

Introduction to Blockchain and Portfolio Optimization with Bitcoins

Germán Creamer

Sources:

Arvind Narayanan et al., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton U. , 2016

Zvi Bodie, Alex Cane & Allan Marcus, Investments, 12 ed., McGraw Hill, 2018

William Stallings and Lawrie Brown, Computer Security: Principles and Practice, 2011

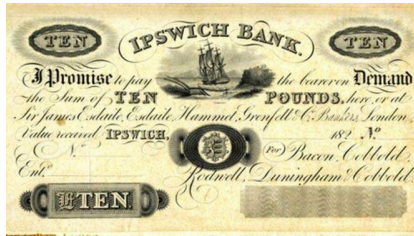
- Introduction to Blockchain and Cryptocurrencies
- Bitcoin as a financial asset and portfolio optimization

- Introduction to Blockchain and Cryptocurrencies
- Bitcoin as a financial asset and portfolio optimization

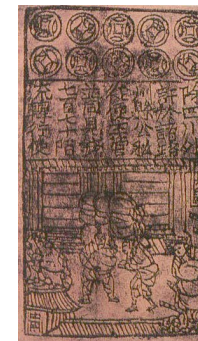
Role of Money

- Medium of exchange
- Store of value
- Unit of account

Is the bitcoin money?



US private bank note



Currency

- Legal tender for public and private debts, and can pay taxes
- Represented by:
 - Central Bank Notes (US dollar)
 - Central Bank Reserves &
 - Commercial Bank Deposits
- Relies upon system of ledgers
- Backed by the power of the sovereign
- High network effects from being unit of account
- Supported by the rule of law
- A currency is a currency because of the users' common beliefs: everyone agrees to use US dollars based on the belief that everyone will accept US dollars: accept dollars for private debt is by "fiat"



Bitcoin as a currency

- Bitcoin (BTC) or other cryptocurrencies are currencies, although BTC is not recognized as legal tender by any sovereign
- By itself, it does not have any value; however, used as a medium of exchange or a store of value may have value.
- Allows online transactions, offline transactions without cash or any transaction conducted by credit cards

Bitcoin as a decentralized currency

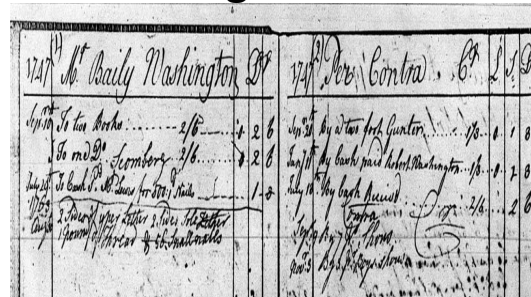
As the bitcoin does not depend on any external authority or intermediary, it should have:

- System of ownership rights: self-enforcing
- Maintain an accurate and secure ledger: self-enforcing

Proto Cuneiform
Uruk, ca 3000 B.C



Personal Ledger
G. Washington 1747



IBM 1961



Additionally, there are clear rules that define the currency supply and support trading.

Satoshi Nakamoto (alias): circulates the paper: Bitcoin: a peer-to-peer electronic cash system, 10/31/2008 (no trusted third party) <https://bitcoin.org/bitcoin.pdf>

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

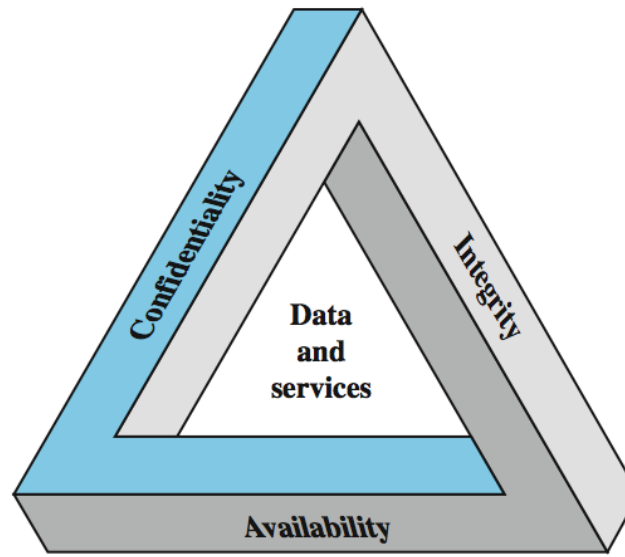
Cryptocurrencies failures

- Mondex (1993), CyberCash (1994), E-gold (1996), Hashcash (1997), Bit Gold (1998), B-Money (1998)
- DigiCash (1989, bankruptcy in 1998) founded by David Chaum.
 - Used CyberBucks with anonymous clients although merchants were not anonymous: no user-to-user transactions
 - Had a patent about a digital blind-signature similar to the one used by Bitcoin
- Lucre (1999): DigiCash without the technology with patents
- Magic Money (Authors: Cypherpunks (mailing list from where Satoshi appeared); violated DigiCash's patent

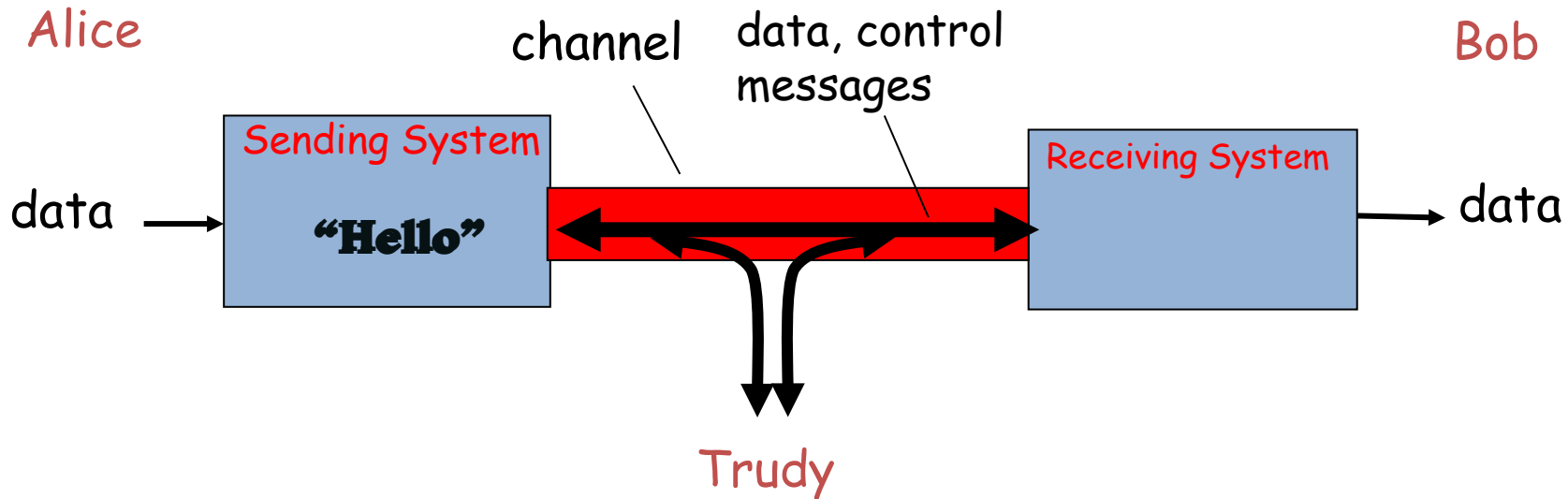
Typical problems: double spending, merchant acceptance and how to manage centralization vs. decentralization

Information Security

Protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity**, **availability** and **confidentiality** of information system resources (includes hardware, software, firmware, information/data, and telecommunications)



Confidentiality



Confidentiality: Preventing unauthorized disclosure of information or disclosure of information to unauthorized entities

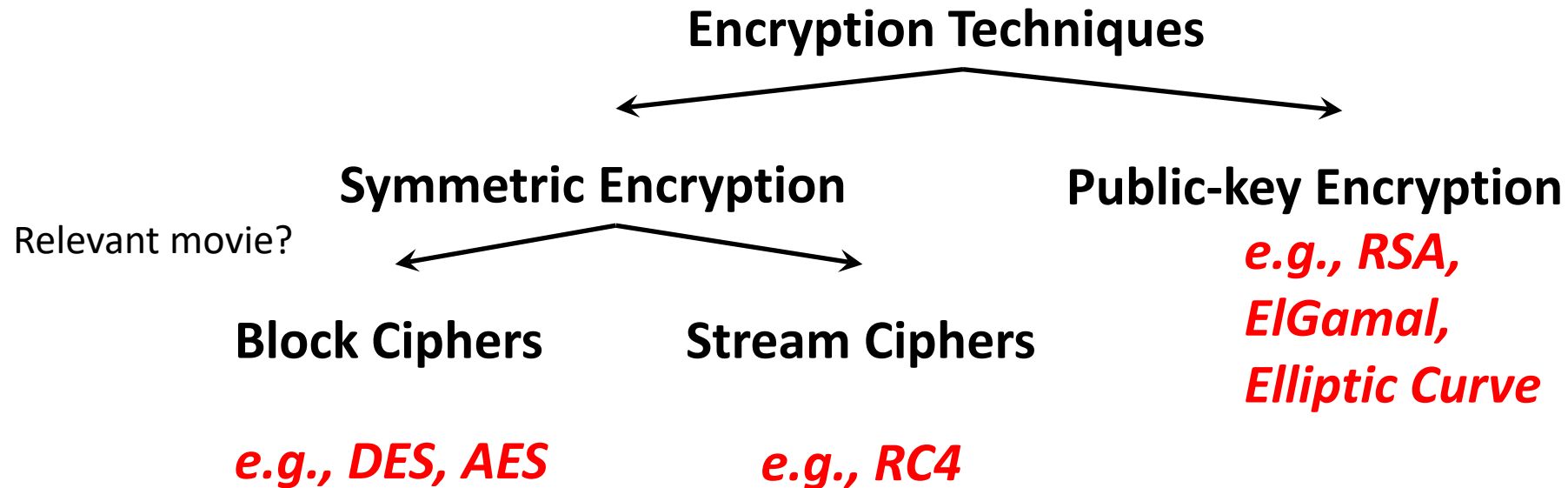
So, how to achieve confidentiality?

Encryption or Encipherment!

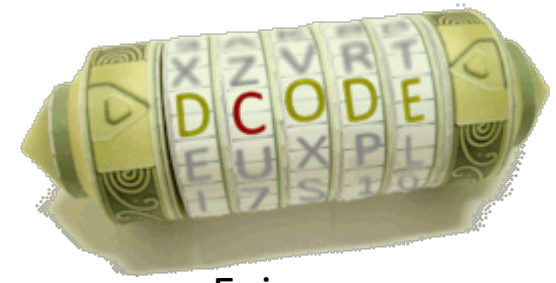
Encryption

What is Encryption (a.k.a Encipherment)?

- Process of perturbing or transforming information that needs to be protected (a.k.a ***plaintext***) into something that is unintelligible (a.k.a ***ciphertext***) to everyone except authorized receivers.



Symmetric Encryption



Enigma

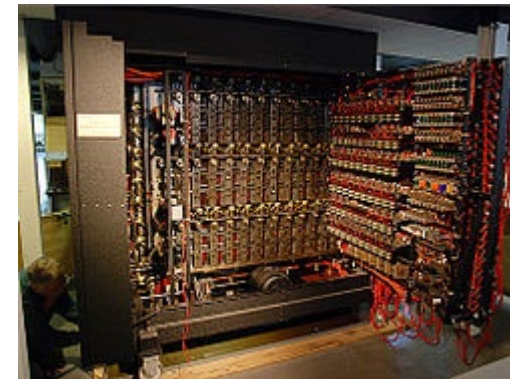
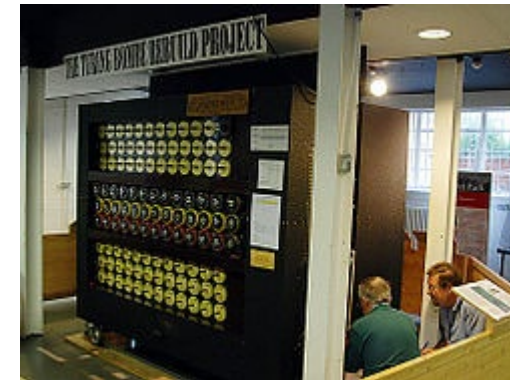
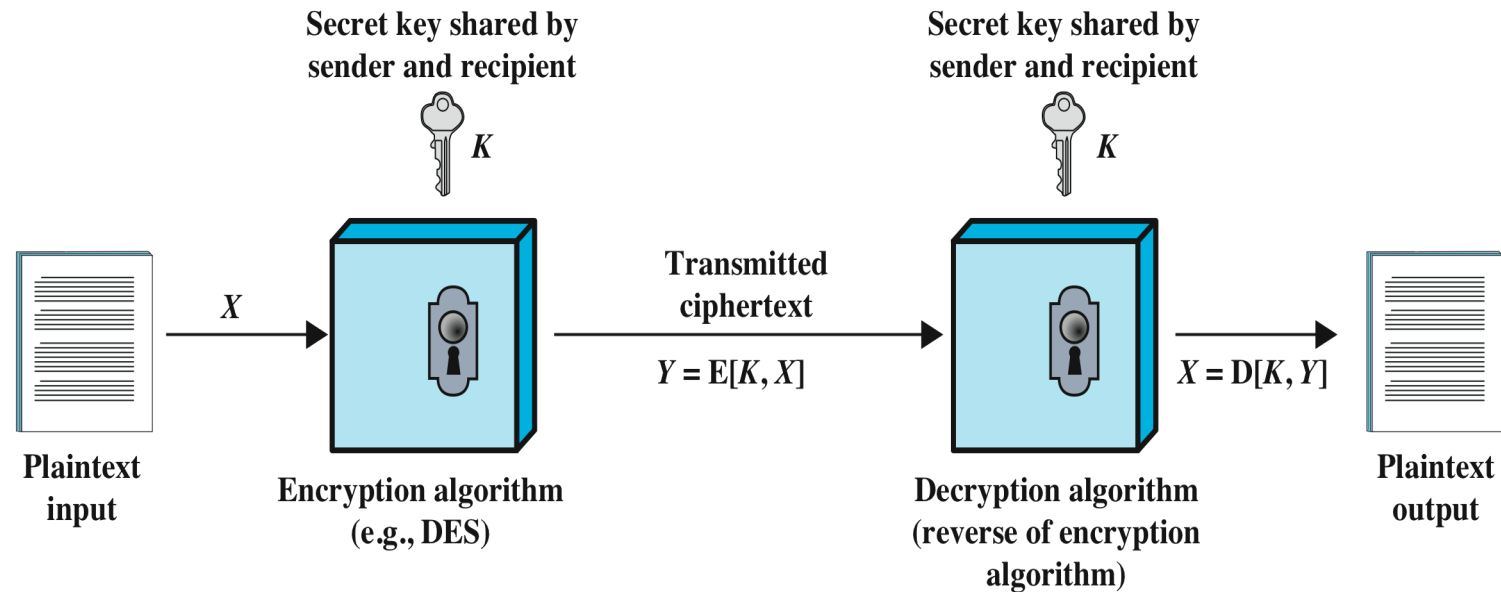
Turing project

Encryption algorithm based on permutation and substitution operations
Algorithm uses the same key for encryption and decryption - also referred to as **single-key** encryption

Two requirements for secure use:

- Needs a strong encryption algorithm

- Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure



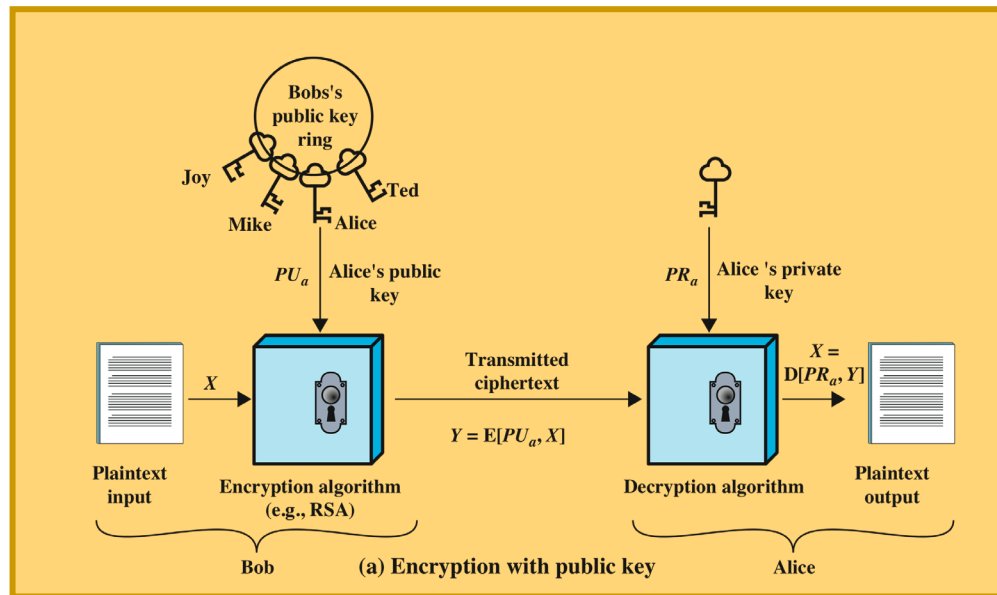
Public-Key Encryption

Encryption algorithms rely on mathematical functions that are easy to compute but difficult to invert!

