HI-TEC 2020 TRANSFORMED

High Impact Technology Exchange Conference

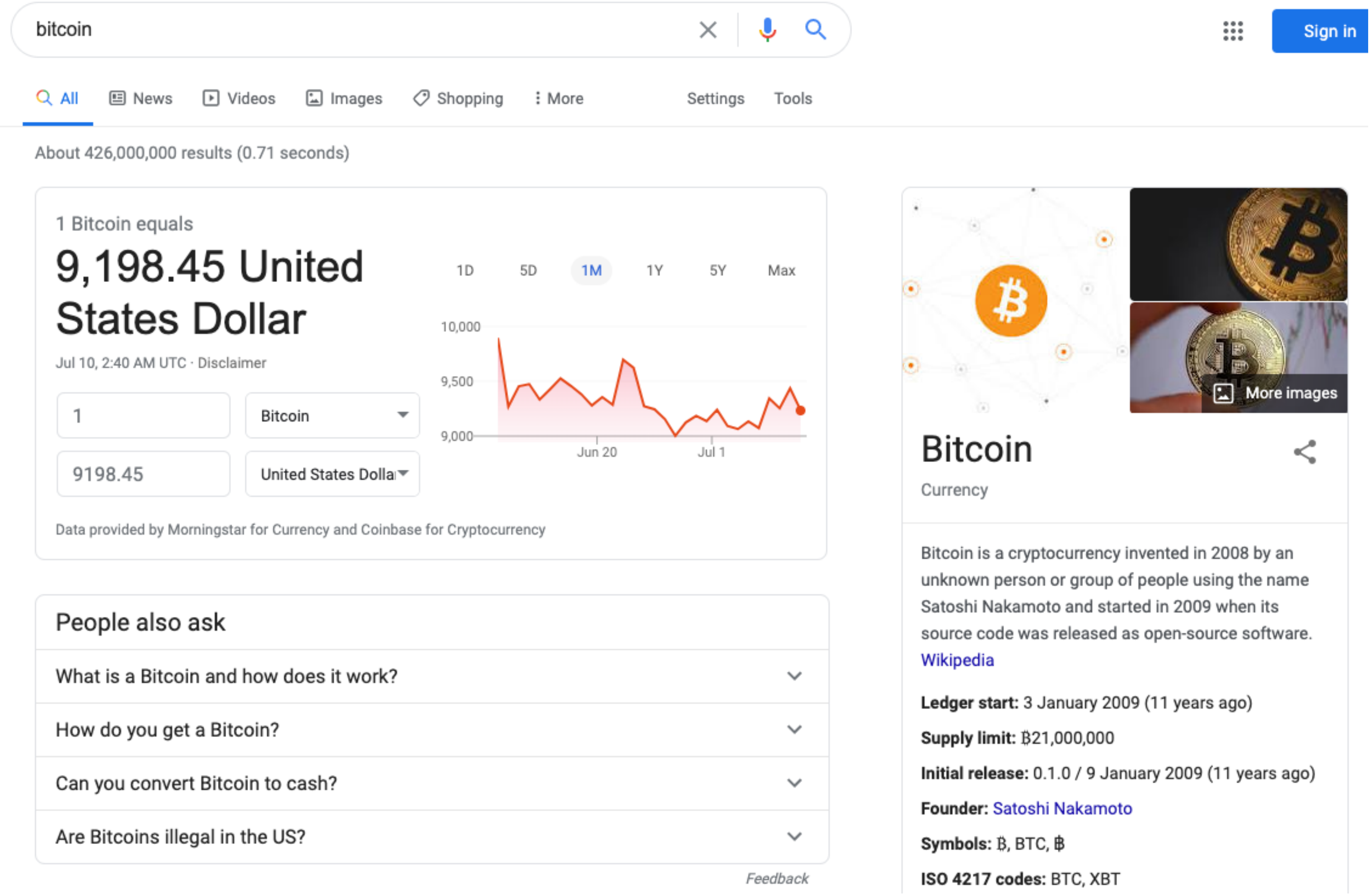
JULY 29–30

Introduction to Bitcoins, Blockchains, and Smart Contracts

Debasis Bhattacharya (debasisb@hawaii.edu, www.maui.hawaii.edu/cybersecurity)
University of Hawaii Maui College, July 2020

Presentation Overview

This presentation introduces bitcoins, blockchains, and smart contracts programmed with Ethereum Blockchains and the Solidity programming language. Cryptocurrencies such as bitcoins use blockchains and smart contracts to enforce transactions. Solidity is the programming language that is used to create smart contracts that are stored on the blockchain.



About 426,000,000 results (0.71 seconds)

1 Bitcoin equals

9,198.45 United States Dollar

Jul 10, 2:40 AM UTC · Disclaimer

1 Bitcoin

9198.45 United States Dolla

Data provided by Morningstar for Currency and Coinbase for Cryptocurrency

People also ask

What is a Bitcoin and how does it work?

How do you get a Bitcoin?

Can you convert Bitcoin to cash?

Are Bitcoins illegal in the US?

Bitcoin

Currency

Bitcoin is a cryptocurrency invented in 2008 by an unknown person or group of people using the name Satoshi Nakamoto and started in 2009 when its source code was released as open-source software. Wikipedia

Ledger start: 3 January 2009 (11 years ago)

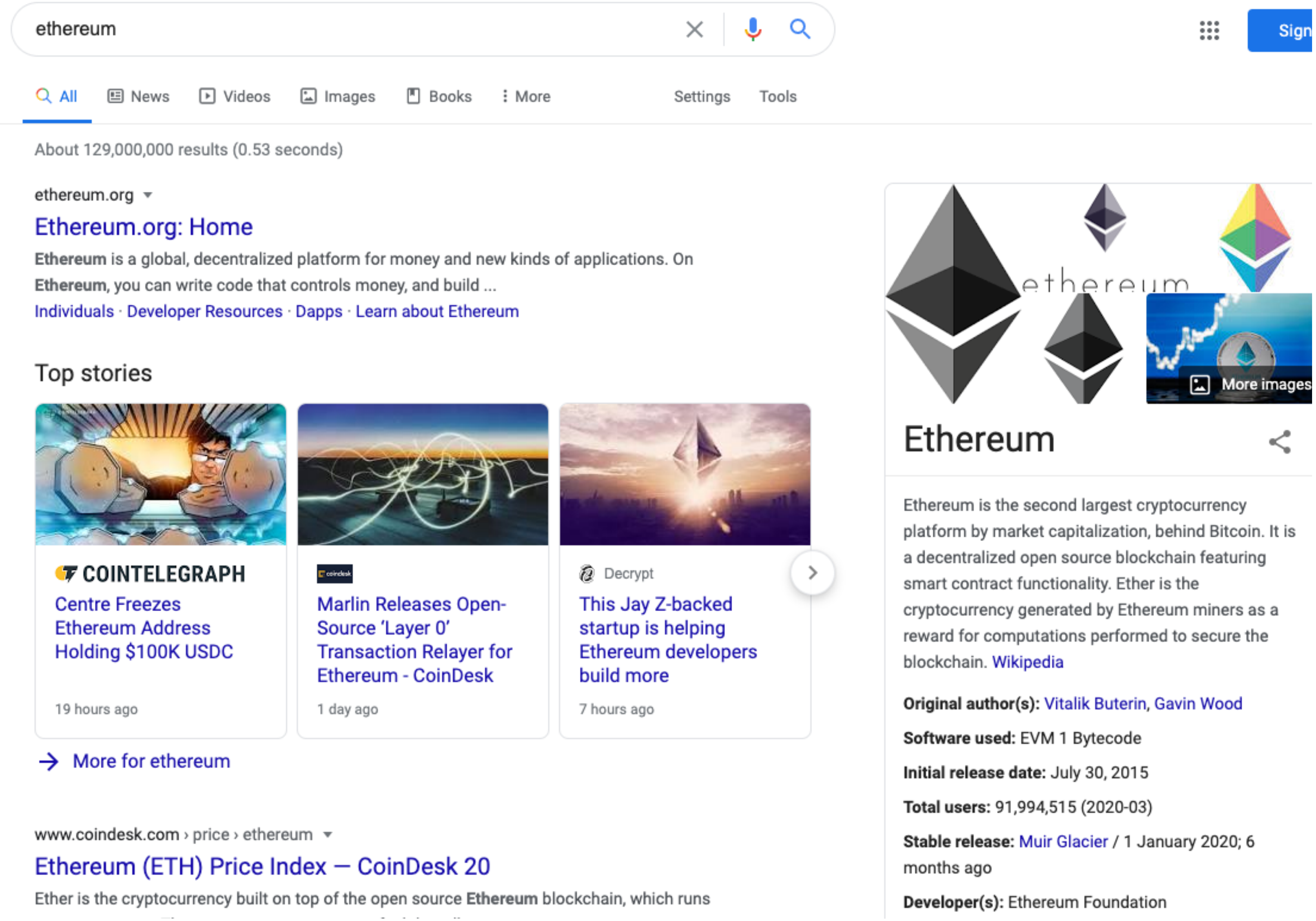
Supply limit: ₿21,000,000

Initial release: 0.1.0 / 9 January 2009 (11 years ago)

Founder: Satoshi Nakamoto

Symbols: ₿, BTC, ฿

ISO 4217 codes: BTC, XBT



About 129,000,000 results (0.53 seconds)

ethereum.org

Ethereum.org: Home

Ethereum is a global, decentralized platform for money and new kinds of applications. On **Ethereum**, you can write code that controls money, and build ...

