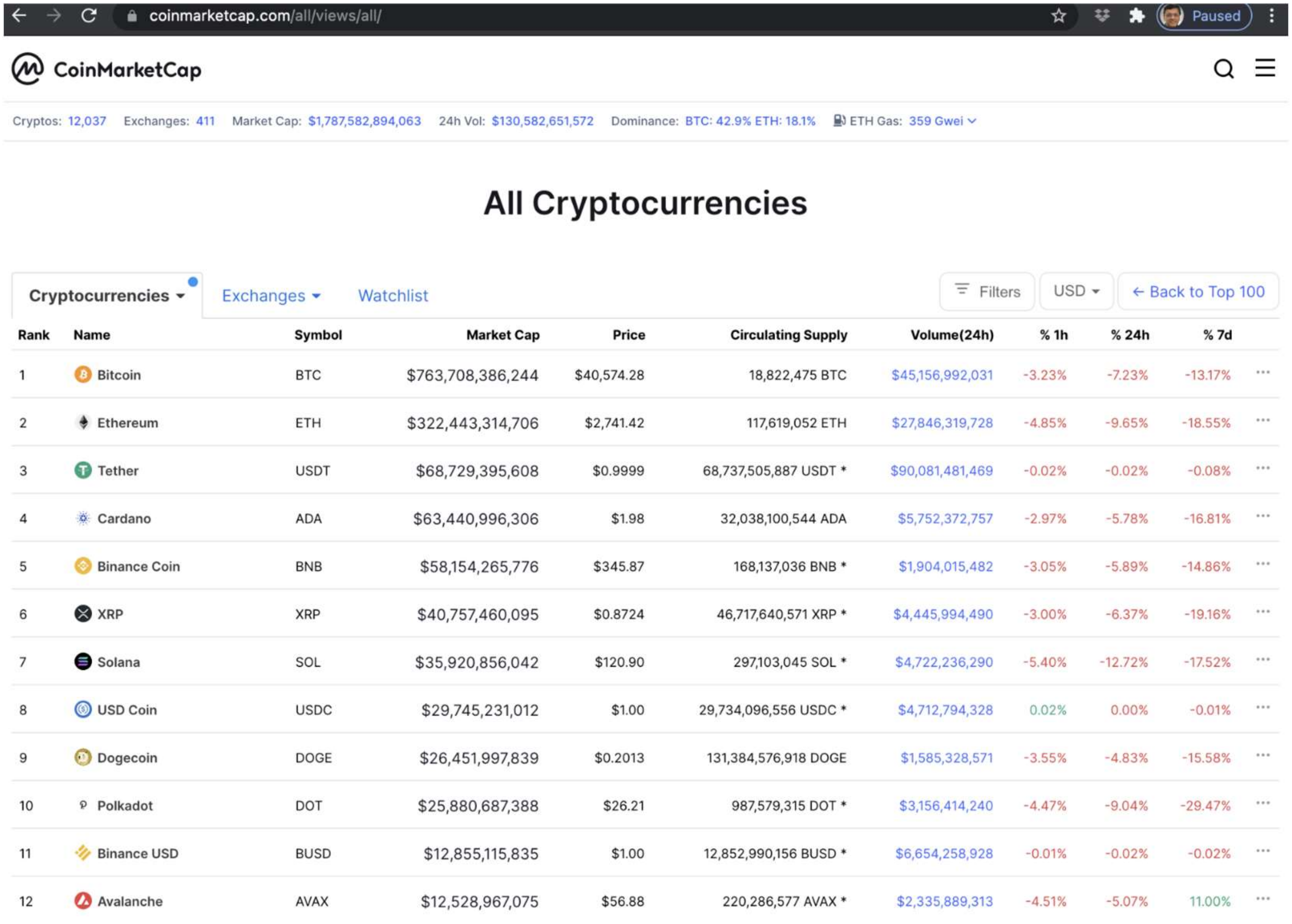
- Improve on Bitcoin's flaws
- Provide competition
- Low transaction fees

✗ Cons

- Value is very volatile
- High potential for scams and fraud



- Ethereum
- Ripple
- Dash
- Litecoin
- NEM
- Monero[6]