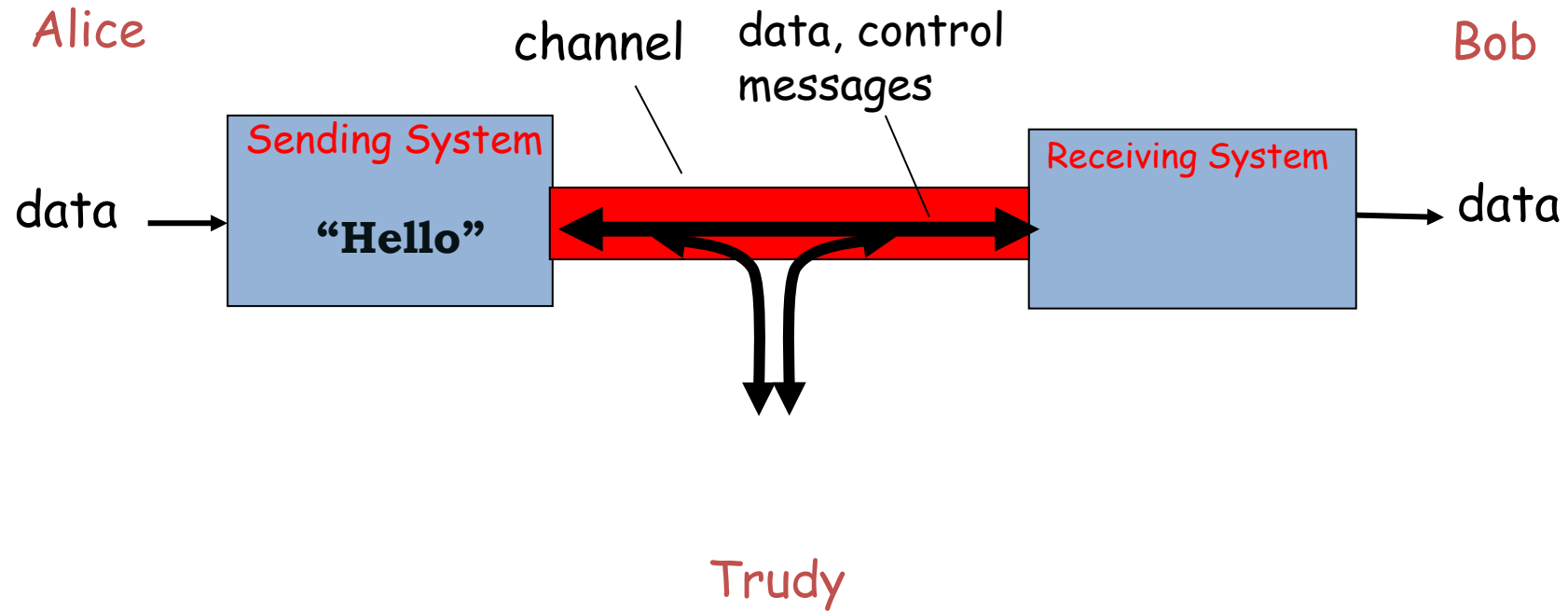
Asymmetric - uses two separate keys

Public key is made public for others to use

Private key is secret and is never released

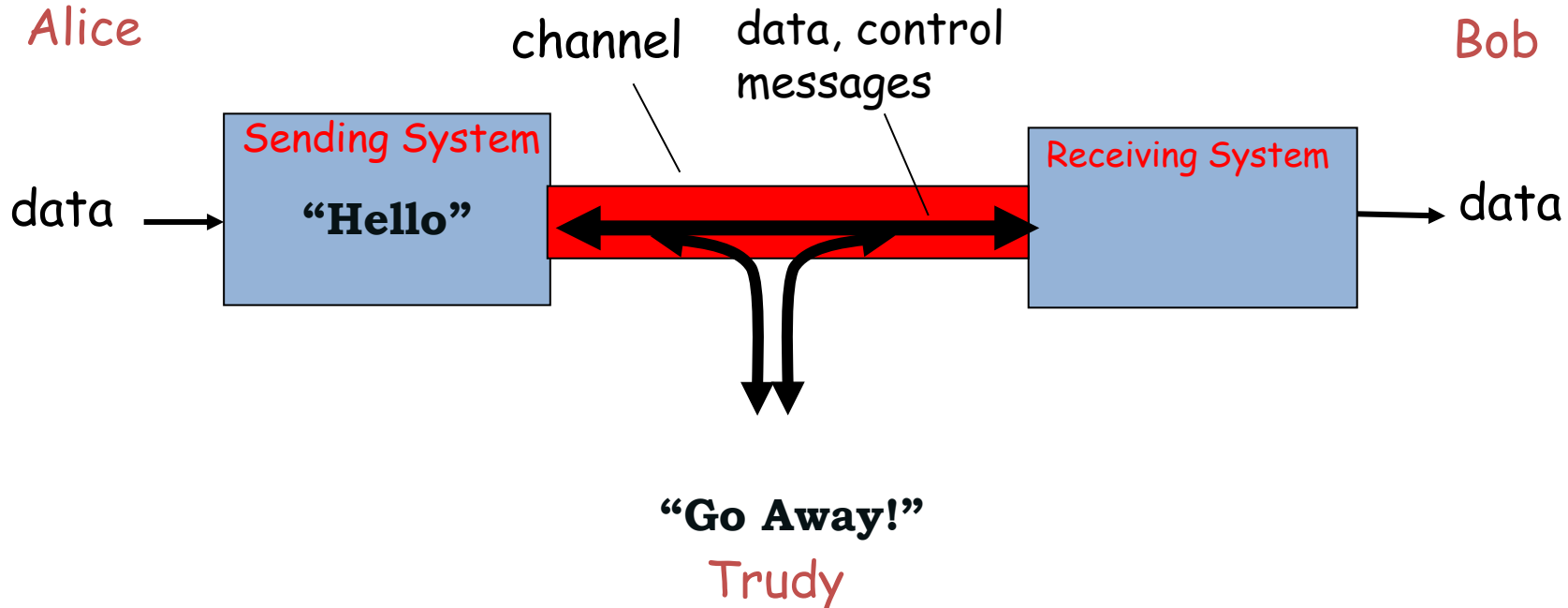


Availability



Ensuring timely and reliable access to and use of information.

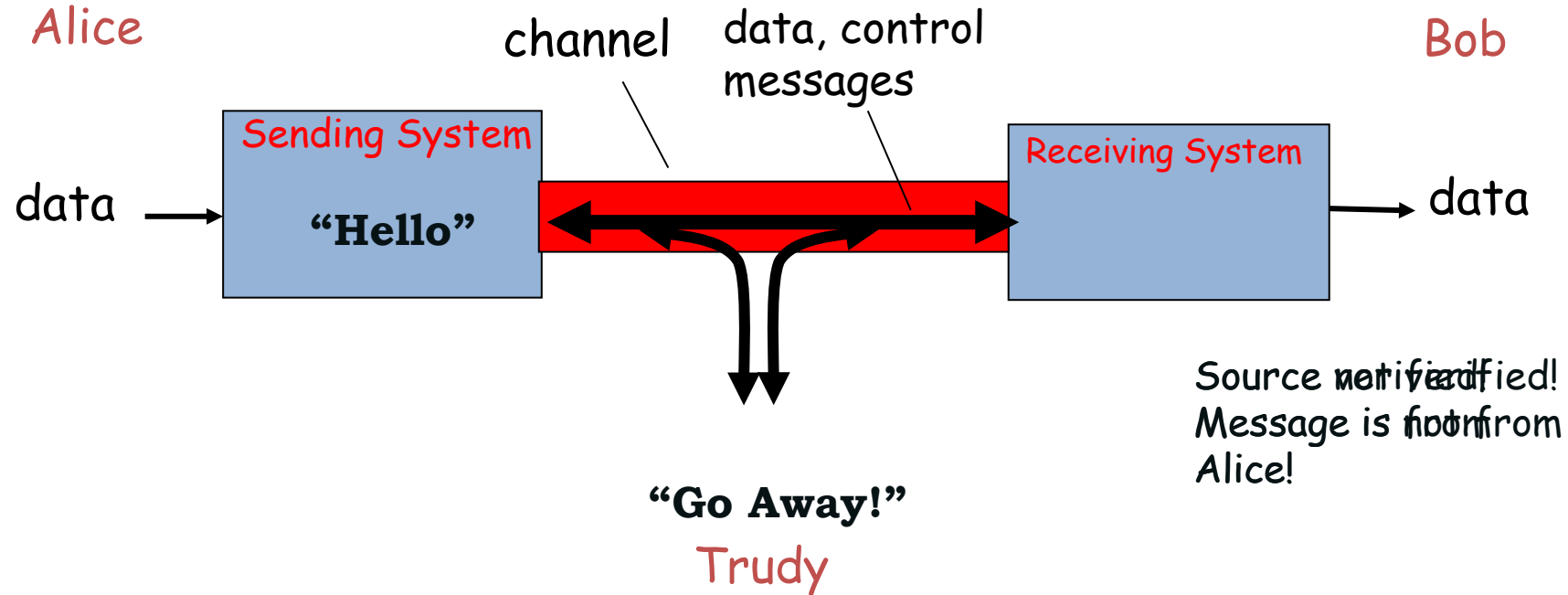
Integrity



Integrity: Preventing unauthorized modification of information or modification of information by unauthorized entities.
Includes **authenticity**

So, how to achieve Integrity?
Message Authentication Codes (MAC)!

Authenticity



Authenticity: Integrity protection + enabling verification of the authenticity of the information (and its origin)

So, how to achieve Authenticity?

Digital Signatures!

Digital Signatures used by Bitcoins

Bitcoin uses Elliptic Curve Digital Signature Algorithm (ECDSA) standard, a US Government standard, over the standard elliptic curve secp256k1:

- Provides 128 bit of security (equivalent to performing 2^{128} symmetric encryptions)

- Private key – 256 bits

- Public key compressed – 257 bits

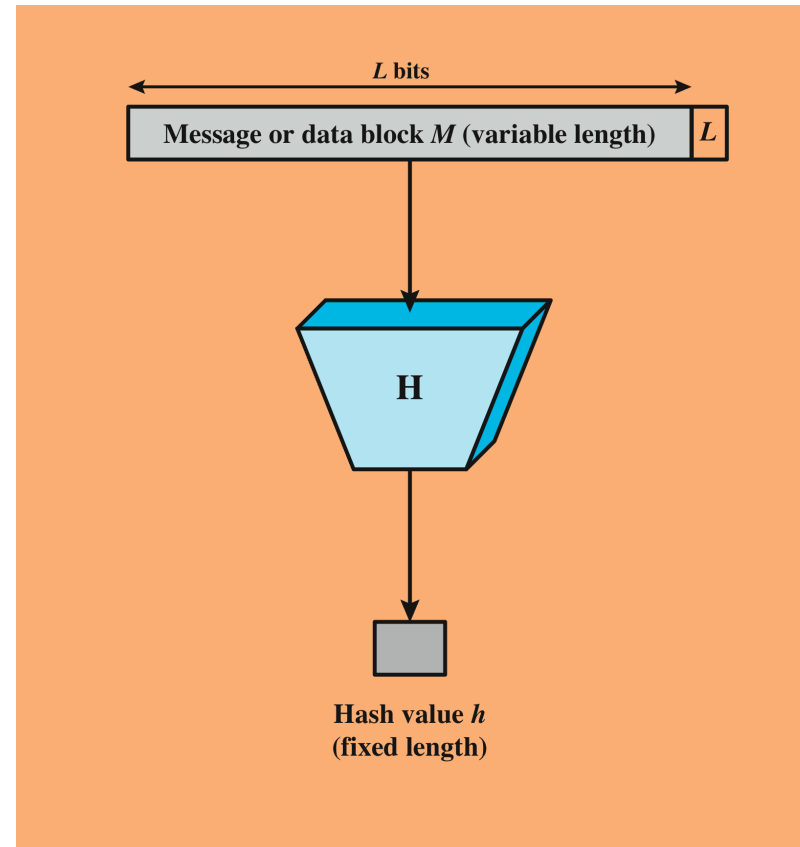
- Message to be signed – 256 bits (as all messages are hashed, any size message can be signed)

- Signature – 512 bits

Good randomness is essential for ECDSA. Otherwise, generateKeys() or sign() → probably leak private key

Secure Hash Functions

Important cryptographic primitive required for both Message Authentication Codes and Digital Signatures



Hash functions are key in the design of cryptocurrencies

What are Hash functions?

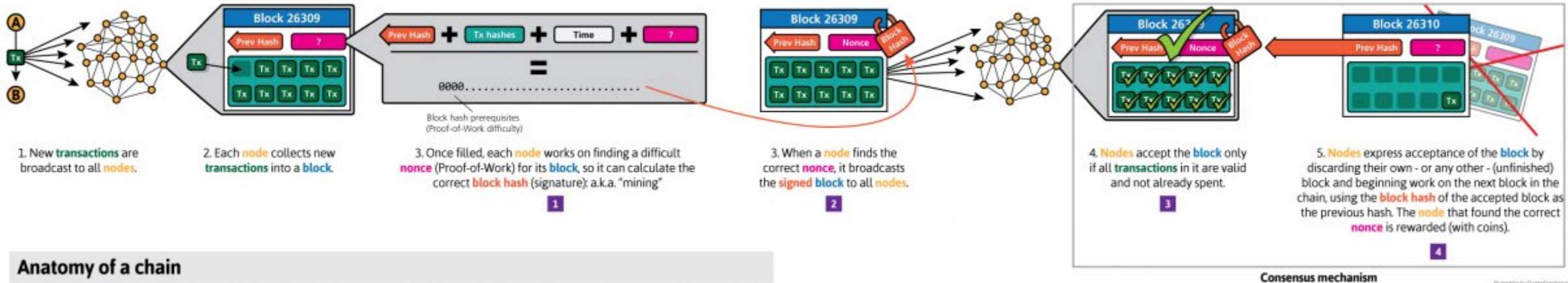
Mathematical functions: A mapping of items (values) in the domain to items (values) in the range.