Individuals · Developer Resources · Dapps · Learn about Ethereum

Top stories

COINTELEGRAPH
Centre Freezes Ethereum Address Holding $100K USDC
19 hours ago

Marlin Releases Open-Source 'Layer 0' Transaction Relayer for Ethereum - CoinDesk
1 day ago

Decrypt
This Jay Z-backed startup is helping Ethereum developers build more
7 hours ago

More for ethereum

www.coindesk.com › price › ethereum

Ethereum (ETH) Price Index — CoinDesk 20

Ether is the cryptocurrency built on top of the open source **Ethereum** blockchain, which runs

Ethereum

Ethereum is the second largest cryptocurrency platform by market capitalization, behind Bitcoin. It is a decentralized open source blockchain featuring smart contract functionality. Ether is the cryptocurrency generated by Ethereum miners as a reward for computations performed to secure the blockchain. Wikipedia

Original author(s): Vitalik Buterin, Gavin Wood

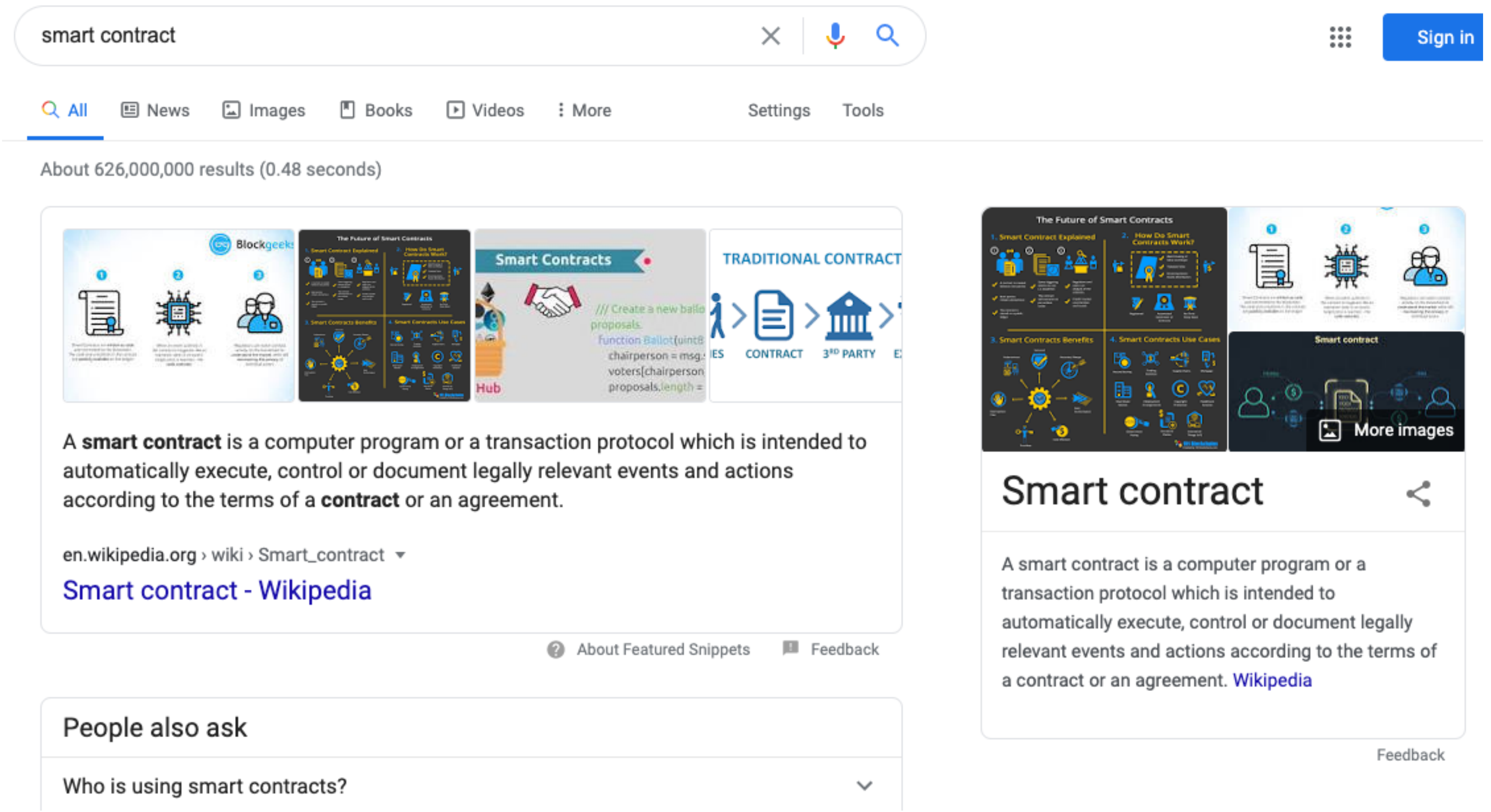
Software used: EVM 1 Bytecode

Initial release date: July 30, 2015

Total users: 91,994,515 (2020-03)

Stable release: Muir Glacier / 1 January 2020; 6 months ago

Developer(s): Ethereum Foundation



About 626,000,000 results (0.48 seconds)

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.

en.wikipedia.org › wiki › Smart_contract

Smart contract - Wikipedia

People also ask

Who is using smart contracts?

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

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!

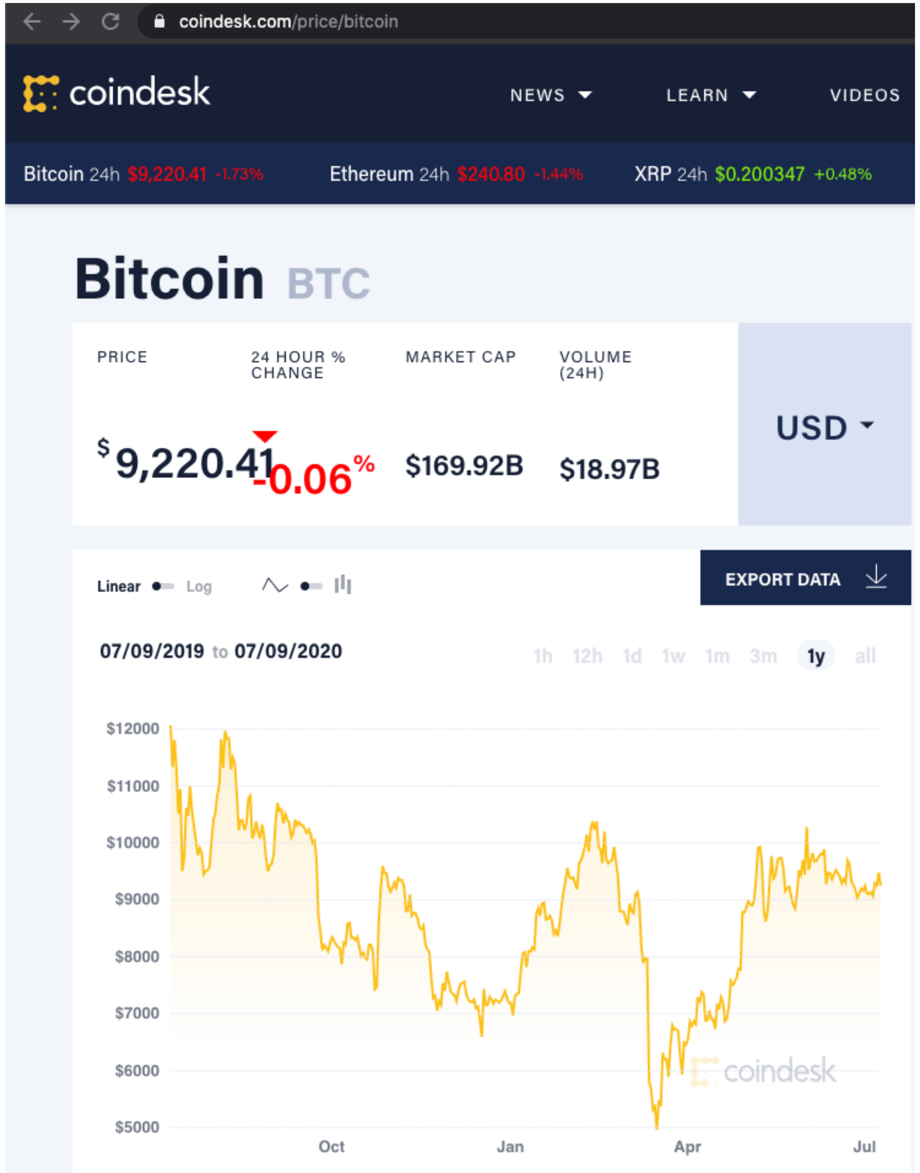
Bitcoin

- 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 ~18.43 million (July 9, 2020)
- Total number of BitCoins generated cannot exceed 21 million.
  - Around 2.6 million left to be mined! Mining will end in the year 2140…
- Average price of a Bitcoin:
  - $9,220.41 on July 9, 2020
  - $10,635.28 on July 18, 2019
  - $10,360.45 on July 1, 2019
  - $4,110 on February 23, 2019
  - $3729 on Dec 29, 2018
  - $8,522 on May 15, 2018
  - $7,149 on April 8, 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!)



coindesk.com/price/bitcoin

coindesk NEWS LEARN VIDEOS

Bitcoin 24h $9,220.41 -1.73% Ethereum 24h $240.80 -1.44% XRP 24h $0.200347 +0.48%