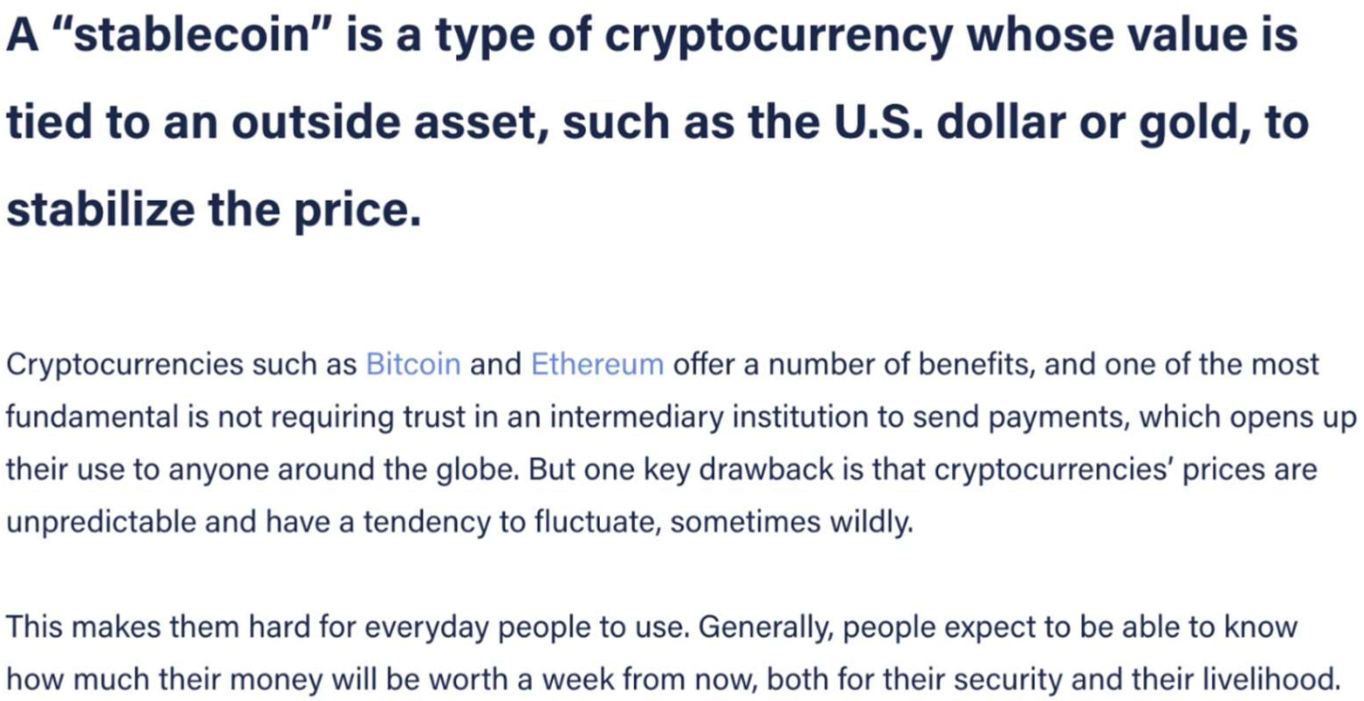
Cryptos: 12,037 Exchanges: 411 Market Cap: $1,787,582,894,063 24h Vol: $130,582,651,572 Dominance: BTC: 42.9% ETH: 18.1% ETH Gas: 359 Gwei

All Cryptocurrencies

Rank	Name	Symbol	Market Cap	Price	Circulating Supply	Volume(24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$763,708,386,244	$40,574.28	18,822,475 BTC	$45,156,992,031	-3.23%	-7.23%	-13.17%
2	Ethereum	ETH	$322,443,314,706	$2,741.42	117,619,052 ETH	$27,846,319,728	-4.85%	-9.65%	-18.55%
3	Tether	USDT	$68,729,395,608	$0.9999	68,737,505,887 USDT *	$90,081,481,469	-0.02%	-0.02%	-0.08%
4	Cardano	ADA	$63,440,996,306	$1.98	32,038,100,544 ADA	$5,752,372,757	-2.97%	-5.78%	-16.81%
5	Binance Coin	BNB	$58,154,265,776	$345.87	168,137,036 BNB *	$1,904,015,482	-3.05%	-5.89%	-14.86%
6	XRP	XRP	$40,757,460,095	$0.8724	46,717,640,571 XRP *	$4,445,994,490	-3.00%	-6.37%	-19.16%
7	Solana	SOL	$35,920,856,042	$120.90	297,103,045 SOL *	$4,722,236,290	-5.40%	-12.72%	-17.52%
8	USD Coin	USDC	$29,745,231,012	$1.00	29,734,096,556 USDC *	$4,712,794,328	0.02%	0.00%	-0.01%
9	Dogecoin	DOGE	$26,451,997,839	$0.2013	131,384,576,918 DOGE	$1,585,328,571	-3.55%	-4.83%	-15.58%
10	Polkadot	DOT	$25,880,687,388	$26.21	987,579,315 DOT *	$3,156,414,240	-4.47%	-9.04%	-29.47%
11	Binance USD	BUSD	$12,855,115,835	$1.00	12,852,990,156 BUSD *	$6,654,258,928	-0.01%	-0.02%	-0.02%
12	Avalanche	AVAX	$12,528,967,075	$56.88	220,286,577 AVAX *	$2,335,889,313	-4.51%	-5.07%	11.00%