Hash functions are special mathematical functions that satisfy the following three properties:

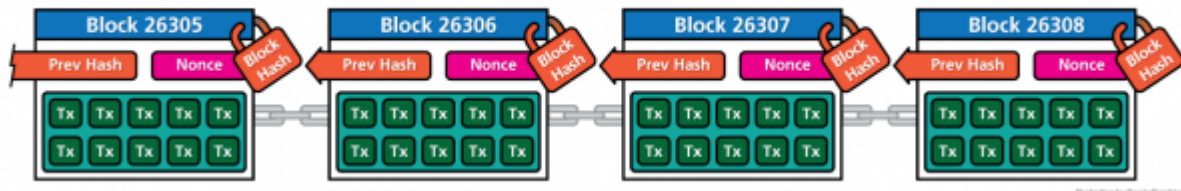
- Inputs (or items in the domain) can be any size (not-fixed)
 - Size of input is not unbounded in practice
- Outputs (or items in the range) are fixed-size (i.e. SHA-256: output of 256 bits)
- Efficiently computable, i.e., the mapping should be efficiently (in polynomial time in terms of the input size) computable

Blockchain: basics

Running the network (Proof of Work example)



Anatomy of a chain

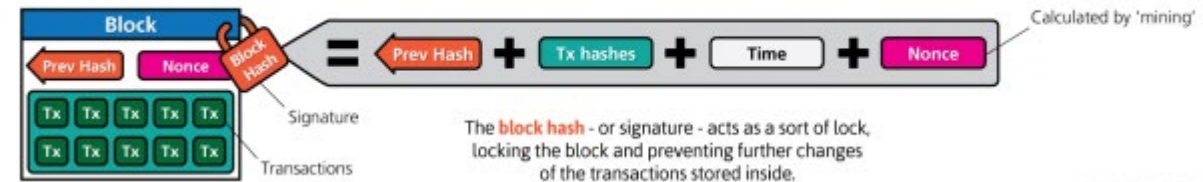


Blockchain simulator:

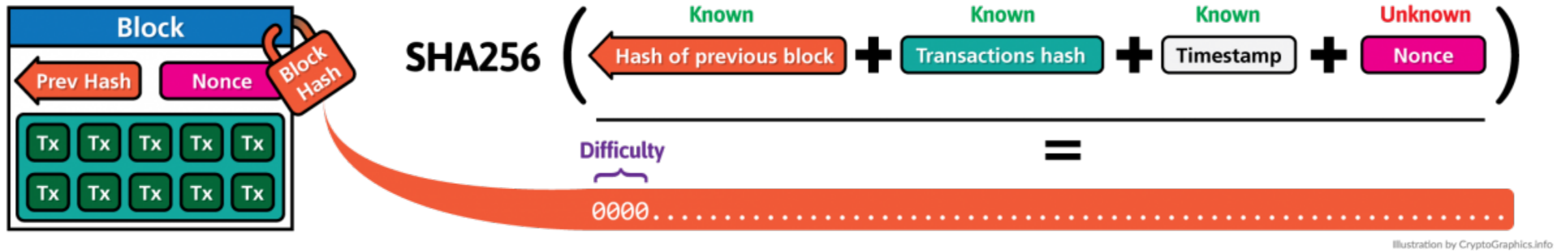
<https://code.hnldesign.nl/blockchain>

Source: cryptographics.info

Anatomy of a block



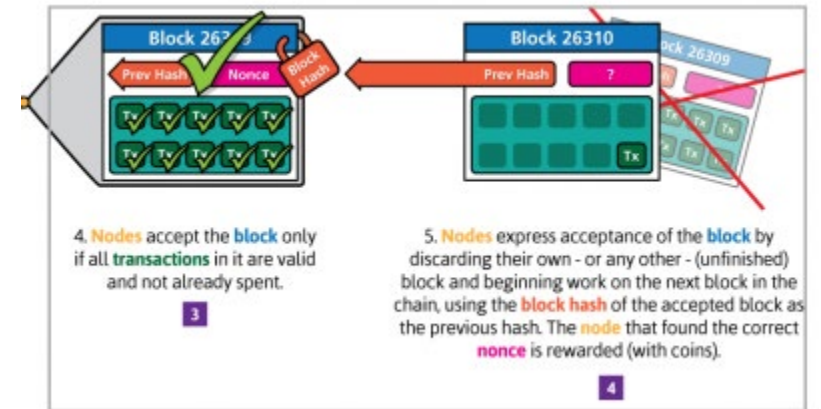
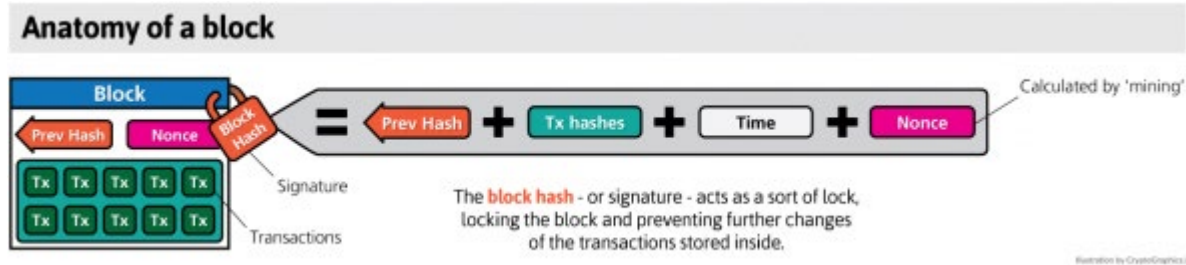
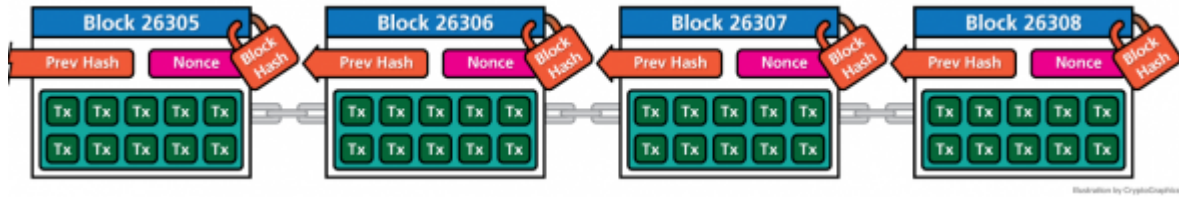
Blockchain: proof of work



Source: cryptographics.info

Blockchain Technology

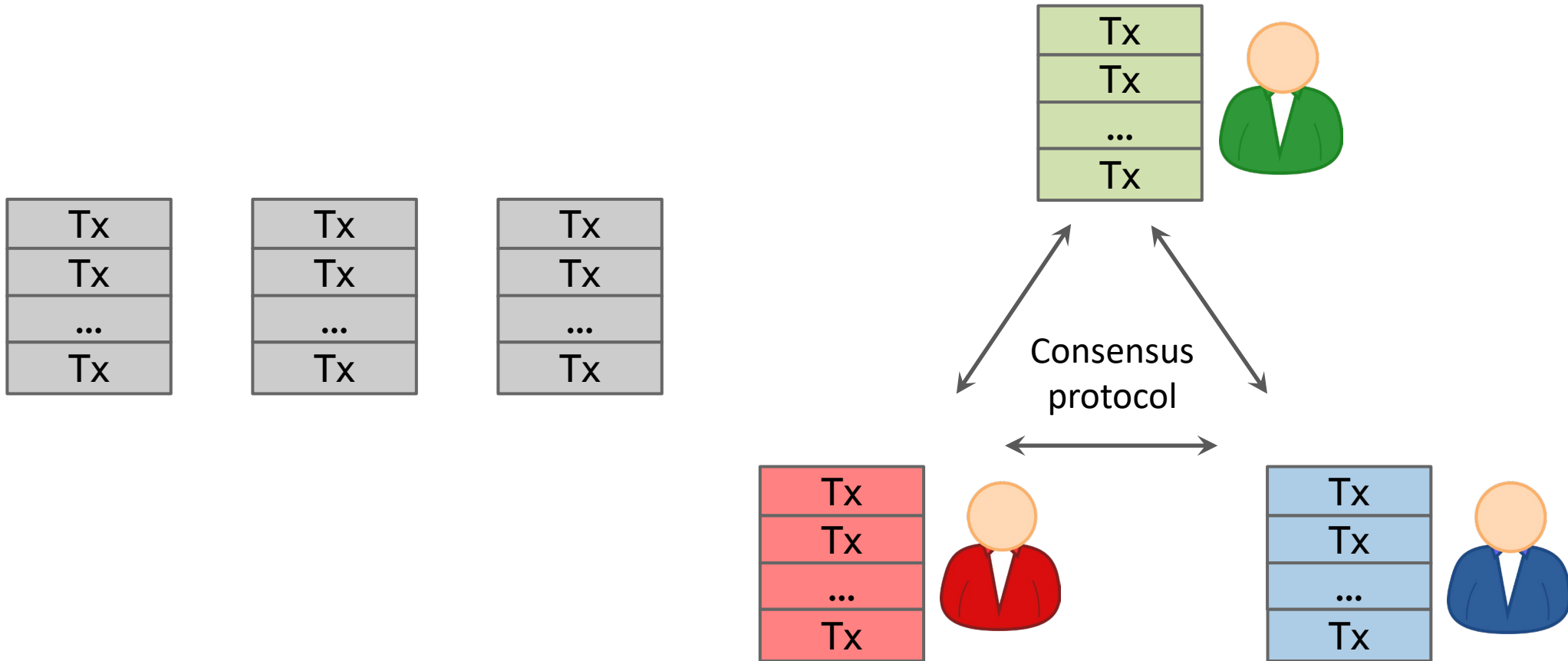
Timestamped append-only log



Consensus protocol: deals with '**cost of trust**' as in the Byzantine Generals problem

Auditable database secured by cryptography: hash functions for integrity & resistance to tamper, digital signatures for consent, consensus

How consensus could work in Bitcoin



OK to select any valid block, even if proposed by only one node

Consensus algorithm (simplified)

1. New transactions are broadcast to all nodes
2. Each node collects new transactions into a block
3. In each round a random node gets to broadcast its block
4. Other nodes accept the block only if all transactions in it are valid (unspent, valid signatures)
5. Nodes express their acceptance of the block by including its hash in the next block they create

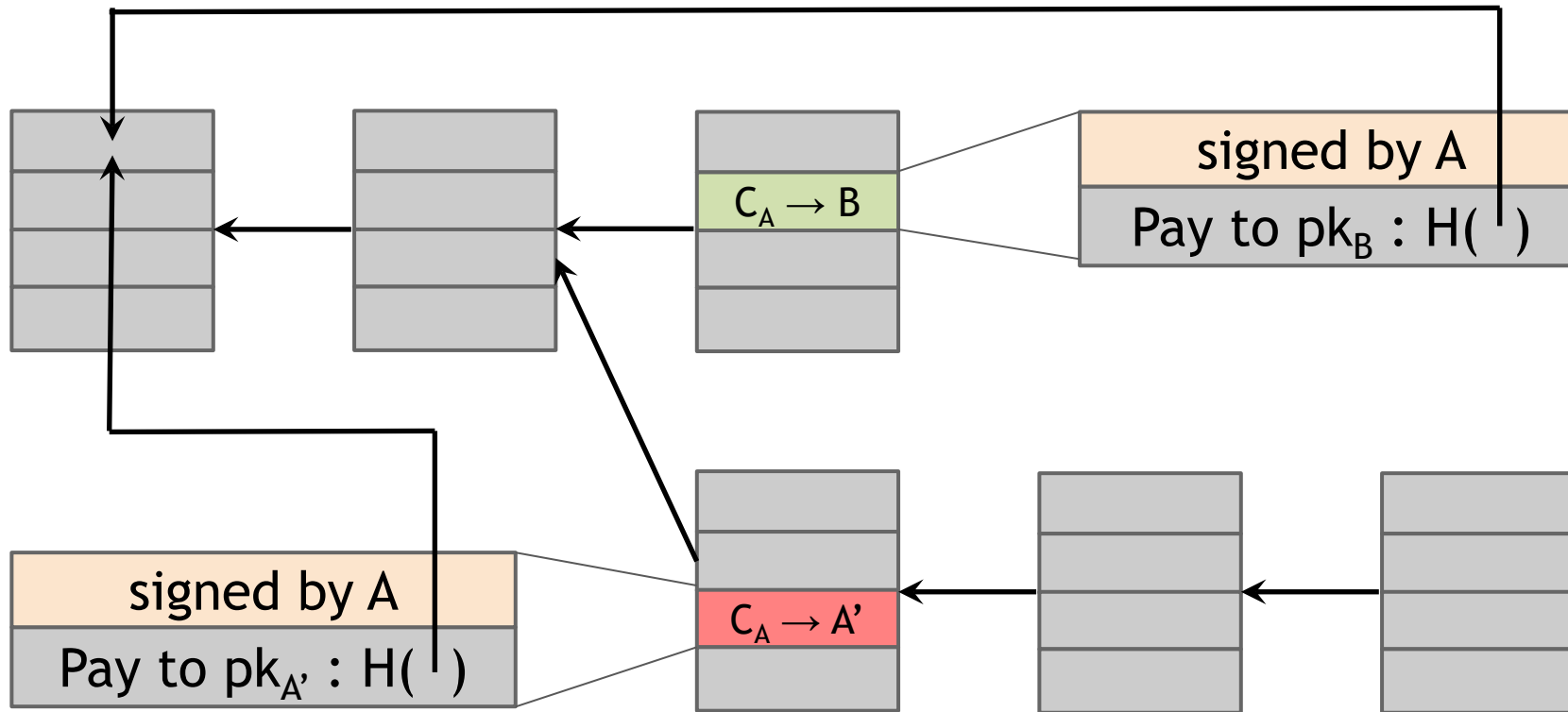
Testing

Assume a malicious adversary.

Can this adversary subvert the implicit consensus process by:

- 1. Stealing Bitcoins?**
- 2. Denial of service?**
- 3. Double spend?**

What can a malicious node do?