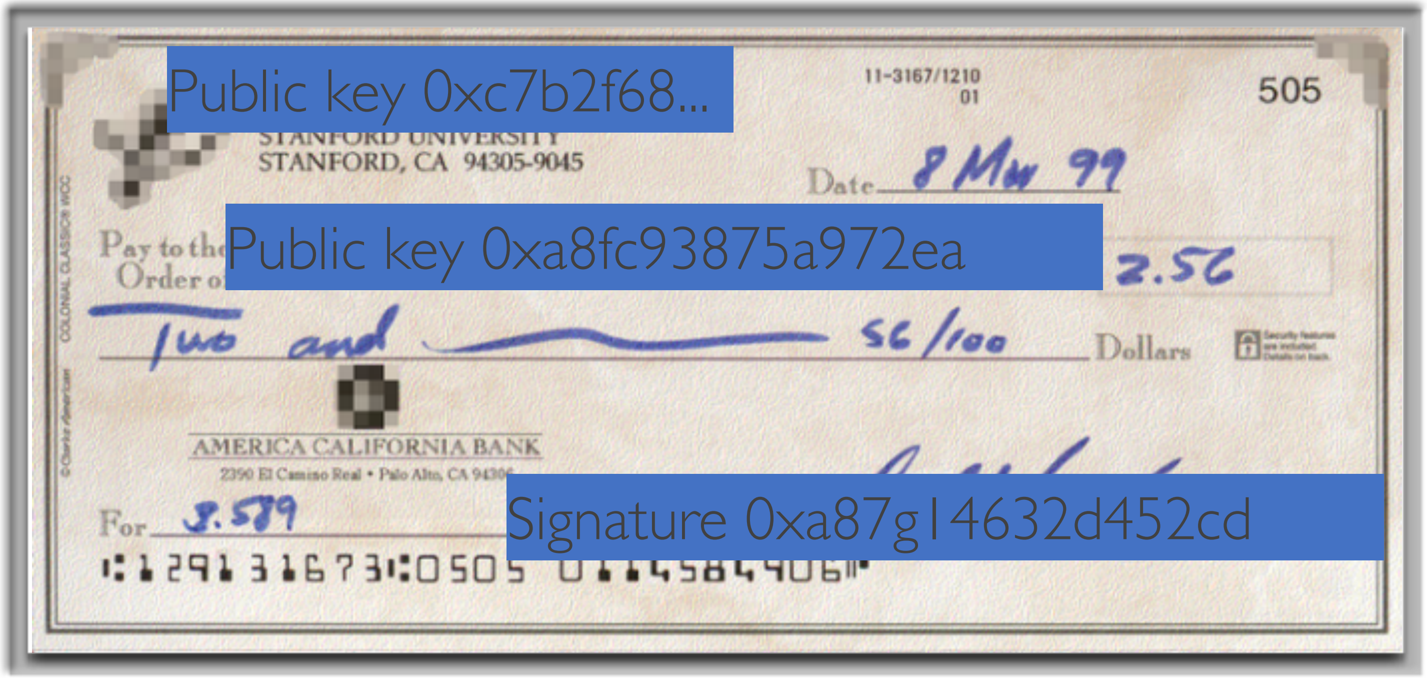
Bitcoin BTC

PRICE	24 HOUR % CHANGE	MARKET CAP	VOLUME (24H)
$9,220.41	-0.06%	$169.92B	$18.97B

USD

07/09/2019 to 07/09/2020

Bitcoin Transactions



Public key 0xc7b2f68...

11-3167/1210
01

505

STANFORD UNIVERSITY
STANFORD, CA 94305-9045

Date 8 May 99

Pay to the
Order of Public key 0xa8fc93875a972ea

2.56

Two and 56/100 Dollars

AMERICA CALIFORNIA BANK
2390 El Camino Real • Palo Alto, CA 94306

For 3.589

Signature 0xa87g14632d452cd

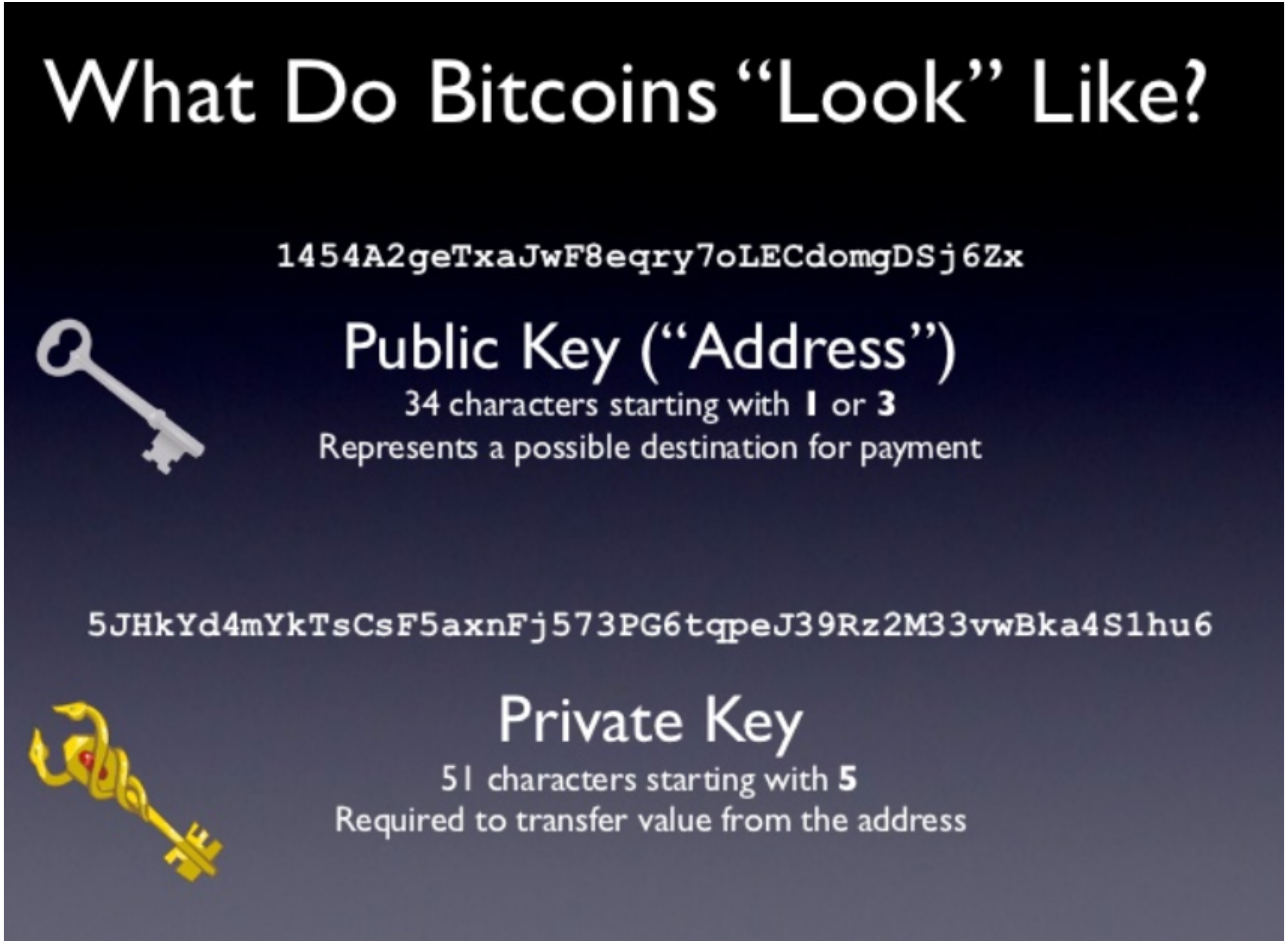
⑆121291316731⑆0505 0114584406⑈

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."



What Do Bitcoins "Look" Like?

`1454A2geTxaJwF8eqry7oLECdomgDSj6Zx`

Public Key ("Address")