https://coinmarketcap.com/all/views/all/

Stablecoin



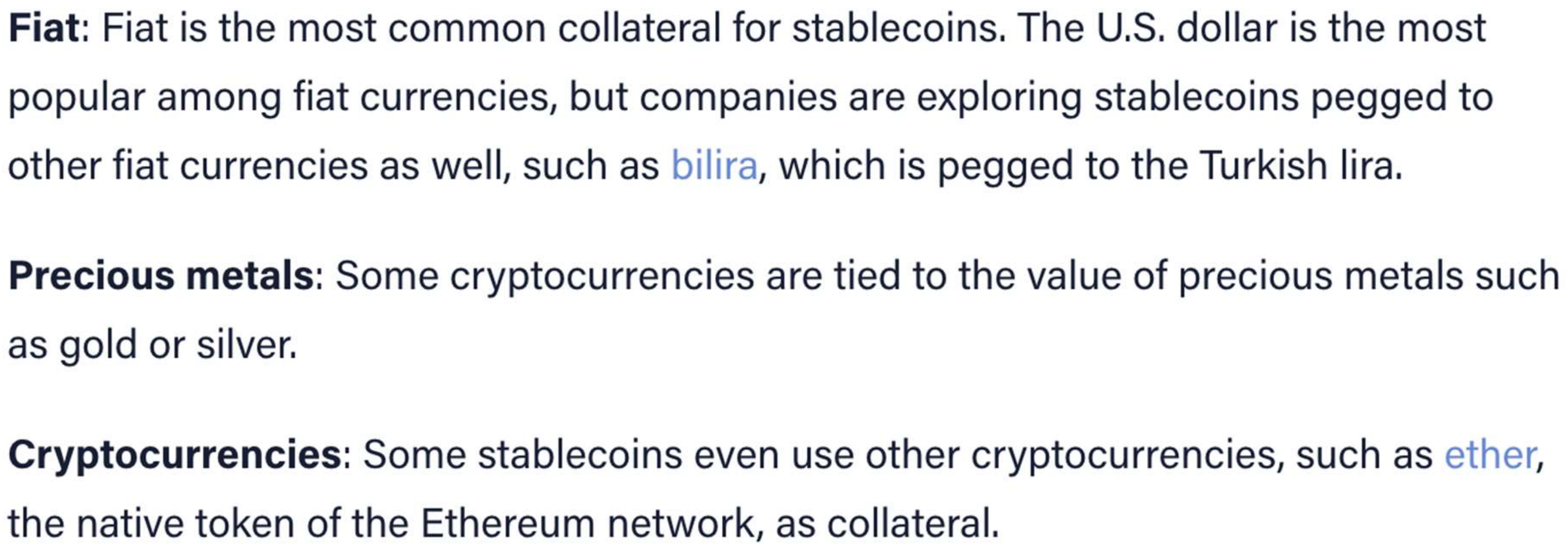
A "stablecoin" is a type of cryptocurrency whose value is tied to an outside asset, such as the U.S. dollar or gold, to stabilize the price.

Cryptocurrencies such as Bitcoin and Ethereum offer a number of benefits, and one of the most fundamental is not requiring trust in an intermediary institution to send payments, which opens up their use to anyone around the globe. But one key drawback is that cryptocurrencies' prices are unpredictable and have a tendency to fluctuate, sometimes wildly.

This makes them hard for everyday people to use. Generally, people expect to be able to know how much their money will be worth a week from now, both for their security and their livelihood.

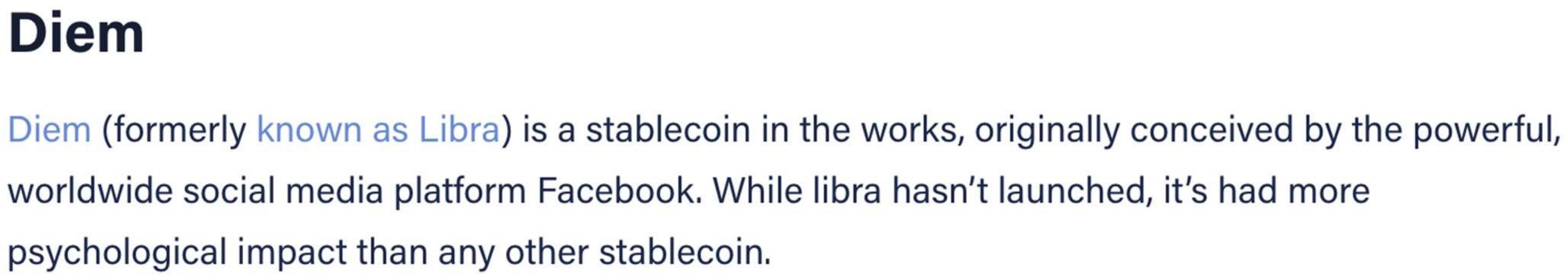
https://www.coindesk.com/what-are-stablecoins

Stablecoin Collateral



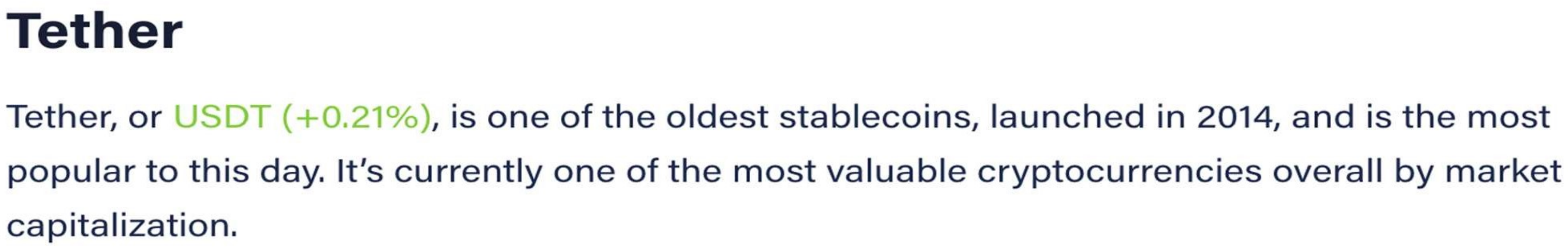
- **Fiat**: Fiat is the most common collateral for stablecoins. The U.S. dollar is the most popular among fiat currencies, but companies are exploring stablecoins pegged to other fiat currencies as well, such as bilira, which is pegged to the Turkish lira.
- **Precious metals**: Some cryptocurrencies are tied to the value of precious metals such as gold or silver.
- **Cryptocurrencies**: Some stablecoins even use other cryptocurrencies, such as ether, the native token of the Ethereum network, as collateral.