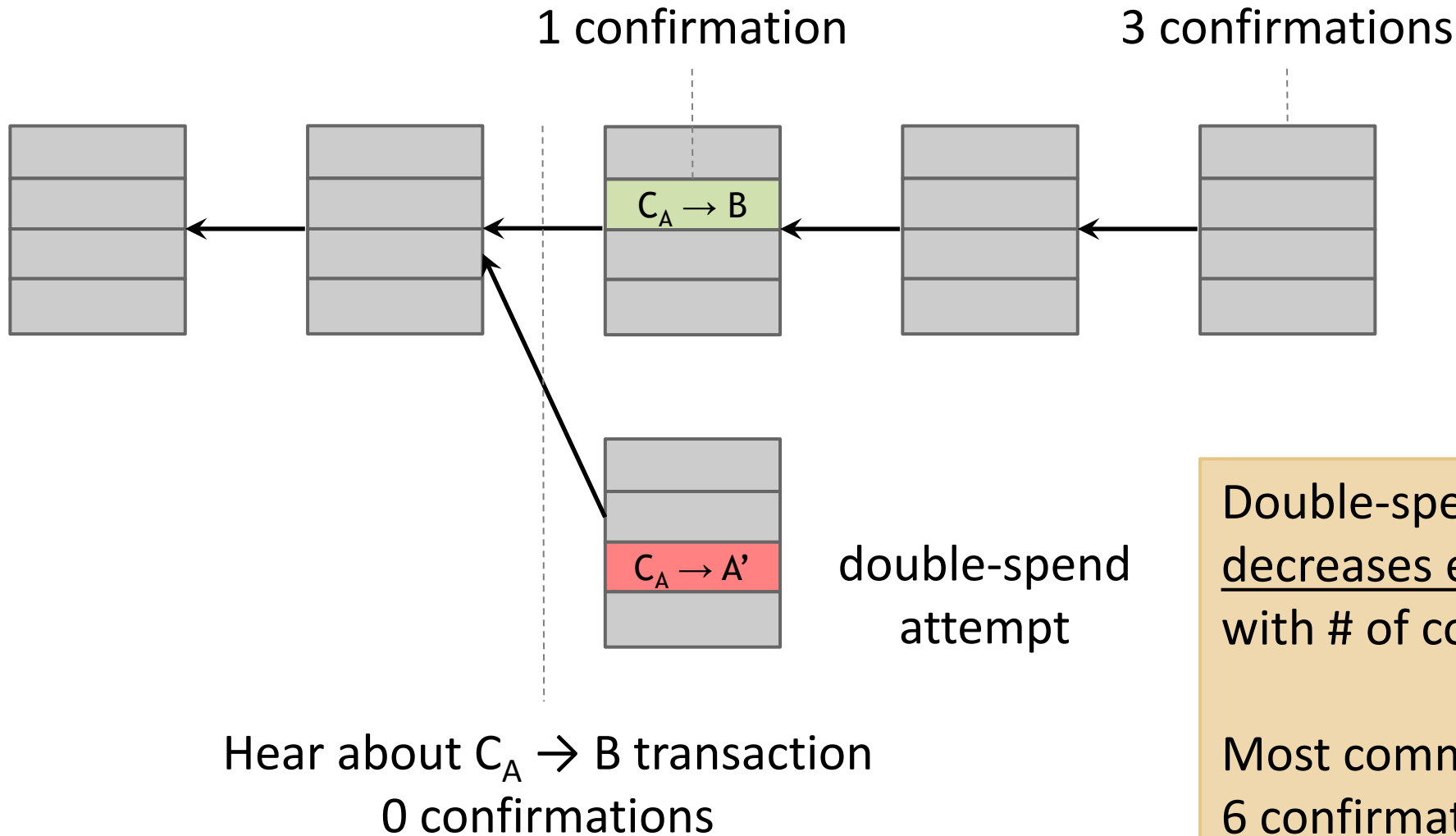


Double-spending attack

Honest nodes will extend the longest valid branch

In practice nodes extend the block that they first detect on the peer-to-peer network (not a solid rule)

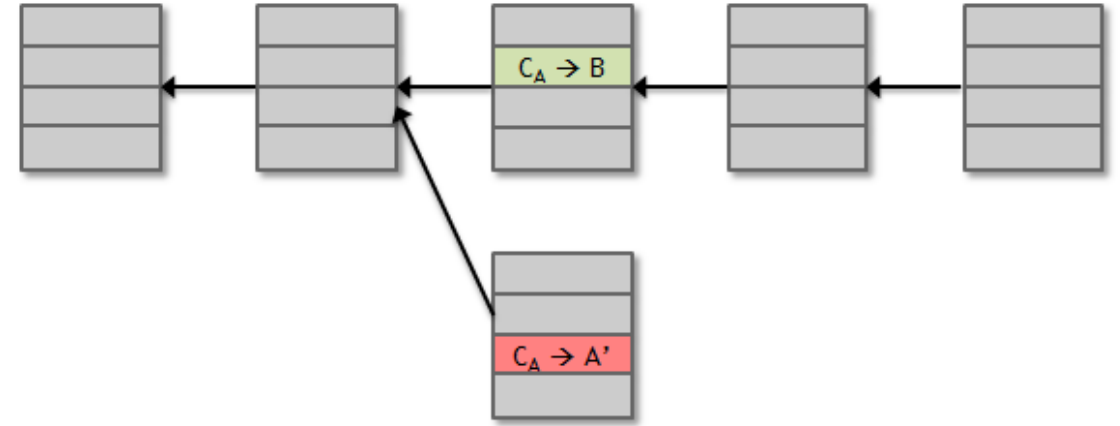
From Bob the merchant's point of view



Double-spend probability
decreases exponentially
with # of confirmations

Most common heuristic:
6 confirmations

Invalid transactions/double spending



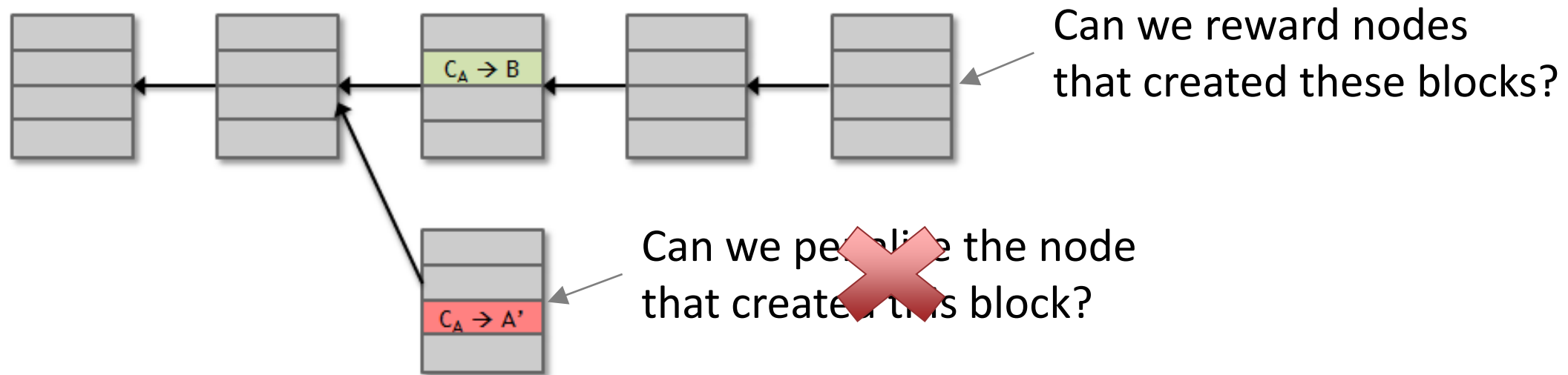
Protection against invalid transactions is cryptographic,
but enforced by consensus

Protection against double-spending is by consensus

Never 100% sure a transaction is on the consensus branch.
Guarantee is probabilistic

Assumption of honesty is problematic

Can we give nodes incentives for behaving honestly?



Everything so far is just a distributed consensus protocol
But now we utilize the fact that the currency has value

Incentive 1: Block Reward

Creator of block

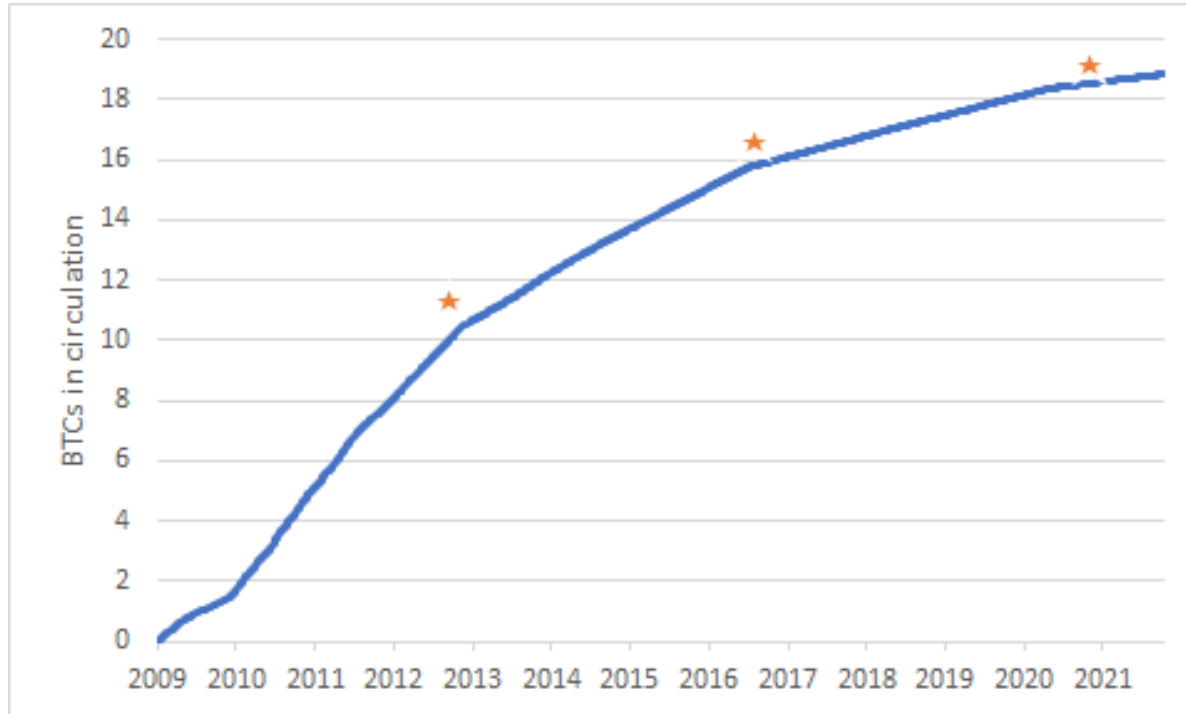
- includes special coin-creation transaction in the block
- Chooses recipient address of this transaction

Incentive is fixed: halves the pace of new BTC creation every 210,000 blocks created (or every 4 years at the current rate of block creation) until 21 millions are mined.

First period block reward was 50 BTC. Halved in: 2012 to 25 BTC. 2016: to 12.5 BTC; May 11, 2020 to 6.25 BTC per block mined.

Block creator gets to “collect” the reward only if the block ends up on long-term consensus branch! Incentivizes nodes to behave in way that motivate other nodes to extend their block

There's a finite supply of bitcoins



→ 21 million BTCs

Block reward is how
new bitcoins are created

Runs out in 2040. No new bitcoins
unless rules change

Stars (2012, 2016, 2020): inflection
points. Halving generation of new
BTCs

Incentive 2: Transaction Fees

Creator of transaction can choose to make output value less than input value

Difference: transaction fee for block creator (who puts first that transaction into that block)

Purely voluntary: will become mandatory, as Block rewards run out

Bitcoin Transaction Feed



Fees increased in late-2017 and April 2021, but are lower in October 2021 (\$3.3)

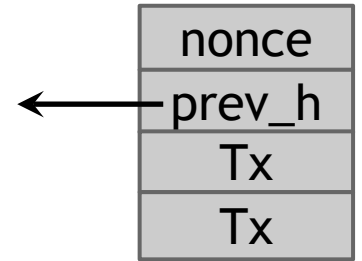
Proof of work

To approximate selecting a random node: *select nodes in proportion to a resource that no one can monopolize*

- **proof-of-work:** in proportion to computing power:
(Used in Bitcoins)
 - Let nodes compete for right to create block
 - Make it moderately hard to create new identities
- **proof-of-stake:** In proportion to ownership of the currency: *(Not used in Bitcoins – used in other cryptocurrencies)*

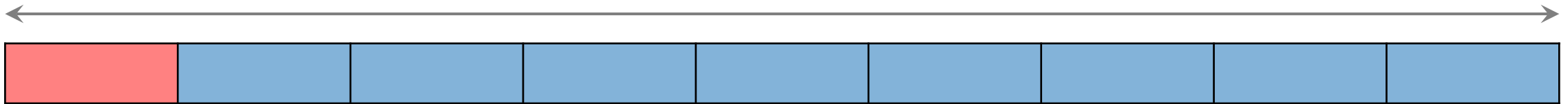
Hash puzzles

To create block, find nonce s.t.
 $H(\text{nonce} \parallel \text{prev_hash} \parallel \text{tx} \parallel \dots \parallel \text{tx})$ is very small



In other words, $H(\text{nonce} \parallel \text{prev_hash} \parallel \text{tx} \parallel \dots \parallel \text{tx}) < \text{target}$

Output space of hash



Target
space

If hash function is secure (*satisfies puzzle-friendliness*):
only way to succeed is to try enough nonces until you get lucky

Advantages of PoW system

Solves problem of picking a random node (to propose a block)

Nodes independently compete by attempting to solve hash puzzles: Once in a while, one will succeed and propose the next block

Result: decentralized system → No one gets to decide which node proposes the next block

Mining benefits and costs

If mining reward (block reward + Tx fees)	>	mining cost (hardware + electricity cost)	→	Profit
--	---	---	---	--------

Complications:

- Fixed (hardware) vs. variable (electricity) costs
- Reward depends on rate at which miners propose blocks (ratio of their hash rate to the global hash rate)
- Cost in dollars, but reward in BTC → profit depends on exchange rate

Summary of Bitcoin's distributed consensus protocol

- Transactions are broadcasted to the network
 - Nodes collect the transactions into a block
 - Nodes are chosen at random to propose a block
 - In subsequent rounds, other nodes accept or reject that block
 - Disagreements become forks in the blockchain
 - Short forks are usually abandoned – it is the policy of honest nodes to extend the longest fork
-
- Bitcoin: system of property rights without centralized authorities
 - Across jurisdictions: facilitate international trade

Mechanics of Bitcoins: The Ledger

- The ledger contains a record of all Bitcoin transactions
 - A memory system
- The equivalence between money and memory was proposed by economist Narayana Kocherlakota in 1998
- Along with the digital signature, the accurate ledger is required for the existence of property rights in Bitcoin