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

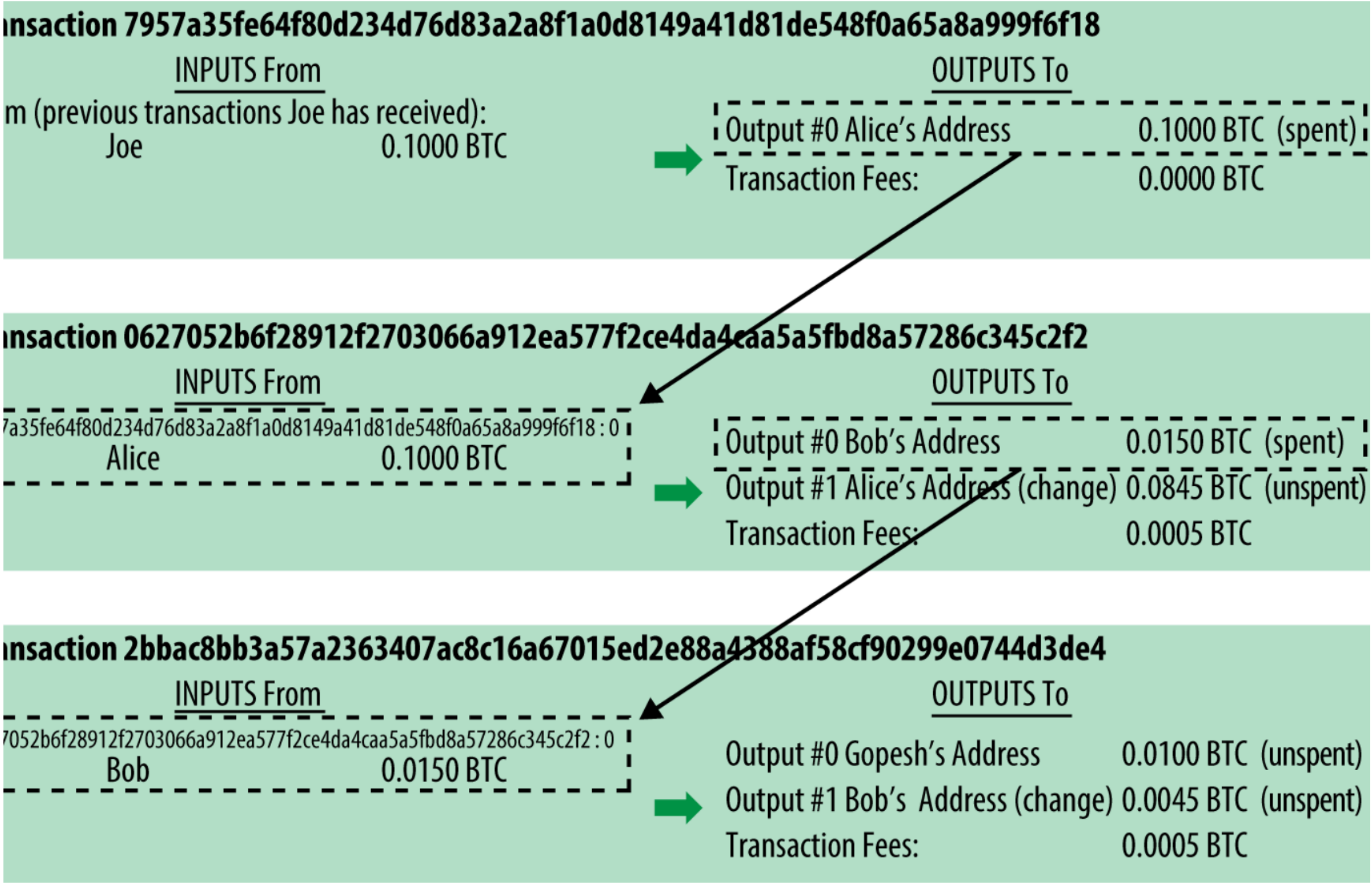
Represents a possible destination for payment

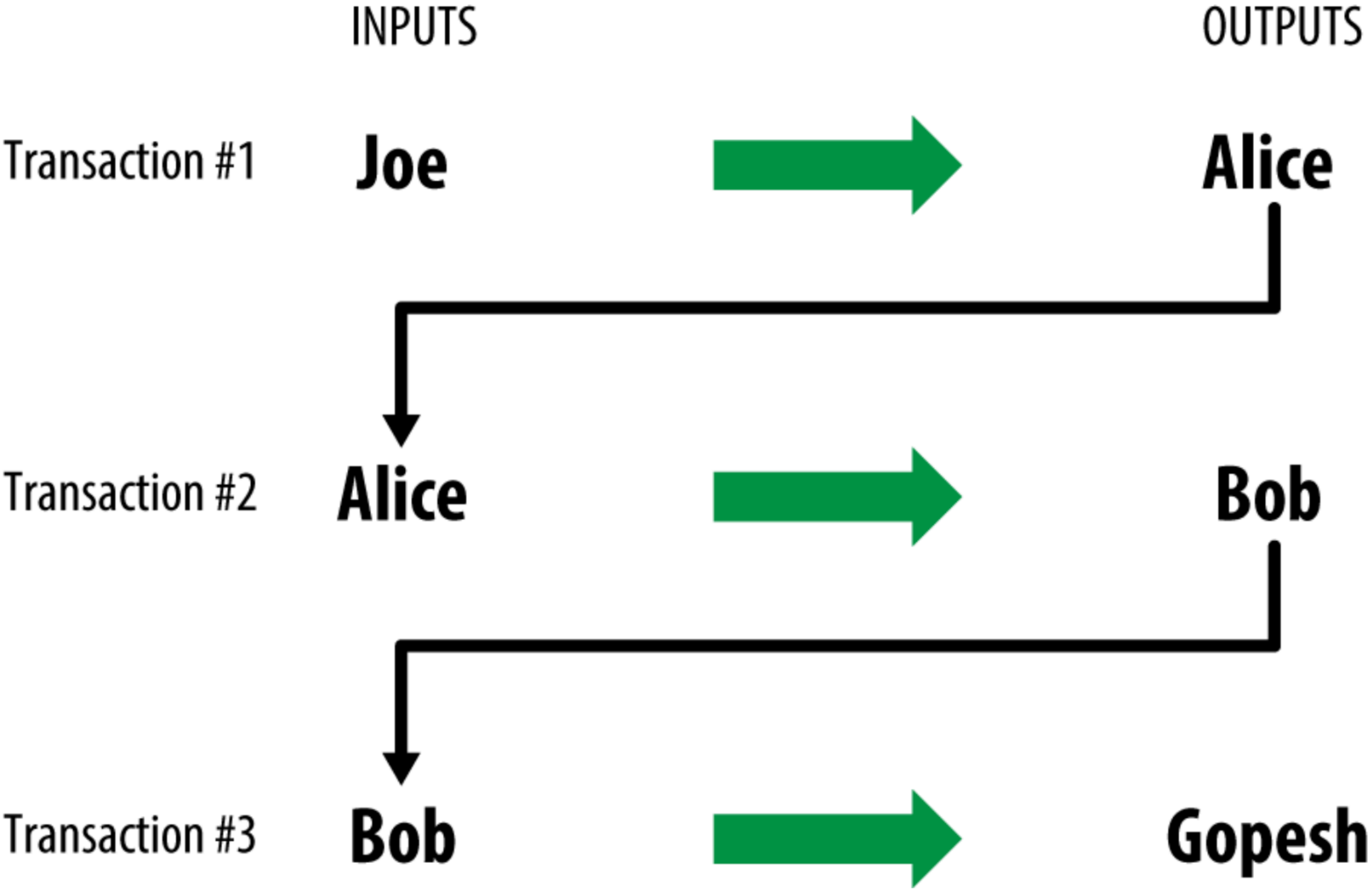
`5JHkYd4mYkTsCsF5axnFj573PG6tqpeJ39Rz2M33vwBka4S1hu6`