Popular Stablecoins



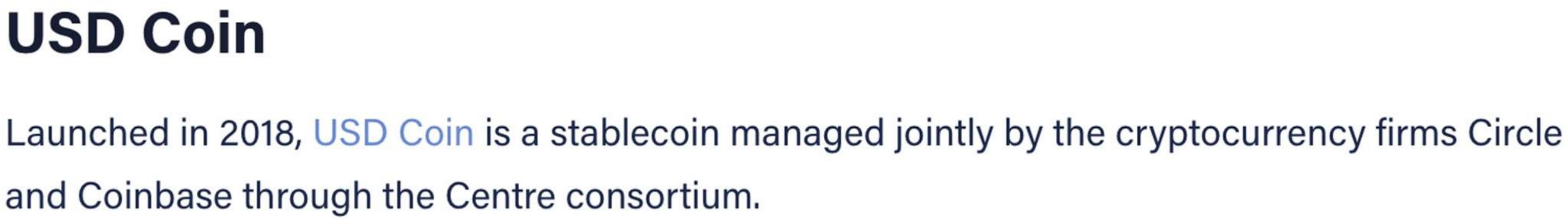
Diem

Diem (formerly known as Libra) is a stablecoin in the works, originally conceived by the powerful, worldwide social media platform Facebook. While libra hasn't launched, it's had more psychological impact than any other stablecoin.



Tether

Tether, or USDT (+0.21%), is one of the oldest stablecoins, launched in 2014, and is the most popular to this day. It's currently one of the most valuable cryptocurrencies overall by market capitalization.



USD Coin

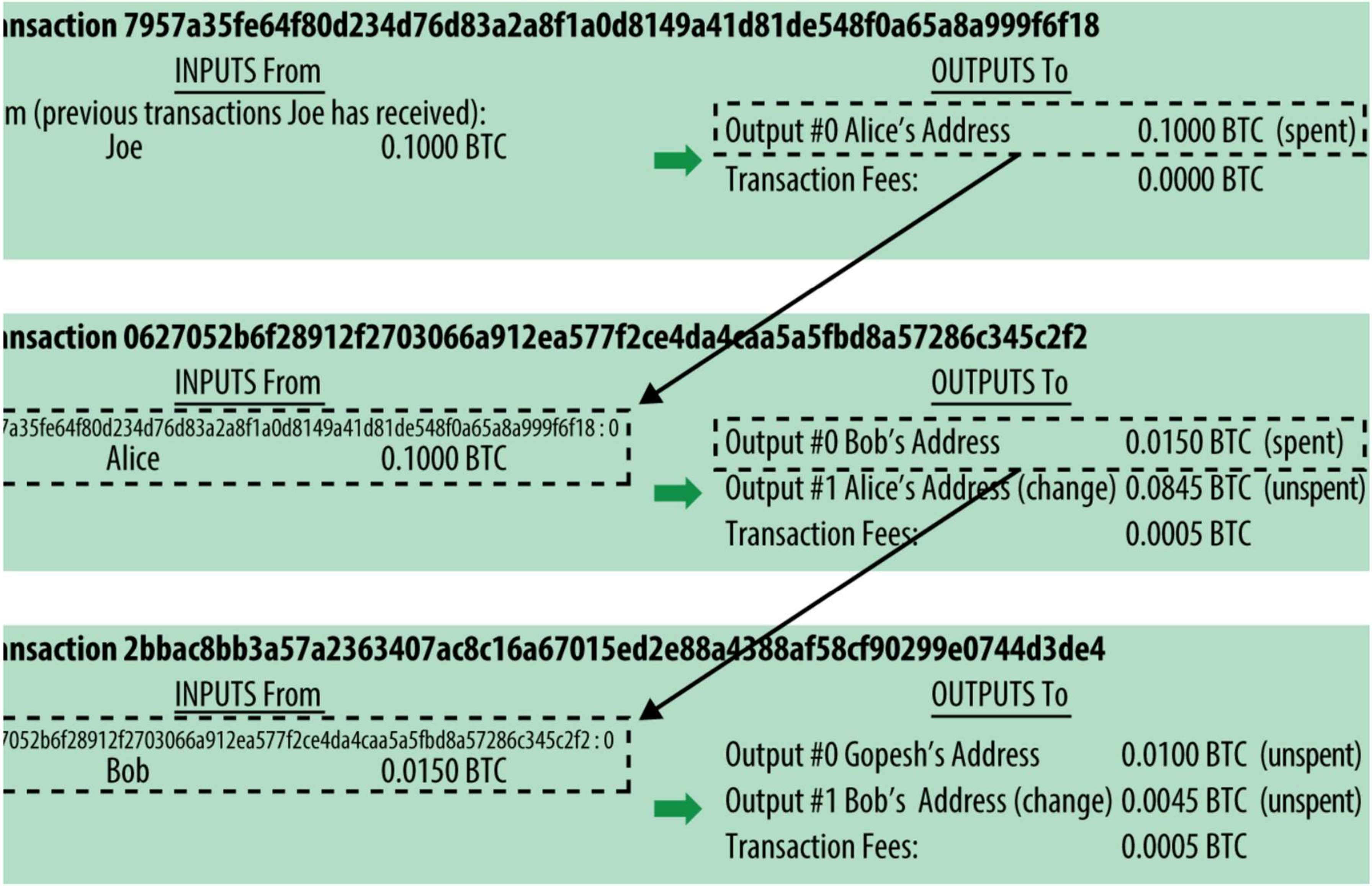
Launched in 2018, USD Coin is a stablecoin managed jointly by the cryptocurrency firms Circle and Coinbase through the Centre consortium.