Bitcoin Innovation: Incentives

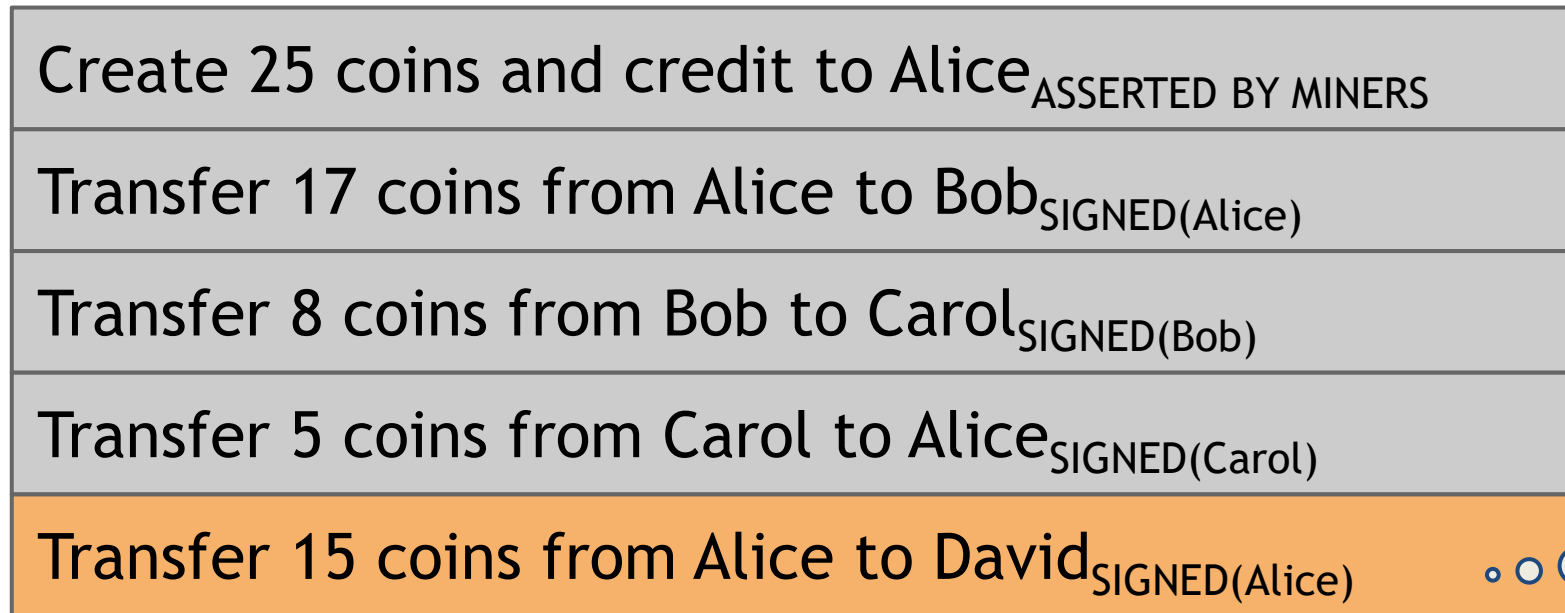
- Satoshi's solution
 - In previous attempts to decentralize, creators focused on making it impossible to tamper with the ledger
 - Satoshi realized that it was sufficient (and much easier) to have incentives not to tamper with the ledger

How to dis-incentivize participants from tampering with the ledger?

- By making it easy to detect that the ledger had been tampered with
 - Any dishonest participant would then be dissuaded from even trying

An account-based ledger (*not* Bitcoin)

time

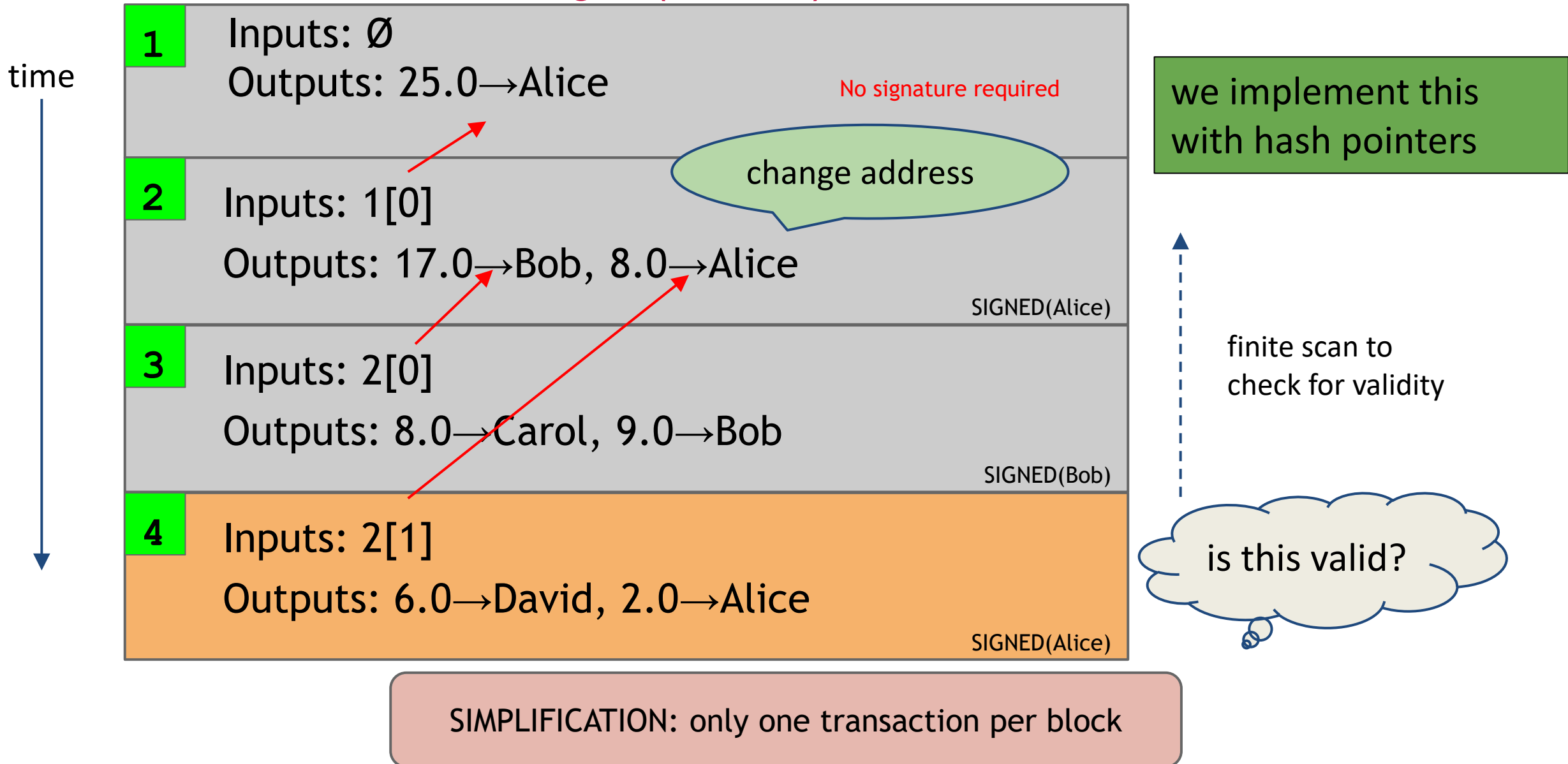


might need to
scan backwards
until genesis!

is this valid?

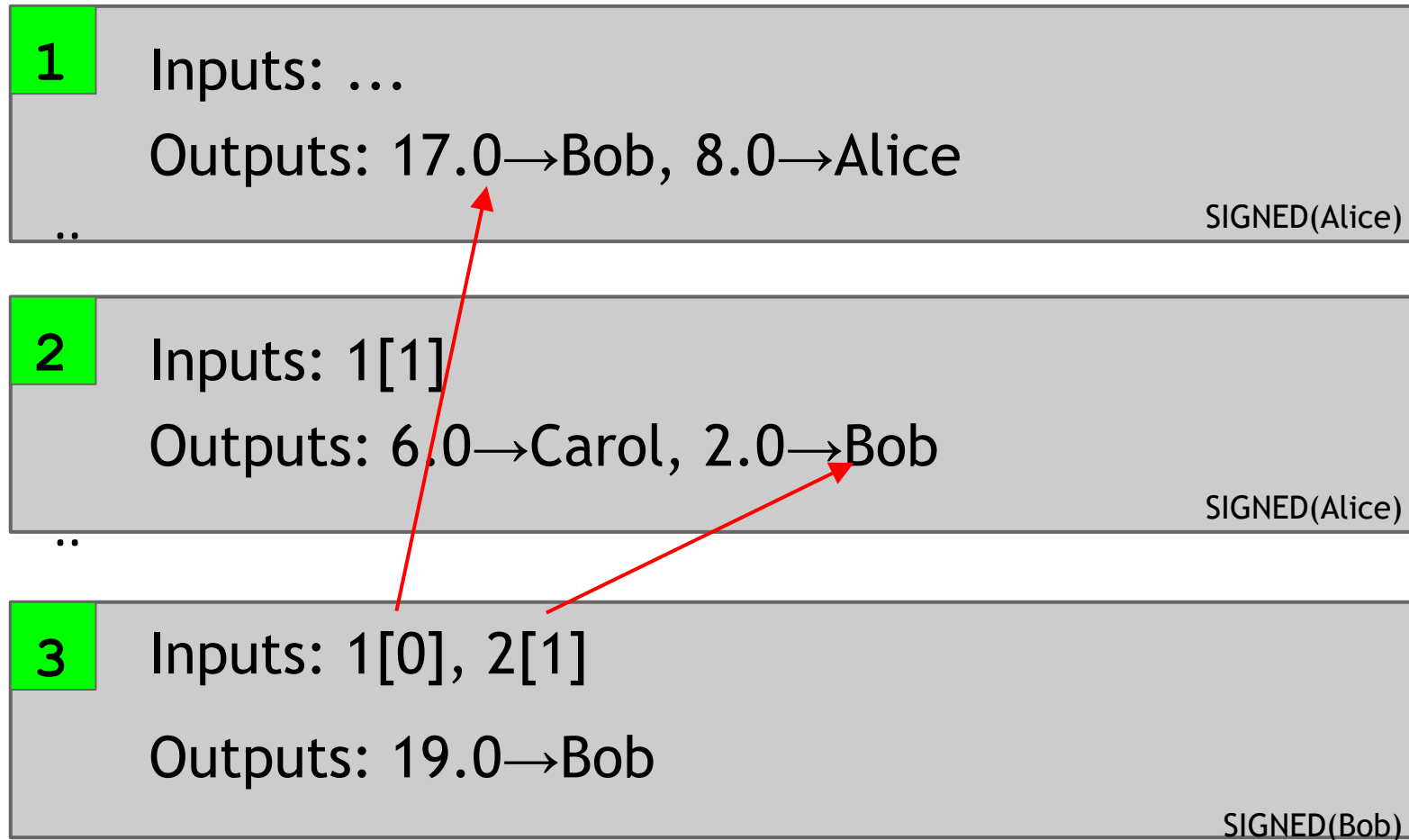
SIMPLIFICATION: only one transaction per block

A transaction-based ledger (Bitcoin)



Merging value

time



Consolidating funds: Bob consolidates 17 + 2 BTC into 19 BTC

Joint payments

time



1 Inputs: ...
Outputs: 17.0→Bob, 8.0→Alice
.. SIGNED(Alice)

2 Inputs: 1[1]
Outputs: 6.0→Carol, 2.0→Bob
.. SIGNED(Alice)

3 Inputs: 2[0], 2[1]
Outputs: 8.0→David
SIGNED(Carol), SIGNED(Bob)

two signatures!

Joint payment: Carol and Bob paid 6 +2 to David

Summary

- A tamper-proof ledger is a key feature of Bitcoin that enforces property rights
- How do you make a ledger tamper-proof when it is distributed?
 - You make sure any attempts will be discovered
 - By making the ledger recursive. Every entry contains a little copy of the previous entry.

The real deal: a Bitcoin transaction



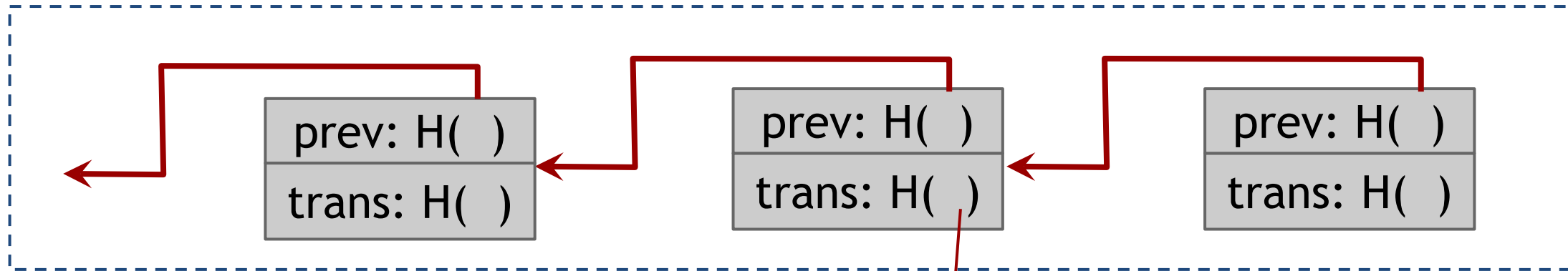
Bitcoin blocks

Transactions are grouped together into blocks

- Single unit of work for miners
- Length of hash-chain of blocks is shorter than a hash-chain of transactions.
 - Faster to verify history

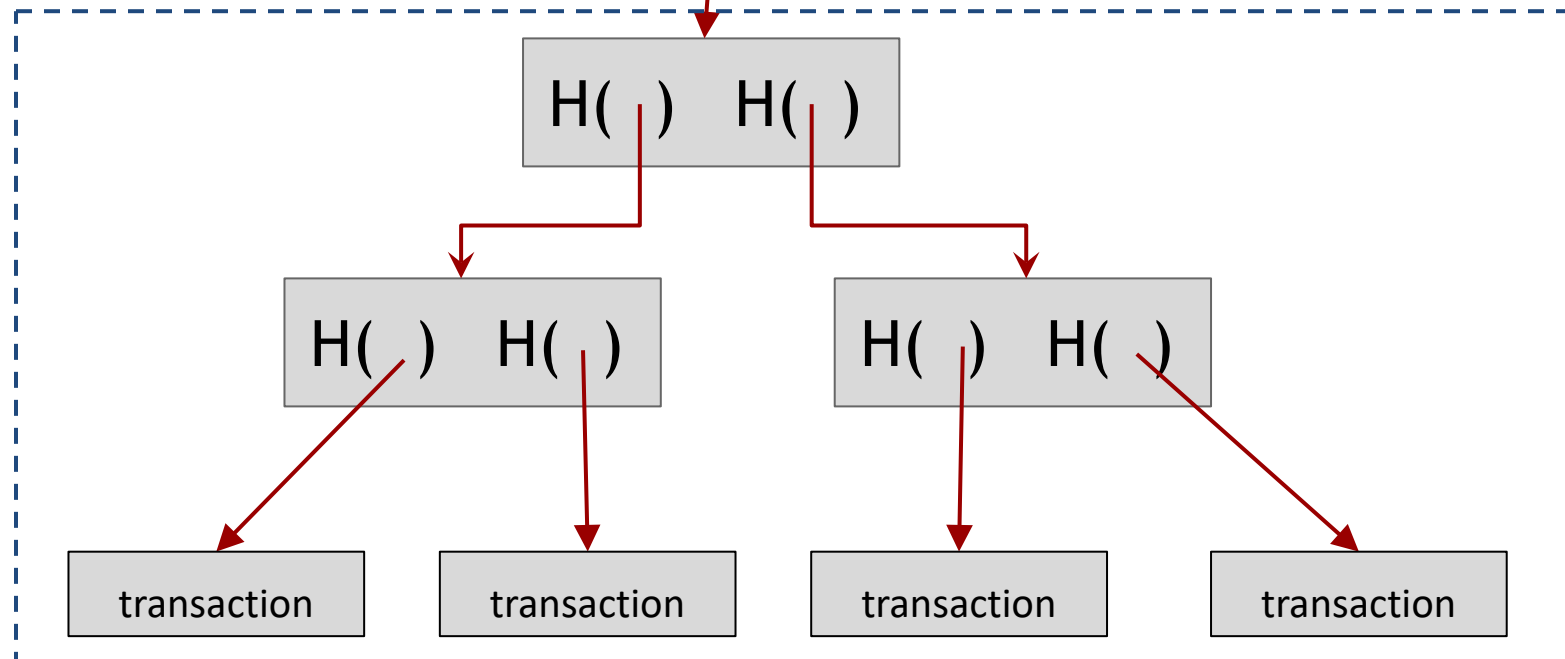
Bitcoin block structure

Hash chain of blocks



Hash tree (Merkle tree) of transactions in each block





To verify a chain of blocks, look at the headers



Explore a transaction

blockchain.com

<https://www.blockchain.com/btc/tx/6dda0b4695a6e83cf0978a7ceb91bb1aa084cda993cf80bdc5cd341760eebec2>

Fee	0.00008112 BTC (24.143 sat/B - 6.036 sat/WU - 336 bytes)	0.00385298 BTC
Hash	6dda0b4695a6e83cf0978a7ceb91bb1aa084cda993cf80bdc5cd341... 	2021-10-24 13:19
	<div>1QJdDEGEtzm38tAcBmPo22N48qDRXmhhA0.00076410 BTC </div> <div>14DLFWvsuhbKrde6N3NyhLaJ3kTn1x4LnY0.00317000 BTC </div>	<div>31j3r3yBJPZp9omQaoB1HF69BQgCpZjRe0.00385298 BTC </div>

This transaction was first broadcast to the Bitcoin network on October 24, 2021 at 1:19 PM EDT. The transaction currently has 1,085 confirmations on the network. At the time of this transaction, 0.00385298 BTC was sent with a value of \$232.37. The current value of this transaction is now \$232.82. Learn more about [how transactions work](#).