Private Key

51 characters starting with **5**

Required to transfer value from the address


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


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

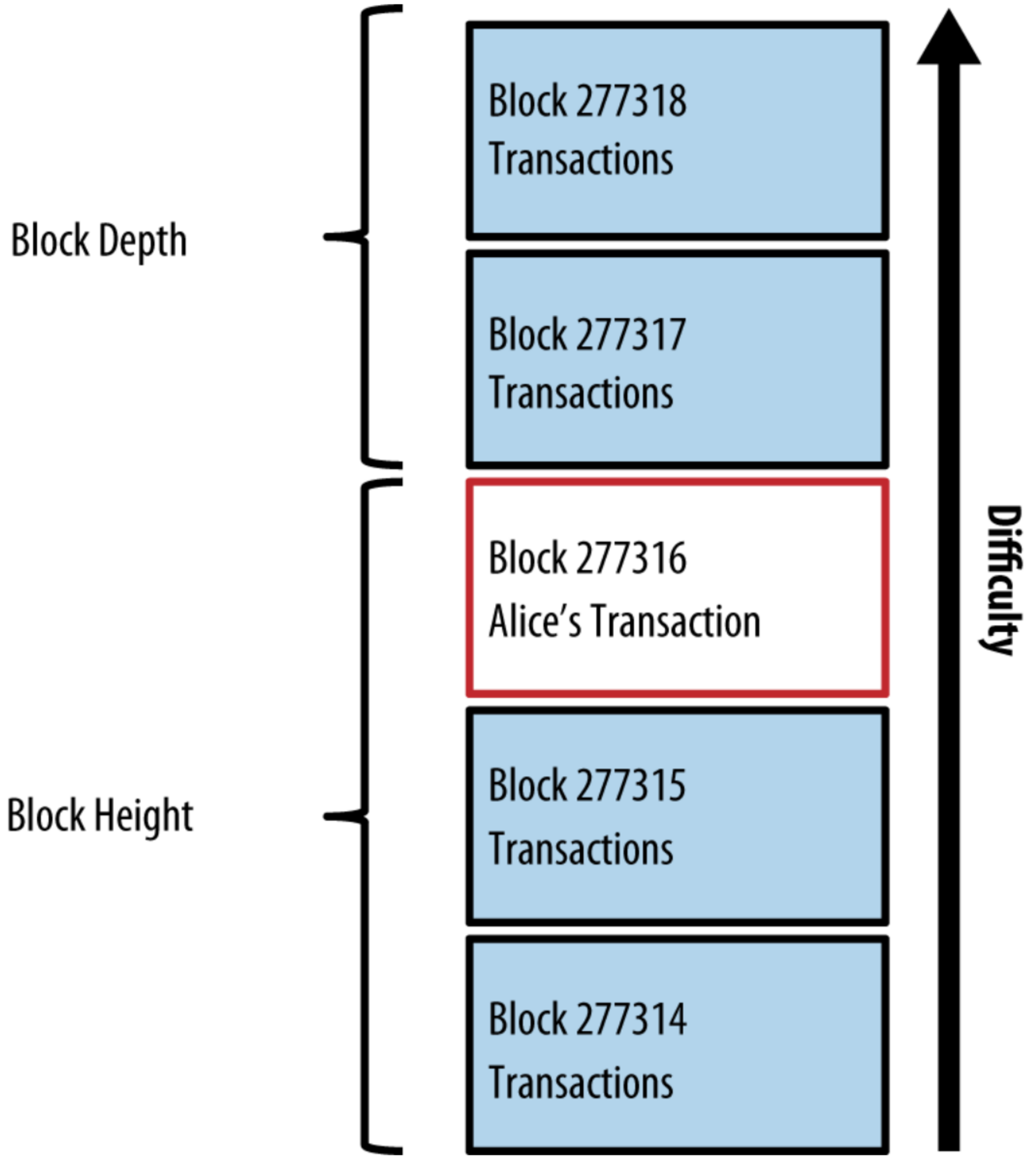
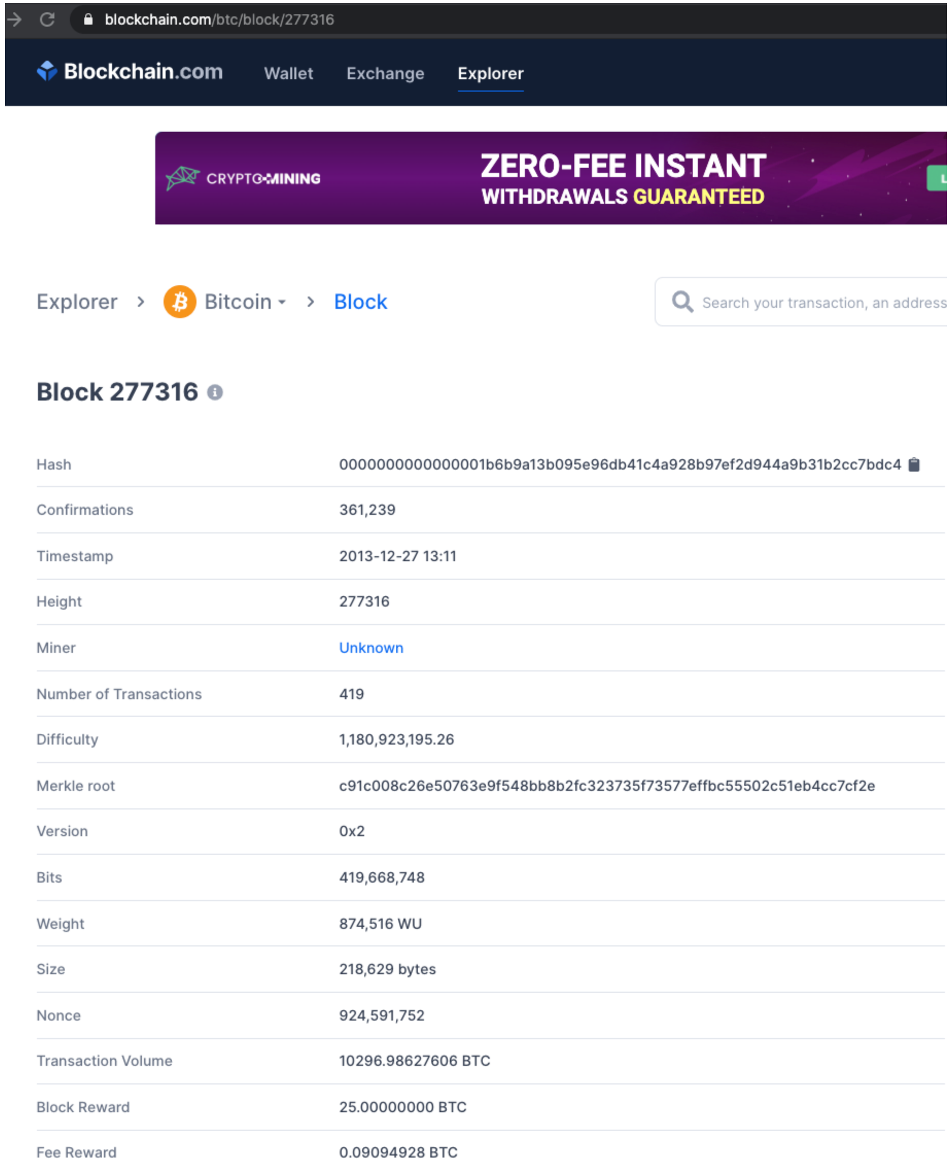


Figure 9. Alice's transaction included in block #277316


blockchain.com/btc/block/277316
Blockchain.com
Wallet
Exchange
Explorer
CRYPTO MINING
ZERO-FEE INSTANT
WITHDRAWALS GUARANTEED
Explorer › Bitcoin › Block
Search your transaction, an address

Block 277316

Hash	0000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2cc7bdc4
Confirmations	361,239
Timestamp	2013-12-27 13:11
Height	277316
Miner	Unknown
Number of Transactions	419
Difficulty	1,180,923,195.26
Merkle root	c91c008c26e50763e9f548bb8b2fc323735f73577effbc55502c51eb4cc7cf2e
Version	0x2
Bits	419,668,748
Weight	874,516 WU
Size	218,629 bytes
Nonce	924,591,752
Transaction Volume	10296.98627606 BTC
Block Reward	25.00000000 BTC
Fee Reward	0.09094928 BTC

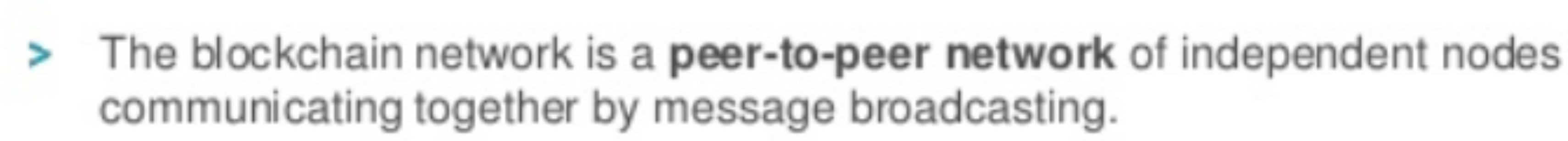
Bitcoin - Activities

- Bitcoin Paper - Satoshi Nakamoto - https://bitcoin.org/bitcoin.pdf
- Blockchain Explorer of Bitcoins etc. - https://www.blockchain.com/explorer
- Coin Market of Various Cryptos- https://coinmarketcap.com/all/views/all/
- Coinbase Web Site Demo - https://www.coinbase.com/
- Stable Coin - USD Coin from Coinbase - https://www.coinbase.com/usdc

Bitcoin - Labs

- Beginner Lab – Where is Bitcoin?
  - https://github.com/UHMC/module-1-lab-beginner
- Intermediate Lab – Visualizing Bitcoin
  - https://github.com/UHMC/module-1-lab-intermediate