Case Study –Track Alice Tx to Bob

Buying a Cup of Coffee
Alice, introduced in the previous chapter, is a new user who has just acquired her first bitcoin. In [getting_first_bitcoin], Alice met with her friend Joe to exchange some cash for bitcoin. The transaction created by Joe funded Alice’s wallet with 0.10 BTC. Now Alice will make her first retail transaction, buying a cup of coffee at Bob’s coffee shop in Palo Alto, California.

Bob’s Cafe recently started accepting bitcoin payments by adding a bitcoin option to its point-of-sale system. The prices at Bob’s Cafe are listed in the local currency (US dollars), but at the register, customers have the option of paying in either dollars or bitcoin. Alice places her order for a cup of coffee and Bob enters it into the register, as he does for all transactions. The point-of-sale system automatically converts the total price from US dollars to bitcoin at the prevailing market rate and displays the price in both currencies:
Total: $1.50 USD 0.015 BTC

Bob says, "That’s one-dollar-fifty, or fifteen millibits."



nsaction 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18

INPUTS From

m (previous transactions Joe has received):
Joe 0.1000 BTC

OUTPUTS To

Output #0 Alice's Address 0.1000 BTC (spent)
Transaction Fees: 0.0000 BTC

nsaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

INPUTS From

7a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18 : 0
Alice 0.1000 BTC

OUTPUTS To

Output #0 Bob's Address 0.0150 BTC (spent)
Output #1 Alice's Address (change) 0.0845 BTC (unspent)
Transaction Fees: 0.0005 BTC

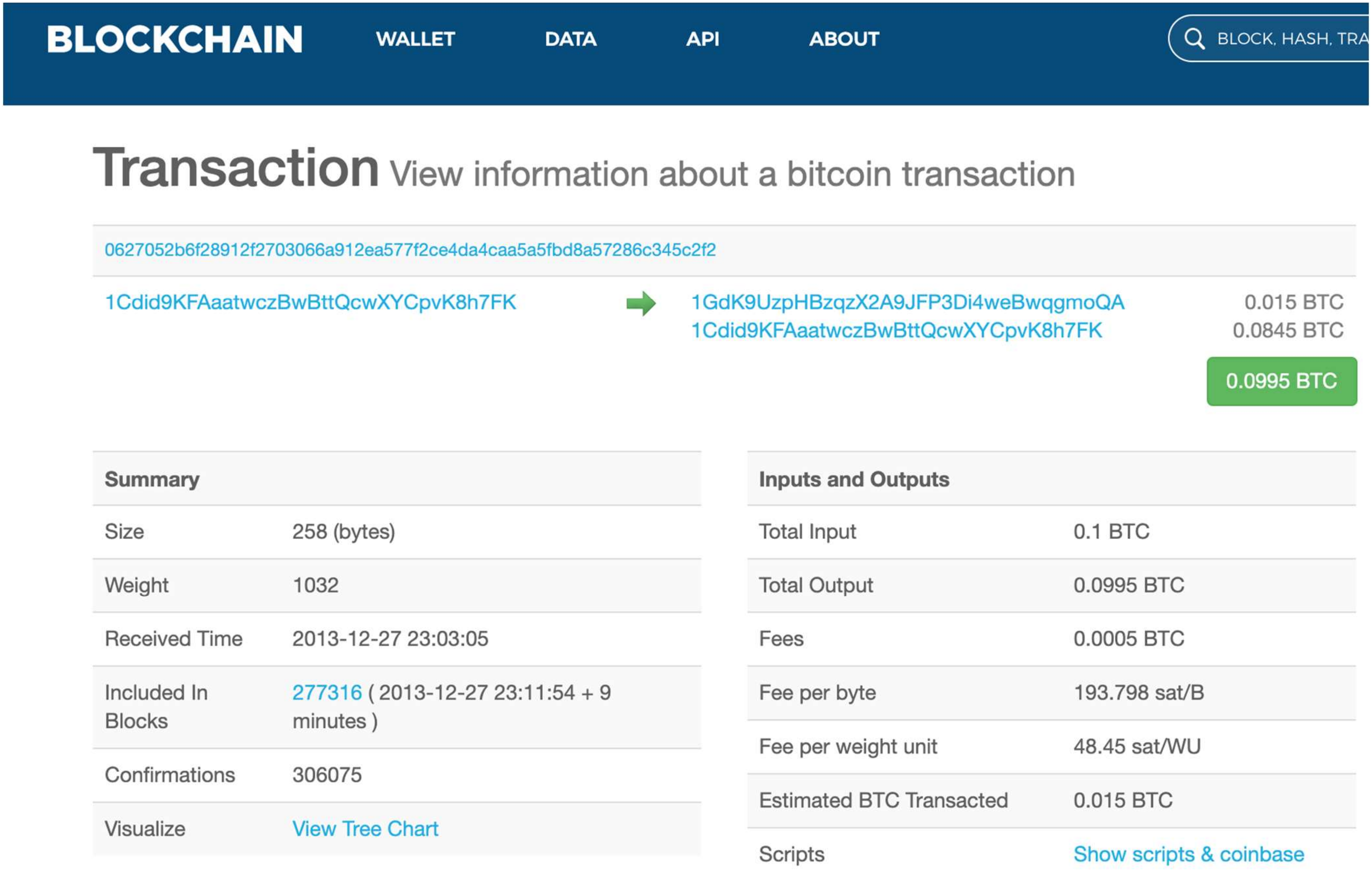
nsaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4