Details ⓘ

Hash	6dda0b4695a6e83cf0978a7ceb91bb1aa084cda993cf80bdc5cd341760eebec2
Status	Confirmed
Received Time	2021-10-24 13:19
Size	336 bytes
Weight	1,344
Included in Block	706484
Confirmations	1,085
Total Input	0.00393410 BTC
Total Output	0.00385298 BTC
Fees	0.00008112 BTC
Fee per byte	24.143 sat/B
Fee per vbyte	N/A

- Introduction to Blockchain and Cryptocurrencies
- Bitcoin as a financial asset and portfolio optimization

Trading and investing in cryptocurrencies

- Valuation of cryptocurrencies using modern finance theory
- Introduction to portfolio theory
- How to include a cryptocurrency in a portfolio?

Cryptocurrency as a Financial Asset

- “Probably rat poison squared”, Warren Buffet, Berkshire Hathaway CEO
5/5/2018
- “If you're stupid enough to buy it, you'll pay the price for it one day”
- “A fraud, worse than tulip bulbs” James Dimon, JP Morgan CEO, 2017

Equity valuation

- A basic principle in finance is that the value of an asset is the present value of its futures cash flows.
- For equity valuation, this leads to the dividend discount model:

$$V_0 = \frac{D_1}{1+k} + \frac{D_2}{(1+k)^2} + \frac{D_3}{(1+k)^3} + \dots$$

V_0 = current value

D_t = dividend at time t

k = required rate of return

DDM says V_0 = the present value of all expected future dividends into perpetuity

Recommendations of equity valuation models for cryptocurrencies

- Gordon growth model: assumes that dividends grow at constant rate g :

$$V_0 = \frac{D_0(1+g)}{k-g} = \frac{D_1}{k-g}$$

V_0 = current value

D_t = dividend at time t

k = appropriate risk-adjusted interest rate

g = dividend growth rate

As cryptocurrencies do not pay dividends or do not have any future cash flows as stocks or bonds, their price should be zero. However, if it is used as a medium of exchange, then it may have a minimum value.

Equity valuation models do not recommend to invest on cryptocurrencies. Is there an alternative view?

Trading with cryptocurrencies

Assuming a daily trading decision to buy a financial asset without any additional cash flow payments in $t = 1$ and sell it in $t = 2$, simple return is:

$$R_t = \frac{P_t - P_{t-1}}{P_{t-1}}$$

- or continuously compounded (or log) return (used in this presentation):

$$r_t = \ln(1 + R_t) = \ln \frac{P_t}{P_{t-1}}$$

- For cryptocurrencies, the price is the US dollar value of each crypto.
- Above calculations overestimate cryptocurrencies' returns as it does not consider transaction costs or any operational challenge which could be substantial during certain periods.
- Survivor bias: historical analysis may not consider cryptos that failed, only evaluating returns of cryptos that have survived.

Top cryptocurrencies by level of capitalization

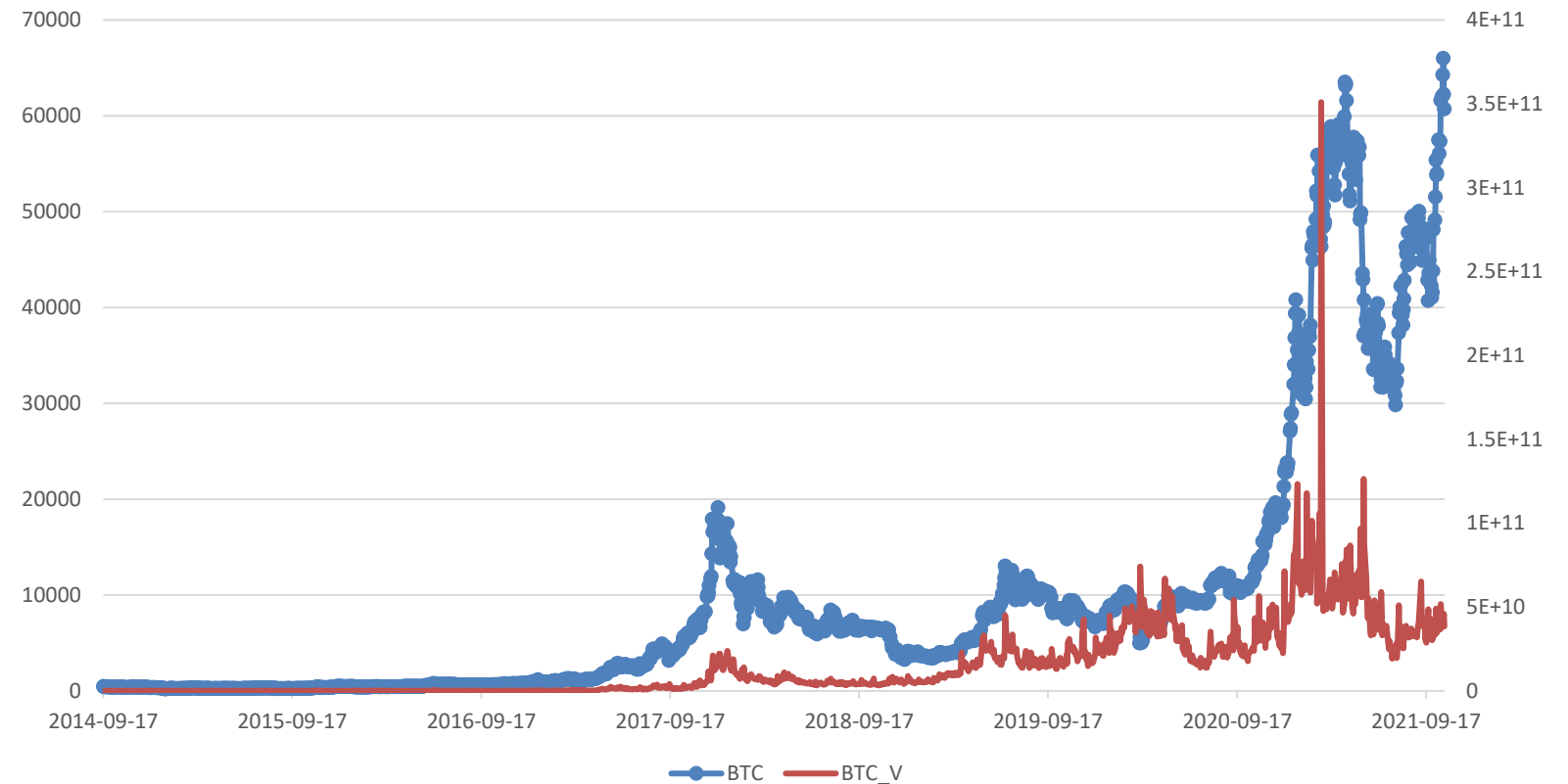
	Symbol	Company Name	Last Price	Change	% Change	Market Time	Volume	Avg Vol (3 month)	Market Cap
→	BTC-USD	-	62130.836	-716.88	-1.14%	8:42 PM GMT+1	31.53B	35.39B	1,171.49B
→	ETH-USD	-	4219.7344	+32.30	+0.77%	8:42 PM GMT+1	14.99B	21.02B	498.30B
(Crypto and exchange)	BNB-USD	-	485.09506	+1.09	+0.22%	8:41 PM GMT+1	1.37B	2.05B	80.91B
→	ADA-USD	-	2.1713064	+0.02	+0.89%	8:41 PM GMT+1	2.59B	4.20B	72.21B
	USDT-USD	-	0.9999574	-0.00	-0.05%	8:41 PM GMT+1	71.55B	76.16B	69.66B
	SOL1-USD	-	208.18259	-2.75	-1.30%	8:42 PM GMT+1	3.08B	3.20B	62.65B

<https://finance.yahoo.com/u/yahoo-finance/watchlists/crypto-top-market-cap/>

October 26, 2021

Bitcoin price in USD (BTC) and trading volume (BTC_V)

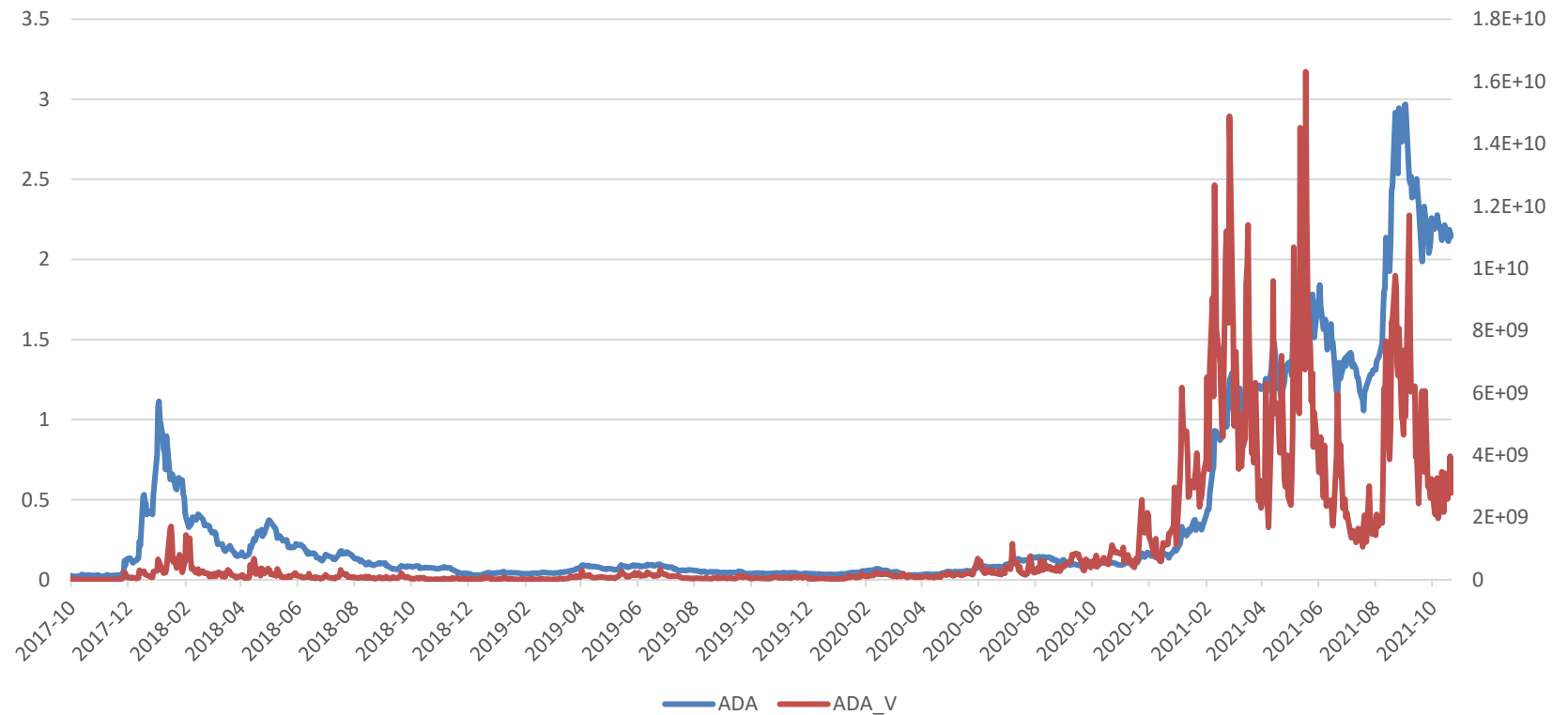
- Created in 2009 by Satoshi Nakamoto
- Runs on a blockchain:
- Proof-of-work validation: high energy consumption
- Prices and trading volume (right axis) tend to move together
- Prices dropped in 2018 and Covid crisis 2020, and in both cases recovered very well.