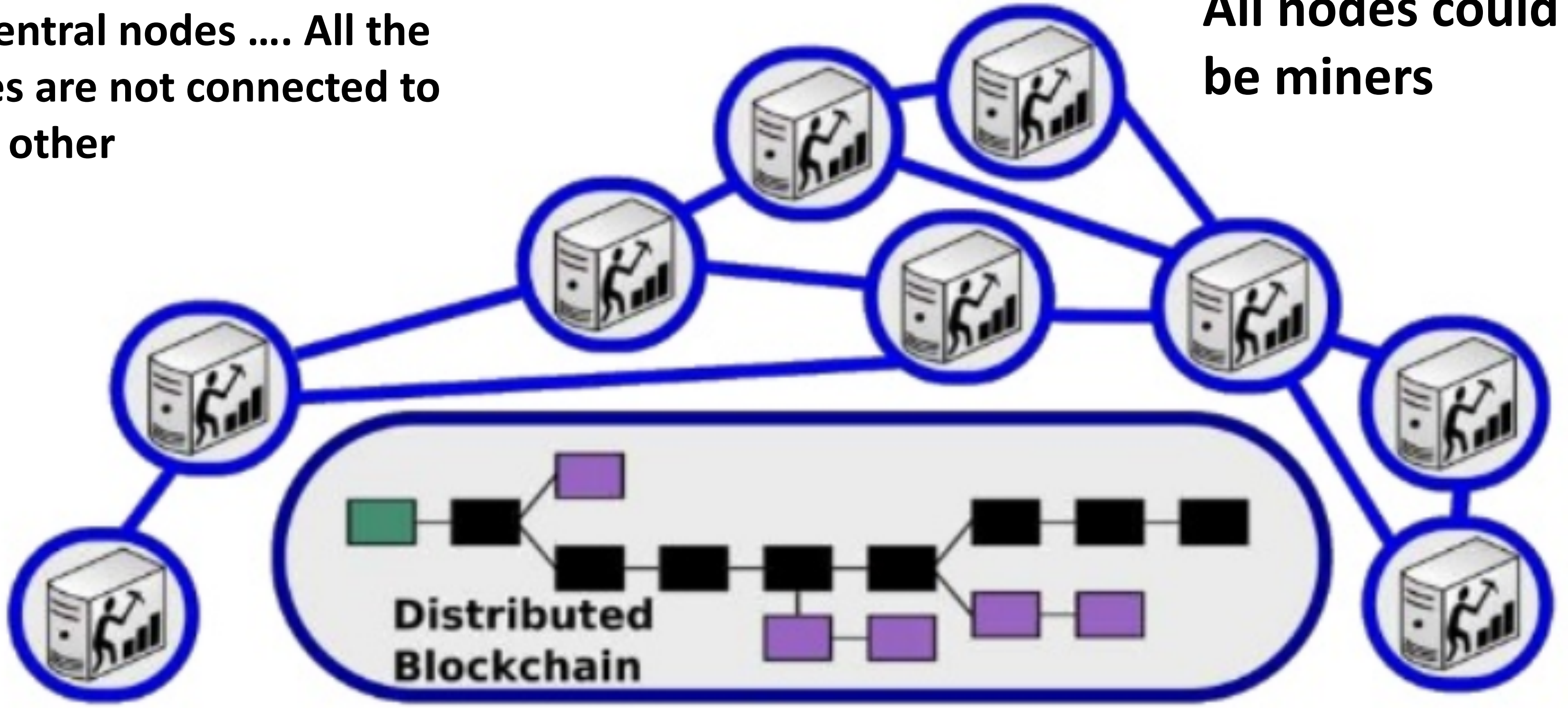
Blockchain Process… Decentralization



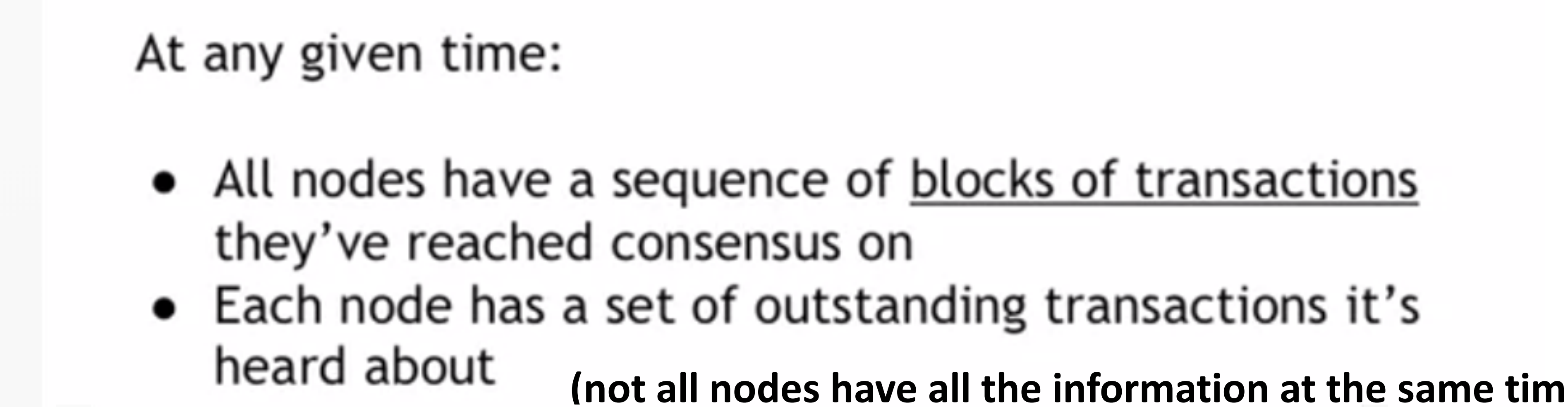
> The blockchain network is a **peer-to-peer network** of independent nodes communicating together by message broadcasting.

No central nodes …. All the nodes are not connected to each other

All nodes could be miners



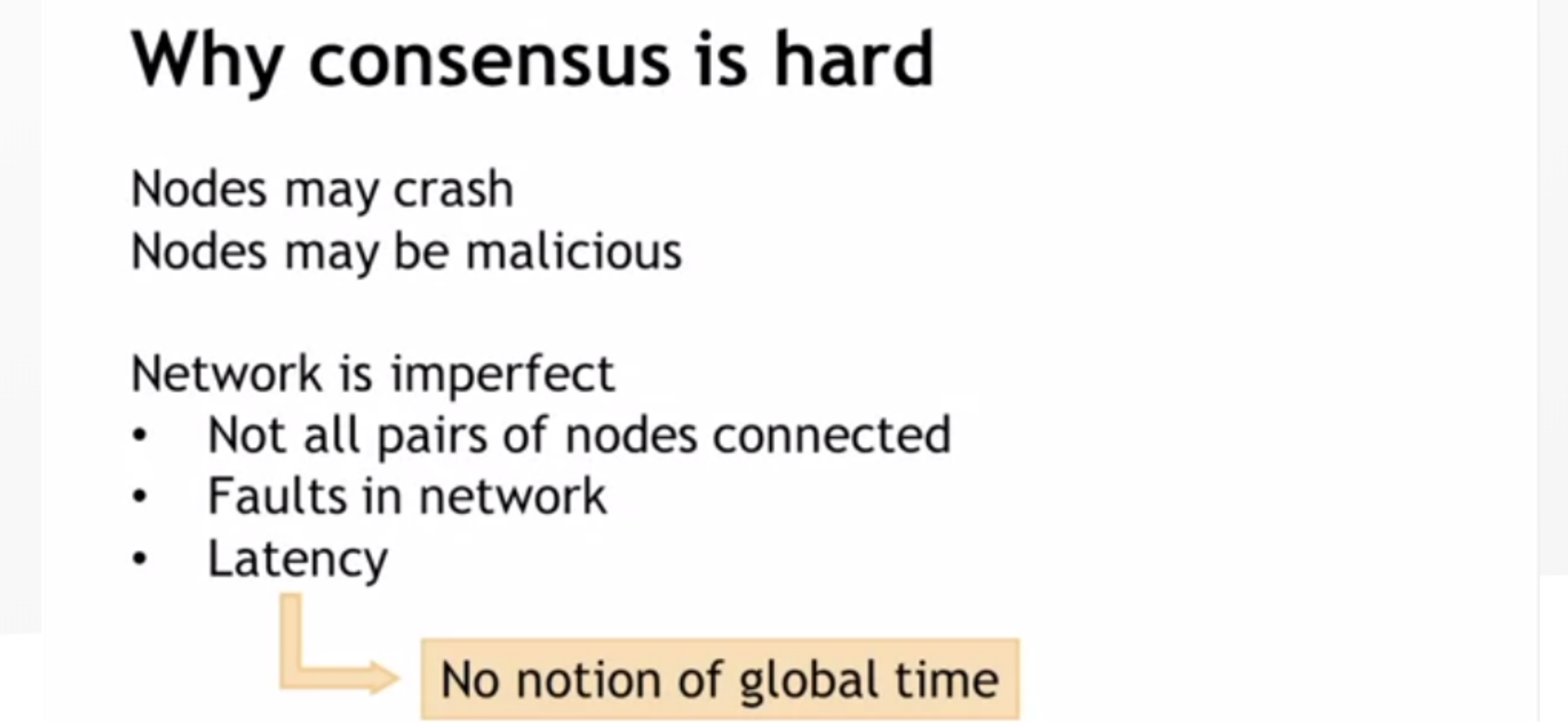
Distributed Consensus



At any given time:

- All nodes have a sequence of <u>blocks of transactions</u> they've reached consensus on
- Each node has a set of outstanding transactions it's heard about

(not all nodes have all the information at the same time(Latency)



Why consensus is hard

Nodes may crash
Nodes may be malicious

Network is imperfect

- Not all pairs of nodes connected
- Faults in network
- Latency

→ No notion of global time

How Blockchain Works

Here are five basic principles underlying the technology.

1. Distributed Database

- Each party on a blockchain has access to the entire database and its complete history.
- No single party controls the data or the information. Every party can verify the records of its transaction partners directly, without an intermediary.

2. Peer-to-Peer Transmission

- Communication occurs directly between peers instead of through a central node.
- Each node stores and forwards information to all other nodes.

3. Transparency with Pseudonymity

- Every transaction and its associated value are visible to anyone with access to the system. **(public key)**
- Each node, or user, on a blockchain has a unique 30-plus-character alphanumeric address that identifies it. **(private key)**
- Users can choose to remain anonymous or provide proof of their identity to others. **(signatures)** Transactions occur between blockchain addresses.