INPUTS From

7052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2 : 0
Bob 0.0150 BTC

OUTPUTS To

Output #0 Gopesh's Address 0.0100 BTC (unspent)
Output #1 Bob's Address (change) 0.0045 BTC (unspent)
Transaction Fees: 0.0005 BTC



Transaction View information about a bitcoin transaction

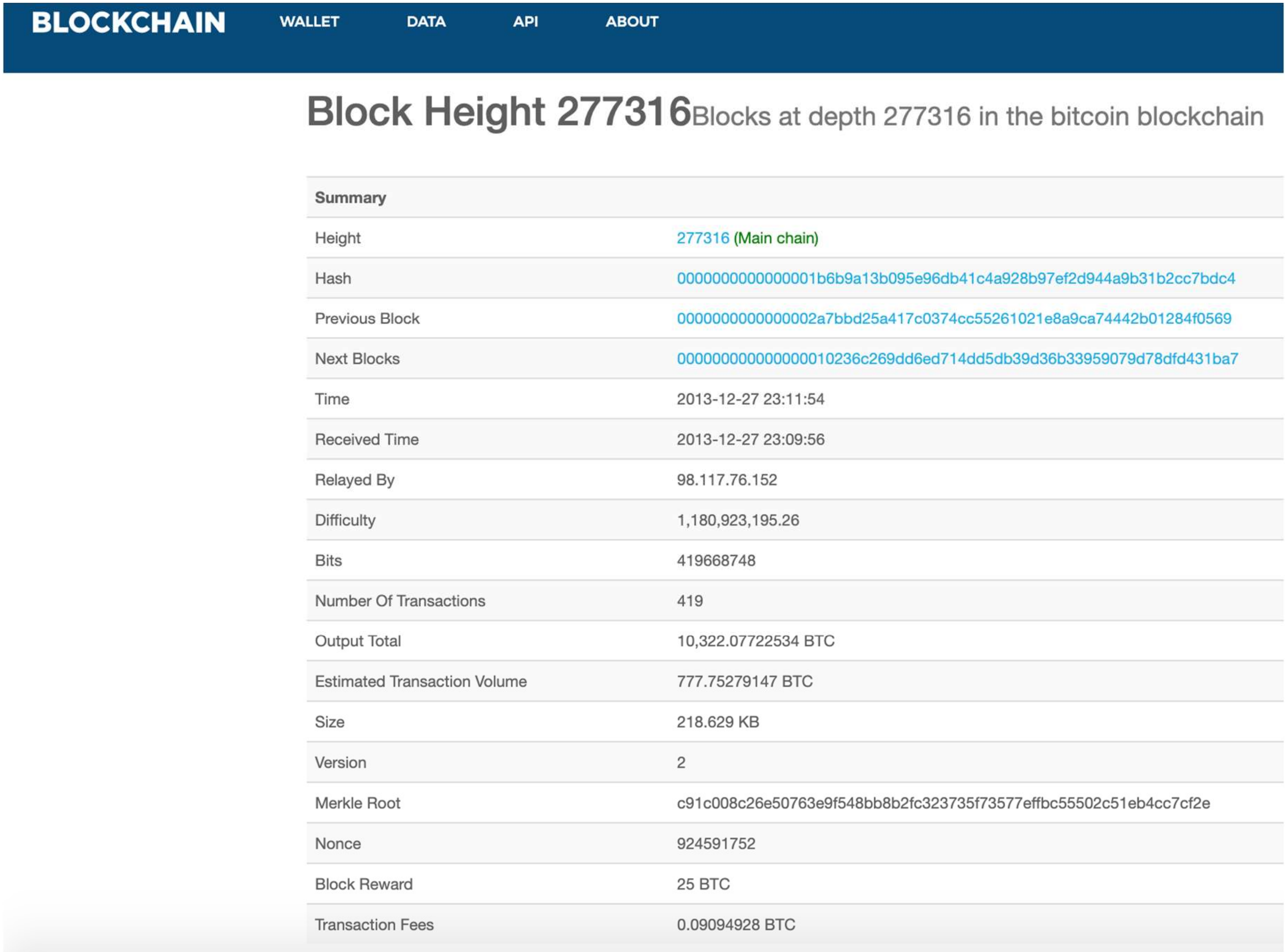
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK	→	1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK	0.015 BTC 0.0845 BTC

0.0995 BTC

Summary	
Size	258 (bytes)
Weight	1032
Received Time	2013-12-27 23:03:05
Included In Blocks	277316 (2013-12-27 23:11:54 + 9 minutes)
Confirmations	306075
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.1 BTC
Total Output	0.0995 BTC
Fees	0.0005 BTC
Fee per byte	193.798 sat/B
Fee per weight unit	48.45 sat/WU
Estimated BTC Transacted	0.015 BTC
Scripts	Show scripts & coinbase