Source: finance.yahoo.com

ADA (ADA) price in USD (ADA) and trading volume (ADA_V)

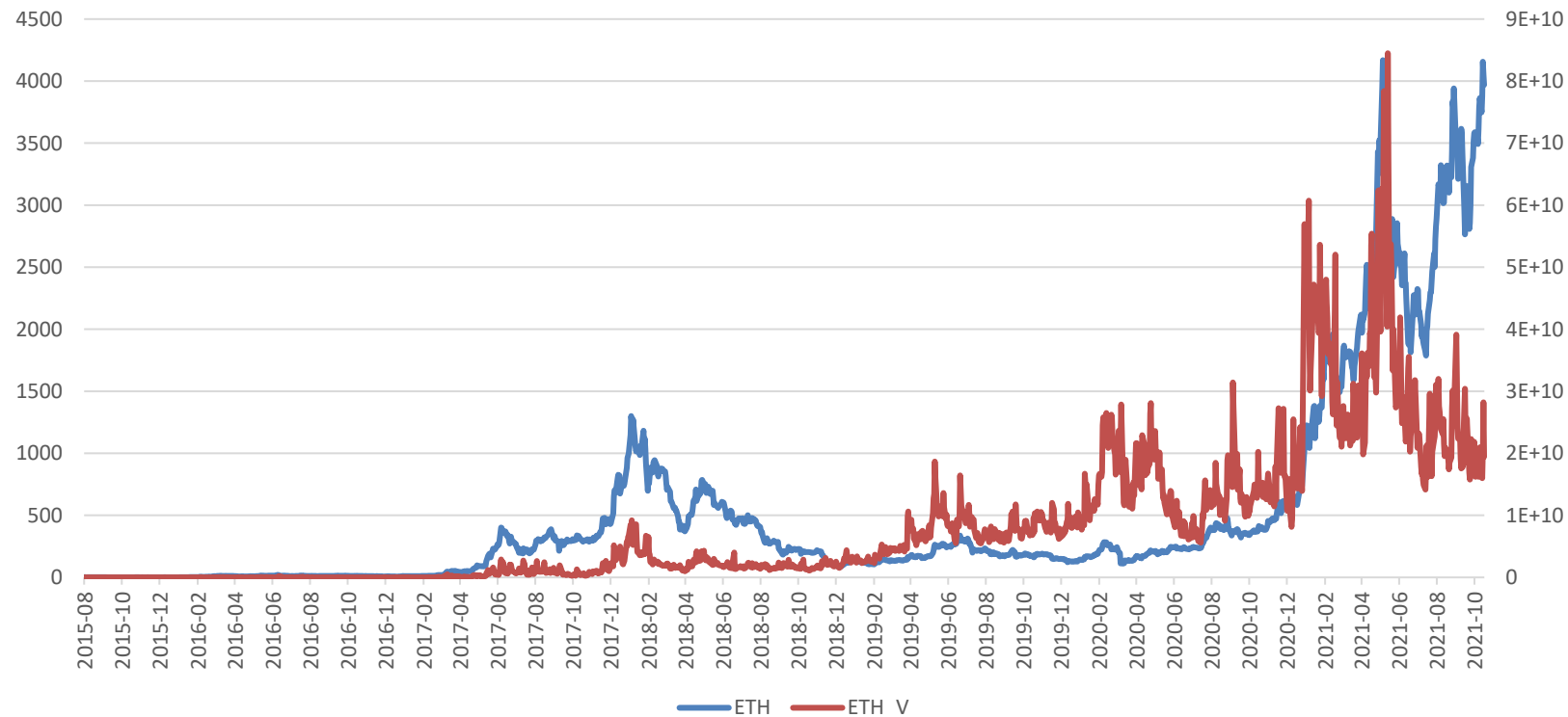
- Proof-of-stake validation: accelerates transaction time and reduces energy usage
- As in Ethereum: enable smart contracts and decentralized applications, driven by ADA (native coin).
- Appeared in September 2017



Source: finance.yahoo.com

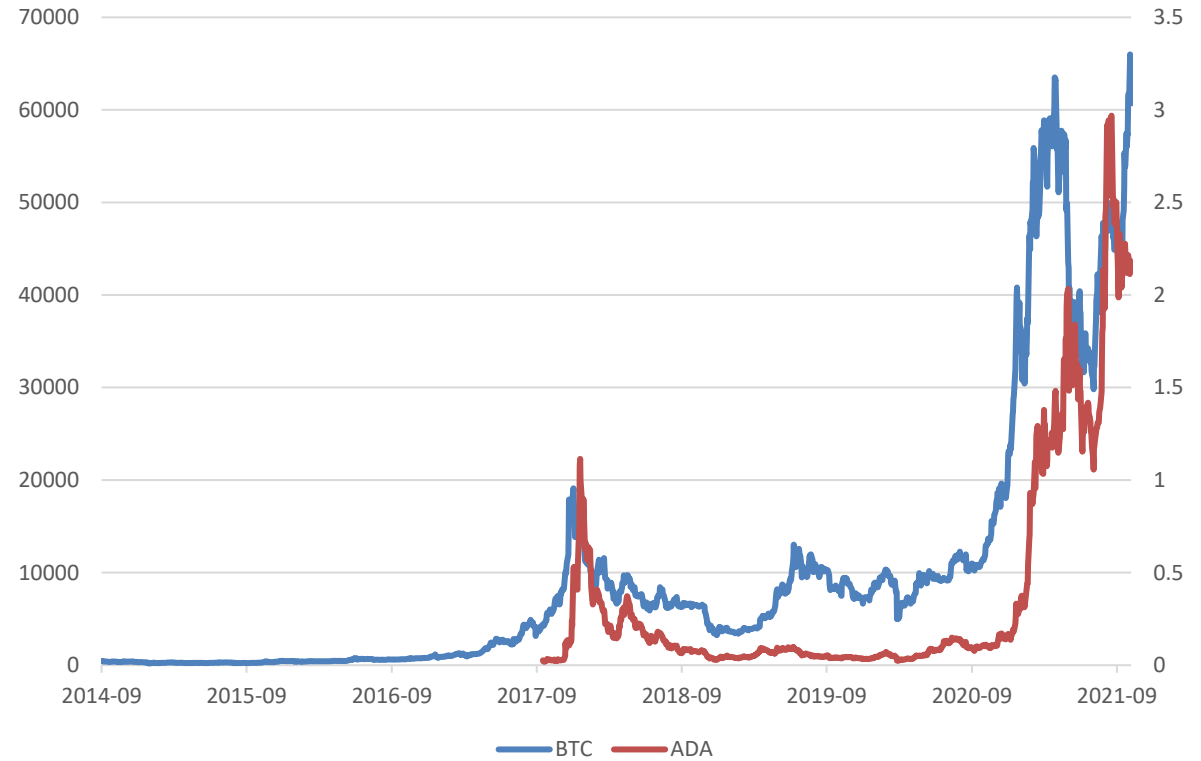
Ethereum closing price in USD (ETH) and trading volume (ETH_V)

- Cryptocurrency and a blockchain platform
- Platform popular for the development of distributed apps (dApps) and smart contracts.
- Moving from proof-of-work to proof-of-stake validation: reduces energy uses



Source: finance.yahoo.com

Comparison between bitcoins (BTC), ADA and Ethereum (ETH)'s closing prices



Source: finance.yahoo.com

Bitcoin prices compared with major Exchanged-Traded Funds (ETFs)

Adjusted daily closing prices for ETFs and BTC:

Core ETFs that represent complete market:

- VTI: Vanguard Total Stock Market ETF
- VXUS: Vanguard Total International Stock ETF
- BND: Vanguard Total Bond Market ETF
- BNDX: Vanguard Total International Bond ETF

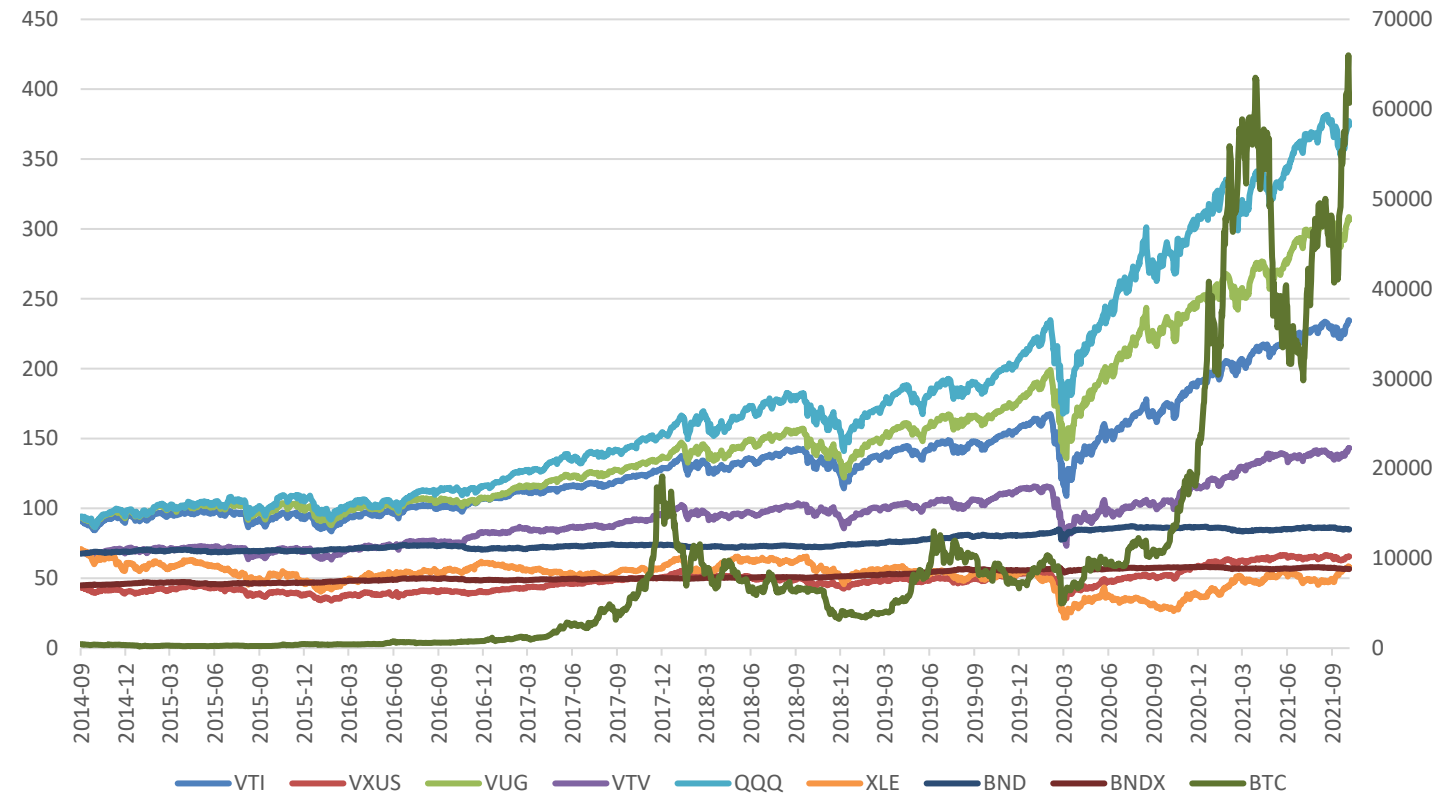
Investment style:

- VUG Vanguard Growth ETF
- VTV Vanguard Value ETF

Sectors: Technology (growth) and energy (value)

- QQQ Invesco Nasdaq
- XLE Energy ETF

- BTC Bitcoin



Source: finance.yahoo.com

Sharpe ratio: risk-adjusted return: excess return/volatility $S_p = \frac{E(r_p) - r_f}{\sigma_p}$

	Basic ETFs				Growth vs Value		Tech & Energy		Cryptocurrencies		
	VTI	VXUS	BND	BNDX	VUG	VTV	QQQ	XLE	BTC	ADA	ETHE
Median return	0.07	0.09	0.02	0.02	0.10	0.07	0.13	-0.01	0.24	0.04	0.11
Average return	0.05	0.02	0.05	0.02	0.01	0.01	0.08	-0.01	0.27	0.43	0.47
Return volatility	1.13	1.12	1.13	1.12	0.29	0.20	1.32	1.97	4.67	9.06	8.30
Sharpe ratio	0.05	0.02	0.05	0.02	0.04	0.07	0.06	-0.01	0.06	0.05	0.06
Until 2019											
Median return	0.05	0.05	0.02	0.02	0.07	0.04	0.10	-0.01	0.21	-0.56	-0.08
Average return	0.04	0.02	0.01	0.02	0.05	0.04	0.06	-0.02	0.21	0.05	0.35
Return volatility	0.85	0.91	0.20	0.18	0.94	0.82	1.08	1.36	4.54	9.98	8.83
Sharpe ratio	0.05	0.02	0.07	0.09	0.05	0.05	0.06	-0.01	0.05	0.00	0.04
2020-21											
Median return	0.17	0.15	0.01	0.02	0.22	0.11	0.24	0.00	0.37	0.69	0.75
Average return	0.09	0.05	0.01	0.00	0.12	0.05	0.13	0.01	0.47	0.92	0.75
Return volatility	1.71	1.58	0.46	0.25	1.81	1.74	1.85	3.12	5.01	7.74	6.80
Sharpe ratio	0.05	0.03	0.02	0.02	0.07	0.03	0.07	0.00	0.09	0.12	0.11

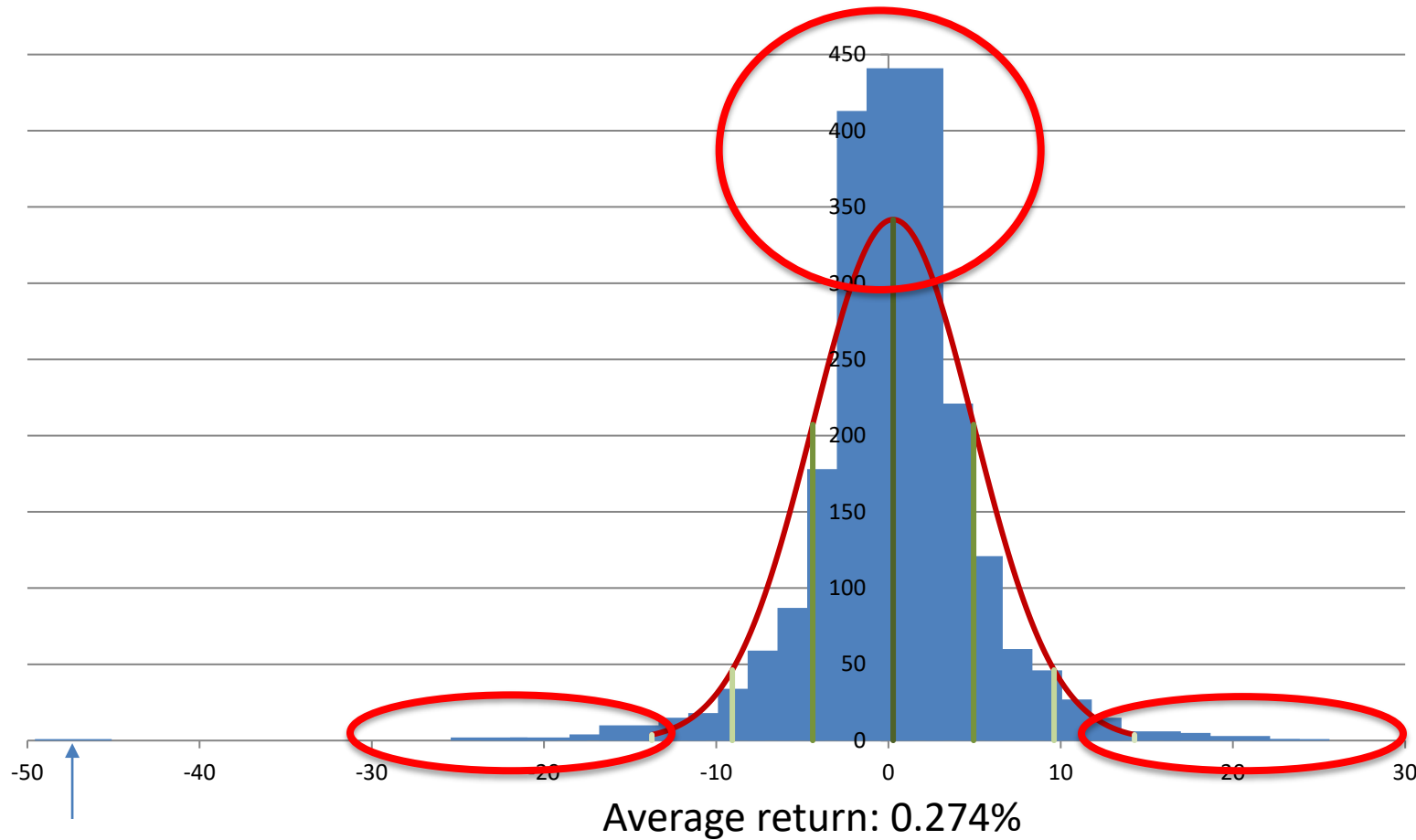
BTC: 2014-09-18 / 2021-10-22

ADA: 2017-10-03 / 2021-10-22

ETH: 2015-08-10 / 2021-10-22

- Sharpe ratio's cryptos very similar to the rest of the market. Only since 2020, they improve significantly.
- BTC's and ETHE's returns are larger than ETFs'. ADA is as profitable as QQQ until 2019, although its Sharpe ratio is about 0. In the last period, it shows the best performance.
- Median < Mean: cryptos' returns skewed to the right (positive)
- Pre-Covid: ADA and ETHE: median is negative and less than average: most days trader lost money. This only happened with the XLE (energy) ETF.
- Cryptos' volatility is much larger (riskier) than ETFs'.
- According to mean variance optimization, invest on portfolio with highest Sharpe ratio. Would you invest in a portfolio with only cryptos? Or only foreign bonds (BNDX) or only technology stocks (QQQ)?