4. Irreversibility of Records

- Once a transaction is entered in the database and the accounts are updated, the records cannot be altered, **because they're linked to every transaction record that came before them (hence the term "chain").**
- **Various computational algorithms and approaches are deployed to ensure that the recording on the database is permanent, chronologically ordered, and available to all others on the network.**

5. Computational Logic

- The digital nature of the ledger means that blockchain transactions can be tied to computational logic and in essence programmed.
- **users can set up algorithms and rules that automatically trigger transactions between nodes.**

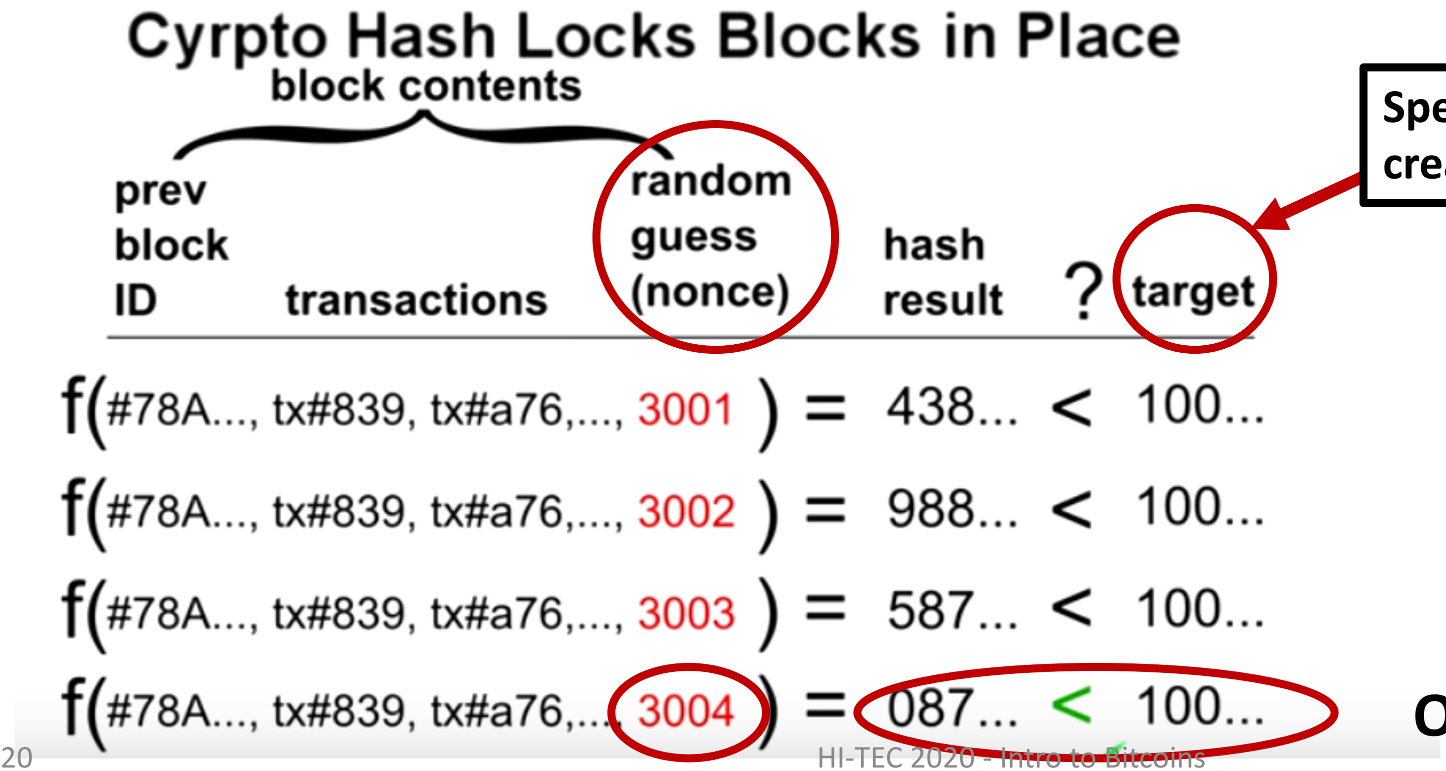
- **Data Security**
  - **Keys**
  - **Signatures**
  - **Hashing**
- **Redundancy**
- **Improved workflow**

The hash output, or fingerprint, is actually what's used as the **"previous block"** reference.

- One result of this is that **there's no way to switch out a block in the middle** of the chain, because the hash value for the new block would be different, and the next's block reference would no longer point to it.

- Even more importantly, **a block cannot be solved before the previous block is solved.** The previous block reference is part of the text that goes through the hash function, so any changes to it would require resolving.

solving a block involves trying to get the cryptographic hash of the block to be below a certain value, and you do that by trying different random numbers . Once solved, the hash output is like a fingerprint that uniquely identifies that block. If even a single character in the block is changed, the block's hash would be completely different



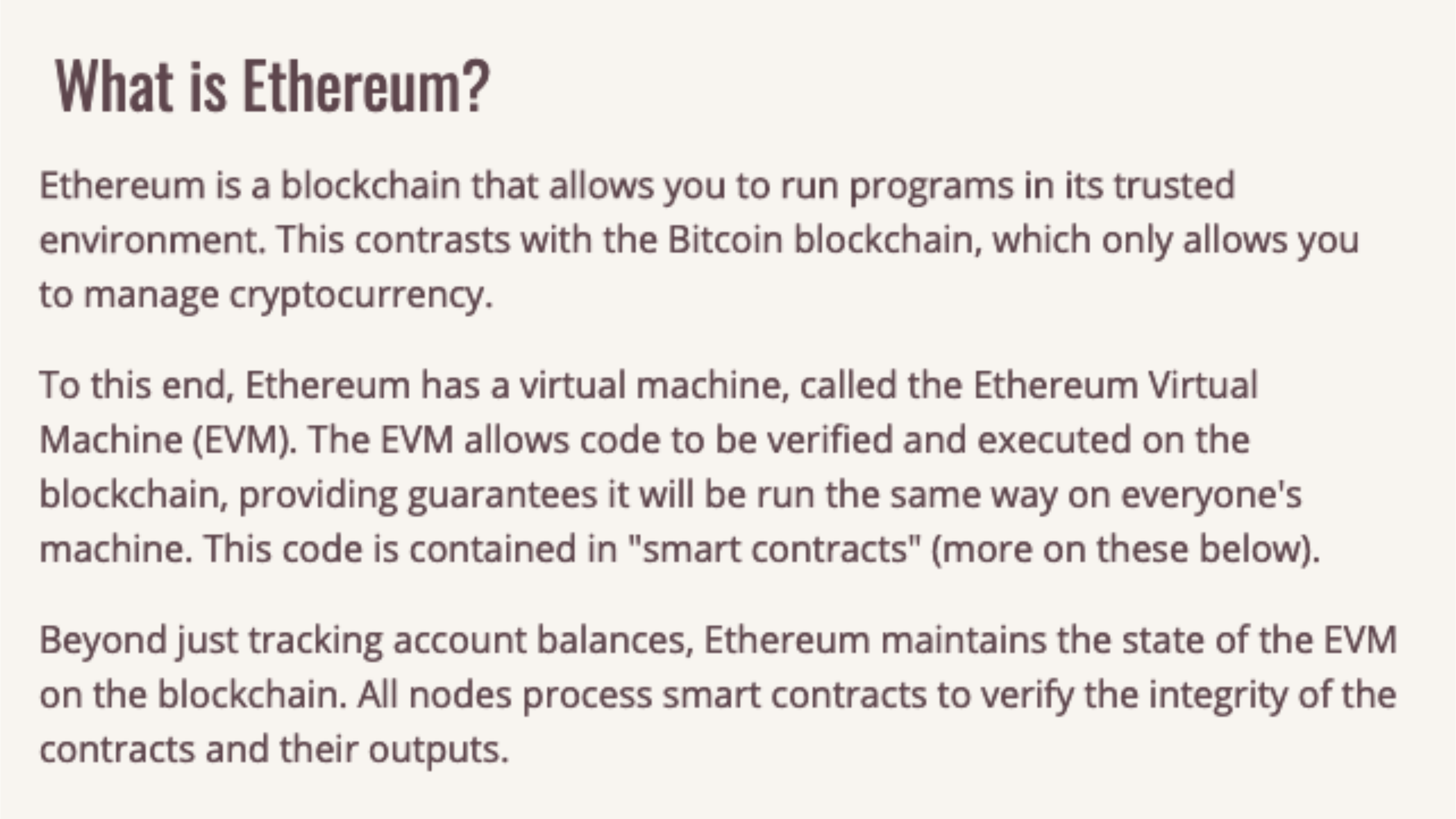
Cyrpto Hash Locks Blocks in Place

block contents

prev block ID	transactions	random guess (nonce)		hash result	?	target
f(#78A...,	tx#839, tx#a76,...,	3001)	=	438...	<	100...
f(#78A...,	tx#839, tx#a76,...,	3002)	=	988...	<	100...
f(#78A...,	tx#839, tx#a76,...,	3003)	=	587...	<	100...
f(#78A...,	tx#839, tx#a76,...,	3004)	=	087...	<	100...