Block Height 277316 Blocks at depth 277316 in the bitcoin blockchain

Summary	
Height	277316 (Main chain)
Hash	0000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2cc7bdc4
Previous Block	0000000000000002a7bbd25a417c0374cc55261021e8a9ca74442b01284f0569
Next Blocks	000000000000000010236c269dd6ed714dd5db39d36b33959079d78dfd431ba7
Time	2013-12-27 23:11:54
Received Time	2013-12-27 23:09:56
Relayed By	98.117.76.152
Difficulty	1,180,923,195.26
Bits	419668748
Number Of Transactions	419
Output Total	10,322.07722534 BTC
Estimated Transaction Volume	777.75279147 BTC
Size	218.629 KB
Version	2
Merkle Root	c91c008c26e50763e9f548bb8b2fc323735f73577effbc55502c51eb4cc7cf2e
Nonce	924591752
Block Reward	25 BTC
Transaction Fees	0.09094928 BTC

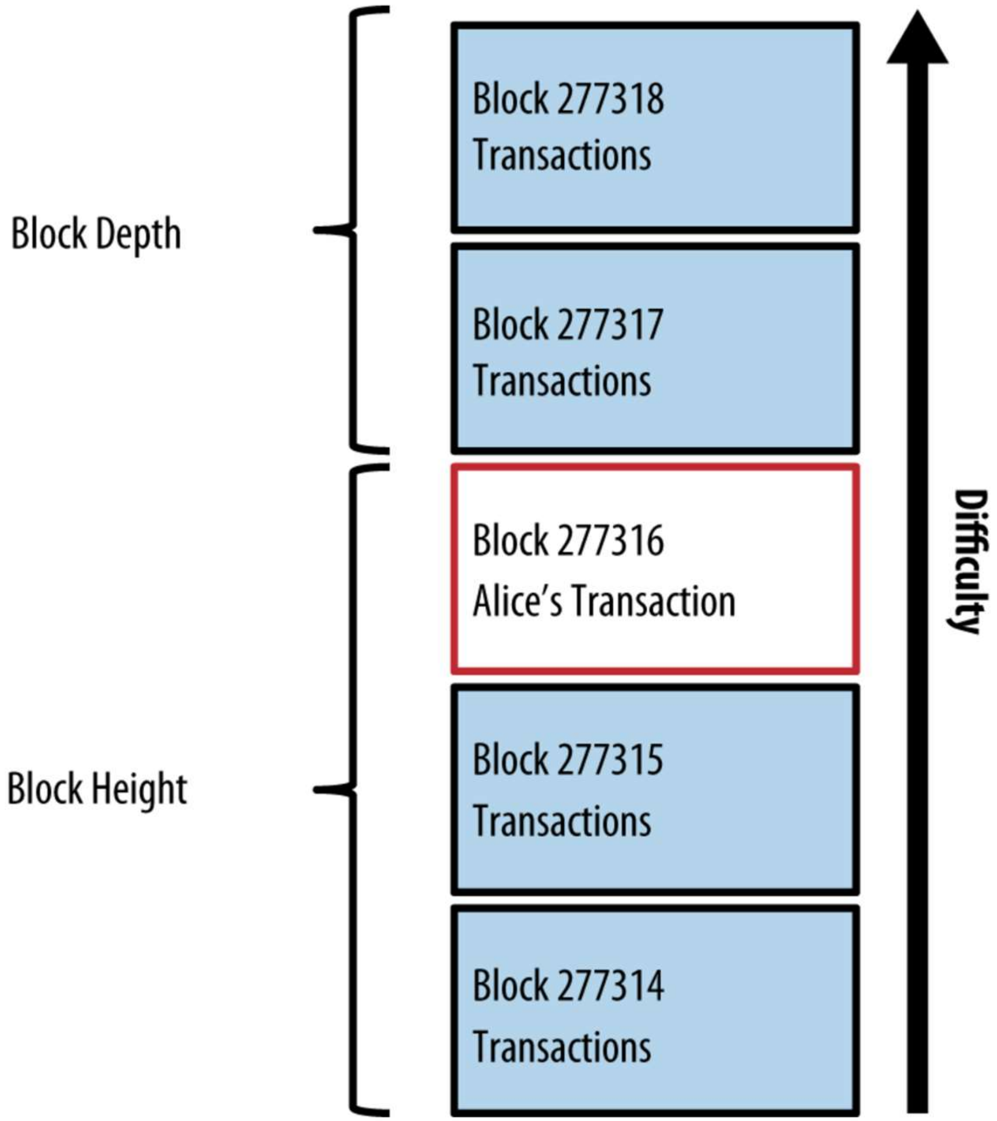
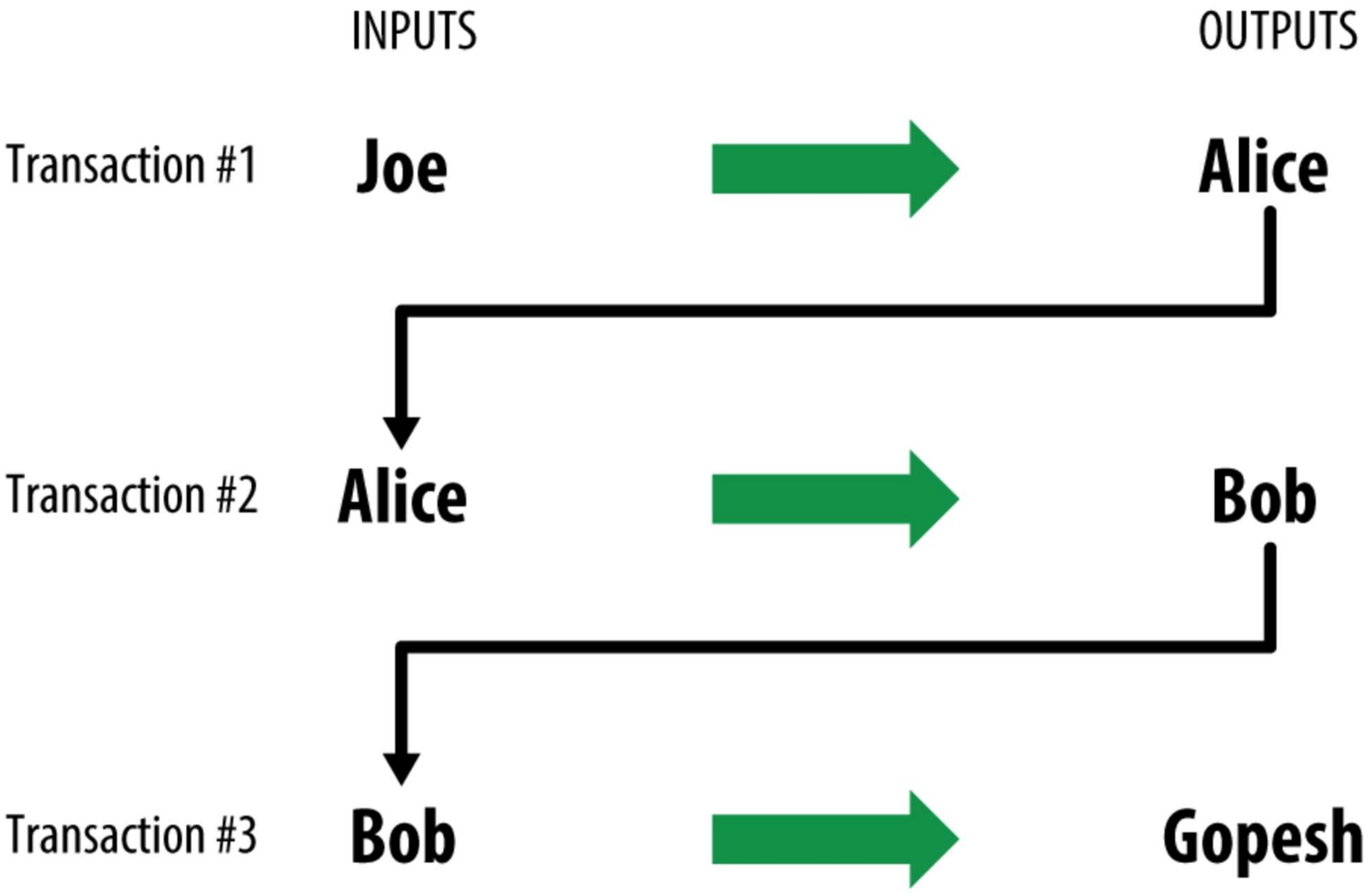