Specified by "Blockchain" creator

OK to proceed

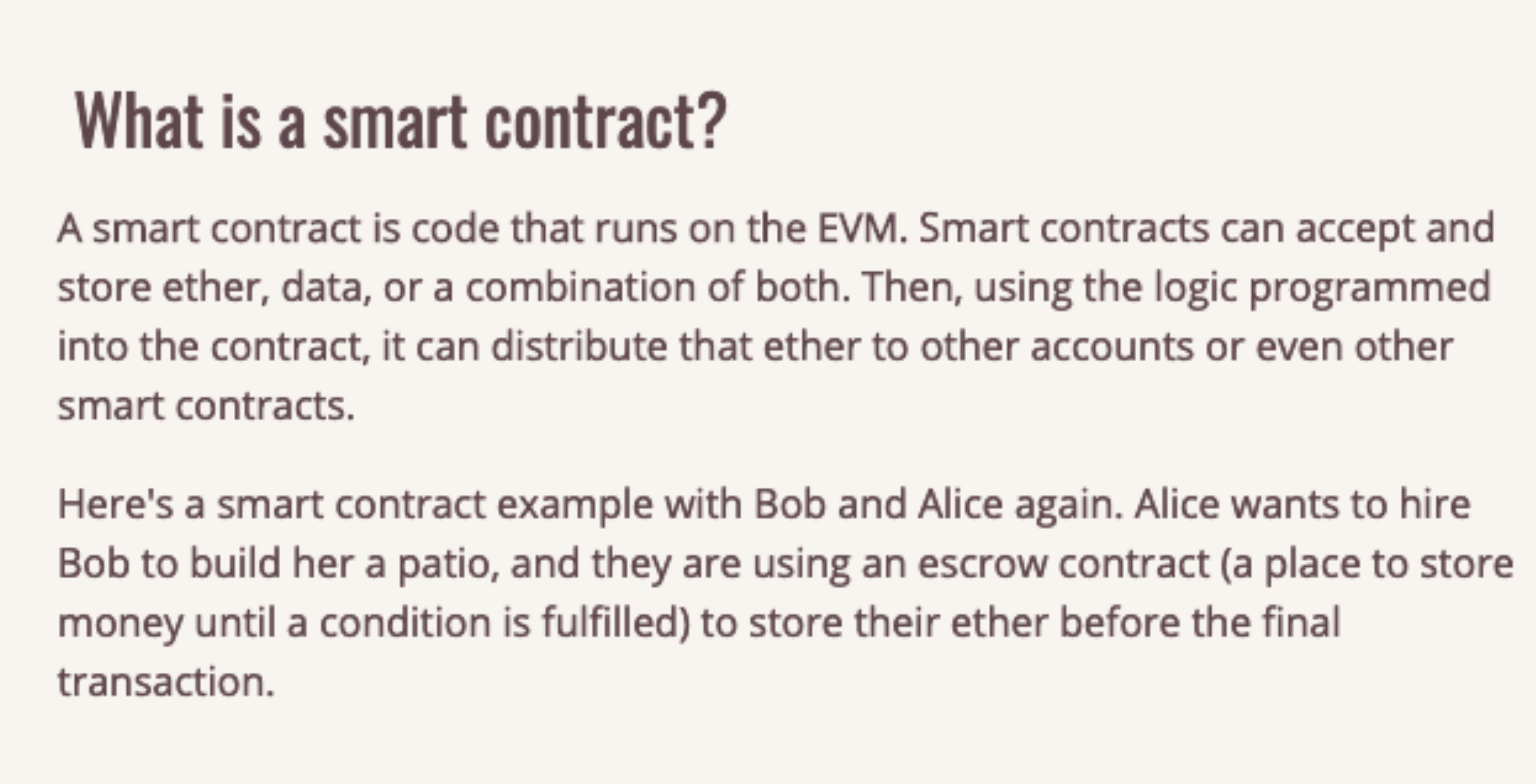


What is Ethereum?

Ethereum is a blockchain that allows you to run programs in its trusted environment. This contrasts with the Bitcoin blockchain, which only allows you to manage cryptocurrency.

To this end, Ethereum has a virtual machine, called the Ethereum Virtual Machine (EVM). The EVM allows code to be verified and executed on the blockchain, providing guarantees it will be run the same way on everyone's machine. This code is contained in "smart contracts" (more on these below).

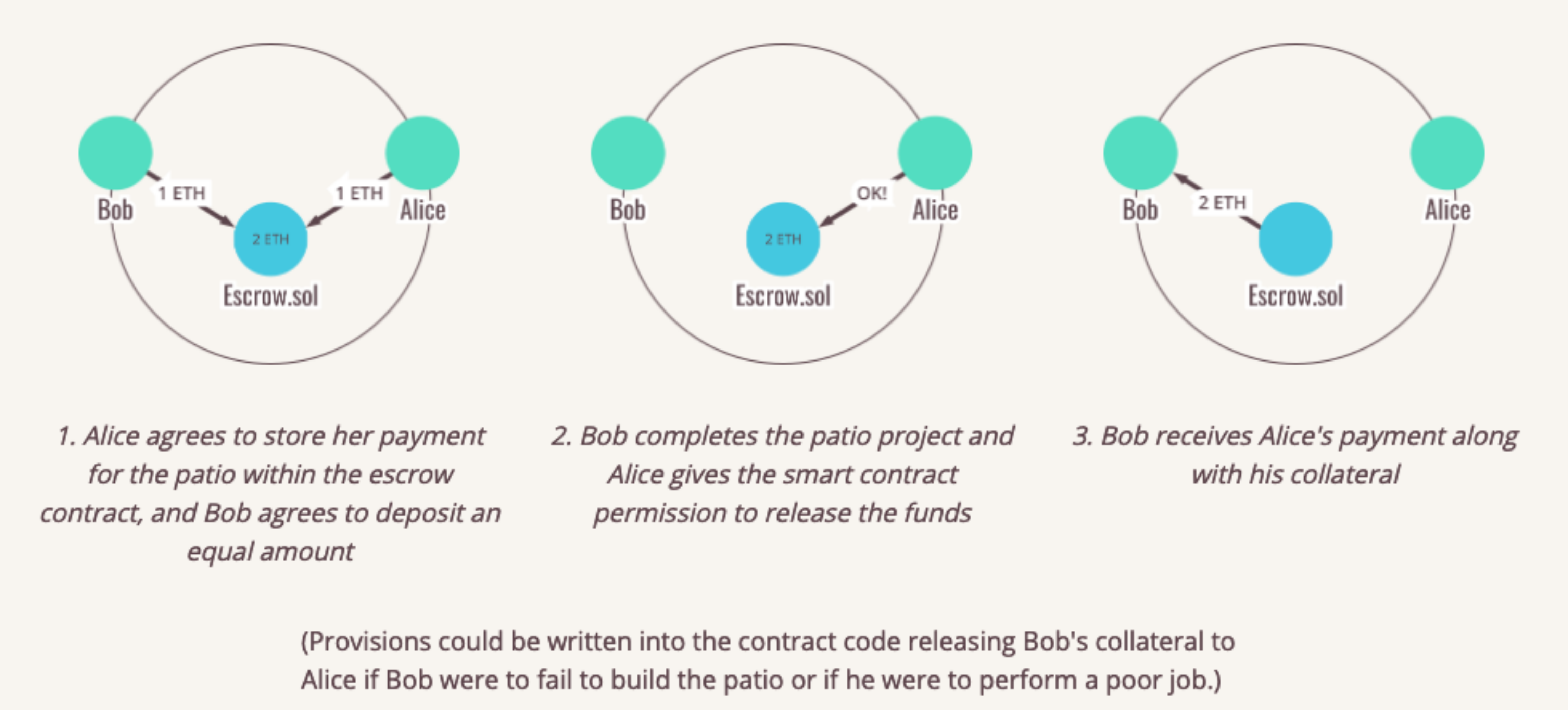
Beyond just tracking account balances, Ethereum maintains the state of the EVM on the blockchain. All nodes process smart contracts to verify the integrity of the contracts and their outputs.



What is a smart contract?

A smart contract is code that runs on the EVM. Smart contracts can accept and store ether, data, or a combination of both. Then, using the logic programmed into the contract, it can distribute that ether to other accounts or even other smart contracts.

Here's a smart contract example with Bob and Alice again. Alice wants to hire Bob to build her a patio, and they are using an escrow contract (a place to store money until a condition is fulfilled) to store their ether before the final transaction.



1. Alice agrees to store her payment for the patio within the escrow contract, and Bob agrees to deposit an equal amount

2. Bob completes the patio project and Alice gives the smart contract permission to release the funds

3. Bob receives Alice's payment along with his collateral

(Provisions could be written into the contract code releasing Bob's collateral to Alice if Bob were to fail to build the patio or if he were to perform a poor job.)

Demo: Sample Helloworld.sol code

```
pragma solidity >= 0.4.22 <0.6.6;

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;
    }
}
```

Demo Instructions

- Start Remix Compiler at https://remix.Ethereum.org
- Environments
  - Solidity
- From Top Left Panel, File Explorers -> Create a New File – Helloworld.sol
  - Cut and paste code into browser and save
- Solidity Compiler
  - Click on Blue Button to Compile Helloworld.sol
- Click on Deploy and Run Transactions
  - Make sure Environment is set to **JavaScript VM**
  - Click on pink button Orange Button Deploy under **Helloworld**
  - A smart contract **Helloworld** will be deployed in memory
- Run Code
  - Click on **down arrow** at **Helloworld** smart contract at bottom of screen (at memory location in blockchain)
  - Access its functions – die and printHello
  - Click on printHello function to see output “0: string: Hello, World”
  - Click on die function to remove smart contract from blockchain

References

- https://bitcoin.org/bitcoin.pdf – Original Paper by Satoshi Nakamoto, 10/28
- www.bitcoin.org – Original cryptocurrency, over 10 years old!
- www.blockchain.com/explorer - Great explorer to find all Bitcoins, Ethereum, BTC in Blockchain
- Byzantine Generals Problem – Lamport, Shostak, Pease, 1982
- www.Ethereum.org – Ethereum Project – founded by Vitalik Buterin in 2013
- https://gavwood.com/paper.pdf - Ethereum paper by Gavin Wood
- Ethereum White Paper and Smart Contracts – by Vitalik Buterin in Nov 2013
- XRP Ledger Consensus Protocol – Chase and MacBrough, 2018
- www.hyperledger.org – The Linux Foundation Project – Hyperledger
- https://anders.com/blockchain/ - Blockchain Demo
- https://www.ibm.com/blockchain - IBM Blockchain
- https://aws.amazon.com/blockchain/ - Amazon AWS Blockchain
- https://azure.microsoft.com/en-us/solutions/blockchain/ - MS Azure Blockchain

Questions, Comments, Feedback?

Debasis Bhattacharya (debasisb@hawaii.edu www.maui.hawaii.edu/cybersecurity)
University of Hawaii Maui College, July 2020