Figure 9. Alice's transaction included in block #277316


INPUTS
OUTPUTS
Transaction #1
Joe
Alice
Transaction #2
Alice
Bob
Transaction #3
Bob
Gopesh

Labs

- Beginner Lab - run helloworld.sol on the Remix IDE
    - Overview - Helloworld.sol is a simple smart contract written in Solidity that contains two functions - printHello and die. While printHello simply prints “Hello World” to the console, the die function terminates the smart contract.
    - Download the Helloworld.sol code to your local hard disk
    - Open the Remix Ethereum IDE - https://remix.ethereum.org/
    - Go to File - **Open File** and open Helloworld.sol
    - Continue using lab instructions
- Intermediate Lab - need to install Metamask Wallet as Chrome Extension

  The lab uses the Kovan Test Network connected via the Metamask Wallet to deploy a smart contract called Faucet. This smart contract is deployed at a specific address in the Kovan Test Network blockchain. Assuming there is test KETH in the wallet, one can send 1 ETH to the Smart Contract, and use the Withdraw function to withdraw 1 wei from the smart contract.

Helloworld.sol

```
pragma solidity >= 0.4.22 <0.6.0;
contract Mortal{
    address owner;
    constructor() public {
        owner = msg.sender;
    }
    function die() public {
        if(msg.sender == owner)
            selfdestruct(msg.sender);
    }
}
contract Helloworld is Mortal{
    string output = "Hello, World!";
    function printHello() public view returns (string memory) {
        return output;
    }
}
```

References

- Cryptocurrencies and underlying blockchain technology
  - https://bitcoin.org/bitcoin.pdf – Original Paper by Satoshi Nakamoto, 10/28
  - www.bitcoin.org – Original cryptocurrency, over 10 years old!
  - www.ZeroCoin.org - Extend Bitcoin to make it private
  - www.Litecoin.org - Open Source P2P Internet Currency
  - www.Ethereum.org – Created a Virtual Machine for any Token
  - www.Hyperledger.org - Blockchains for Business
  - www.ripple.com - Ripple Crytpcurrency (XRP) – Rising star for global tx
  - www.getmonero.org – Monero Cryptocurrency (XMR) – Popular for security
  - www.coinbase.com – Popular Exchange to buy cryptocurrency
  - www.blockexplorer.com – Bitcoin Block Explorer
  - www.blockchain.info – Great source for all sorts of crypto info
  - www.dogecoin.com - Started off as a joke but now favored by Shiba Inus WW