Histogram of bitcoin's daily return compared with a normal distribution



Outlier 03/12/2020: -46.4%

Sept 17, 2014 –Oct. 22, 2021

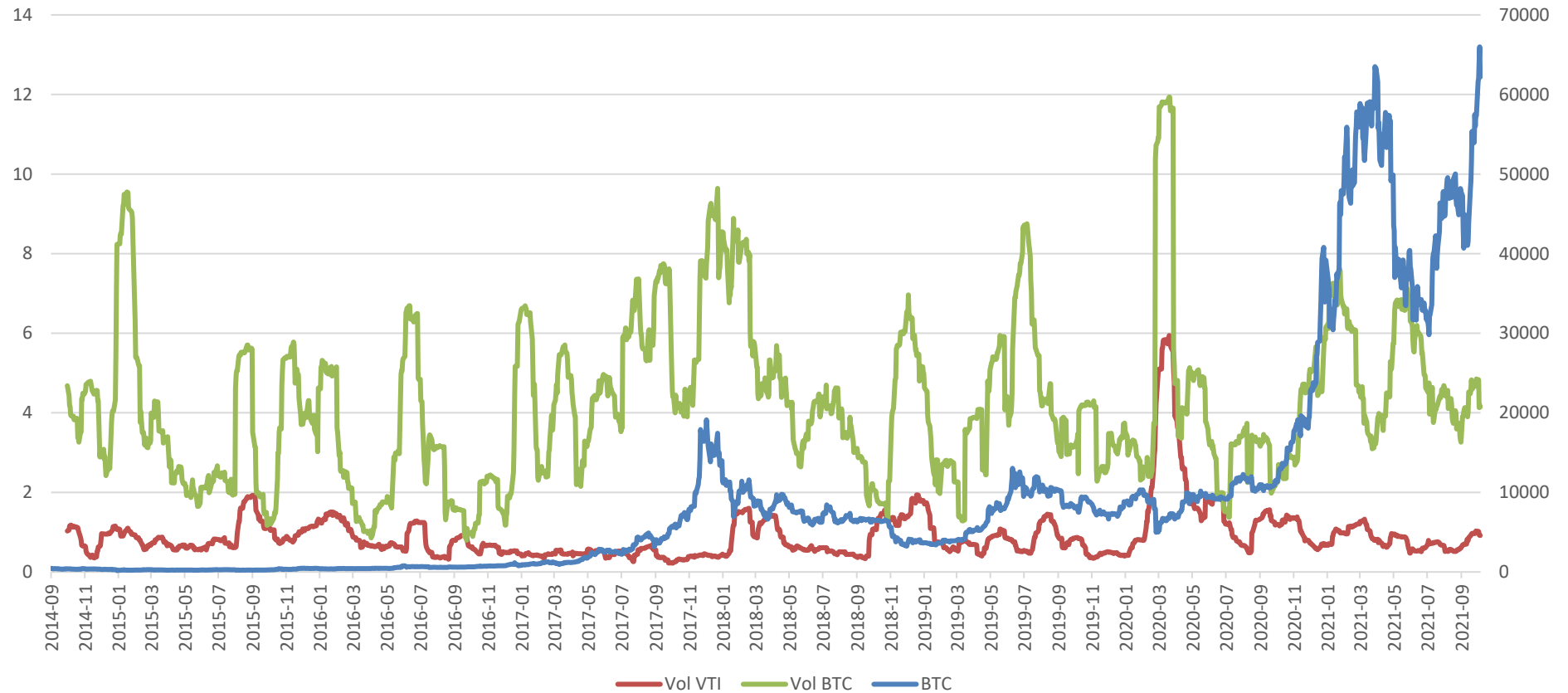
Most returns are more concentrated than in the case of a normal distribution

Large tails -> outliers and high risk: possibility of daily large gains and losses that could not be expected from a normal distribution. Stronger case when return is skewed to the right (positive)

Average return larger than expected in a normal distribution

Bitcoin prices (BTC) and return volatility of VTI (US stock market, Vol VTI), and bitcoin (Vol BTC)

BTC volatility reacts strongly with any market changes in any direction: up or down



Source: finance.yahoo.com

Capital asset pricing model: CAPM

Expected returns on assets are determined by their β s with respect to the market portfolio:

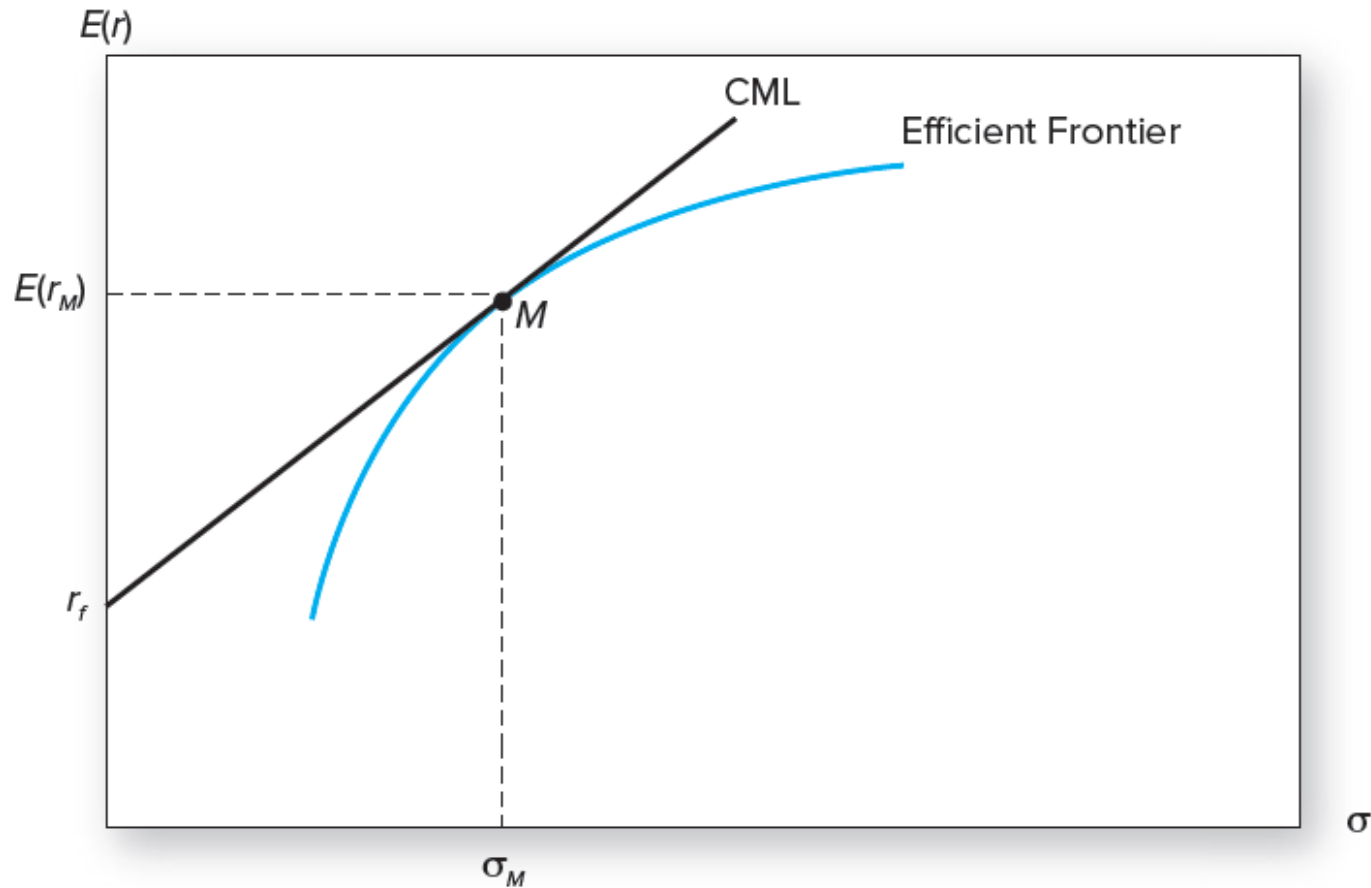
$$E[R_i] = R_f + \beta(E[R_M] - R_f)$$

$\beta = Cov(R_i, R_M) / Var(R_M)$: security risk in relation to market

Market risk premium: $E[R_M] - R_f$

Efficient frontier and the capital market line

B: The Efficient Frontier and the Capital Market Line



Market portfolio is efficient and has the highest Sharpe ratio

Capital market line: Optimal combination of portfolios that combine risk free asset and market portfolio

Recommendations of CAPM for cryptocurrencies

- According to CAPM, investors should weight the securities in their portfolio based on their market- weights.
- CAPM has led to the successful development of indexed funds.
- According to CAPM, investors should not hold or should hold a minimum number of cryptocurrencies:
 - Currencies or cash are useful as a medium of exchange; they do not have underlying value.
- What does the data suggest?

Bitcoin's return correlation with major Exchanged-Traded Funds (ETFs)

	<i>VTI</i>	<i>VXUS</i>	<i>VUG</i>	<i>VTV</i>	<i>QQQ</i>	<i>XLE</i>	<i>BND</i>	<i>BNDX</i>	<i>BTC_C</i>
VTI	1.00								
VXUS	0.88	1.00							
VUG	0.96	0.83	1.00						
VTV	0.96	0.86	0.84	1.00					
QQQ	0.92	0.79	0.98	0.79	1.00				
XLE	0.72	0.71	0.59	0.78	0.52	1.00			
BND	0.04	0.06	0.06	-0.01	0.03	-0.01	1.00		
BNDX	0.05	0.05	0.08	0.01	0.07	-0.01	0.63	1.00	
BTC	0.16	0.16	0.16	0.14	0.15	0.12	0.12	0.08	1.00

Low correlation of BTC with major ETFs that represent the major financial assets in any portfolio

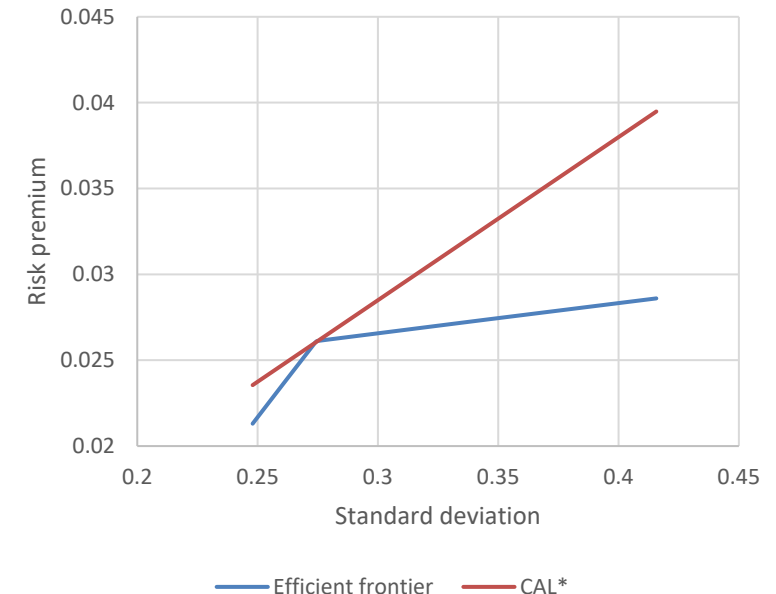
Efficient frontier and portfolio optimization with cryptocurrencies

Panel A	Expected excess return
BTC	0.274
VTI	0.053
VXUS	0.023
VUG	0.067
VTV	0.041
BND	0.013
BNDX	0.013

Panel B		Bordered Covariance Matrix						
Portfolio weights		<div> <div></div> <div>→</div> </div>						
		<div> <div>↓</div> </div>						
		BTC	VTI	VXUS	VUG	VTV	BND	BNDX
0.0294	BTC	21.80	0.84	0.84	0.90	0.74	0.17	0.07
0.0000	VTI	0.84	1.28	1.12	1.32	1.22	0.01	0.01
0.0000	VXUS	0.84	1.12	1.26	1.13	1.08	0.02	0.01
0.1007	VUG	0.90	1.32	1.13	1.49	1.16	0.02	0.02
0.0000	VTV	0.74	1.22	1.08	1.16	1.27	0.00	0.00
0.0000	BND	0.17	0.01	0.02	0.02	0.00	0.08	0.04
0.8699	BNDX	0.07	0.01	0.01	0.02	0.00	0.04	0.04
1.0000		0.02	0.00	0.00	0.02	0.00	0.00	0.03

$$\sigma_p^2 = \sum_{i=1}^n \sum_{j=1}^n w_i w_j \text{Cov}(r_i, r_j)$$

Panel C		Various points along the efficient frontier.					Optimal (tangency) portfolio				
	Minimum variance portfolio										
Risk Premium	0.01	0.02	0.02	0.02	0.03	0.03	0.03	0.03	0.03	0.04	
Std Deviation	0.19	0.20	0.22	0.25	0.27	0.28	0.42	0.45	0.48	0.52	
Sharpe ratio	0.07	0.08	0.08	0.09	0.09	0.09	0.07	0.07	0.07	0.07	
BTC	0.00	0.01	0.02	0.03	0.03	0.03	0.06	0.07	0.08	0.09	
VTI	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	
VXUS	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	
VUG	0.00	0.00	0.00	0.00	0.10	0.10	0.00	0.00	0.00	0.00	
VTV	0.03	0.01	0.01	0.01	0.00	0.00	0.00	0.00	0.00	0.00	
BND	0.06	0.06	0.06	0.06	0.00	0.00	0.94	0.93	0.92	0.91	
BNDX	0.91	0.91	0.91	0.91	0.87	0.87	0.00	0.00	0.00	0.00	



Fama-French Five-Factor Model: extension of CAPM

$$R_{it} = \alpha_i + \beta_{i,M}(R_{Mt} - R_f) + \beta_{i,SMB}SMB_t + \beta_{i,HML}HML_t + \beta_{i,RMW}RMW_t + \beta_{i,CMA}CMA_t + e_{it}$$

Alpha: excess return above expected by market return and other factors

$R_M - R_f$: market return minus risk free rate (market risk premium)

SMB: Small Minus Big (firm size): difference of average return on 9 small and 9 big stock portfolios

HML: High Minus Low (value): difference of average return on 2 value and 2 growth portfolios

RMW (Robust Minus Weak): difference of average return on 2 robust and 2 weak operating profitability portfolios

CMA (Conservative Minus Aggressive): difference of average return on 2 conservative and 2 aggressive investment portfolios

A multi-index CAPM inherits its risk factors from sources that a broad group of investors deem important enough to hedge

Do the cryptocurrencies' return is above the expected return considering the US stock market and other factors (alpha)?

Fama French five factor model on cryptocurrencies

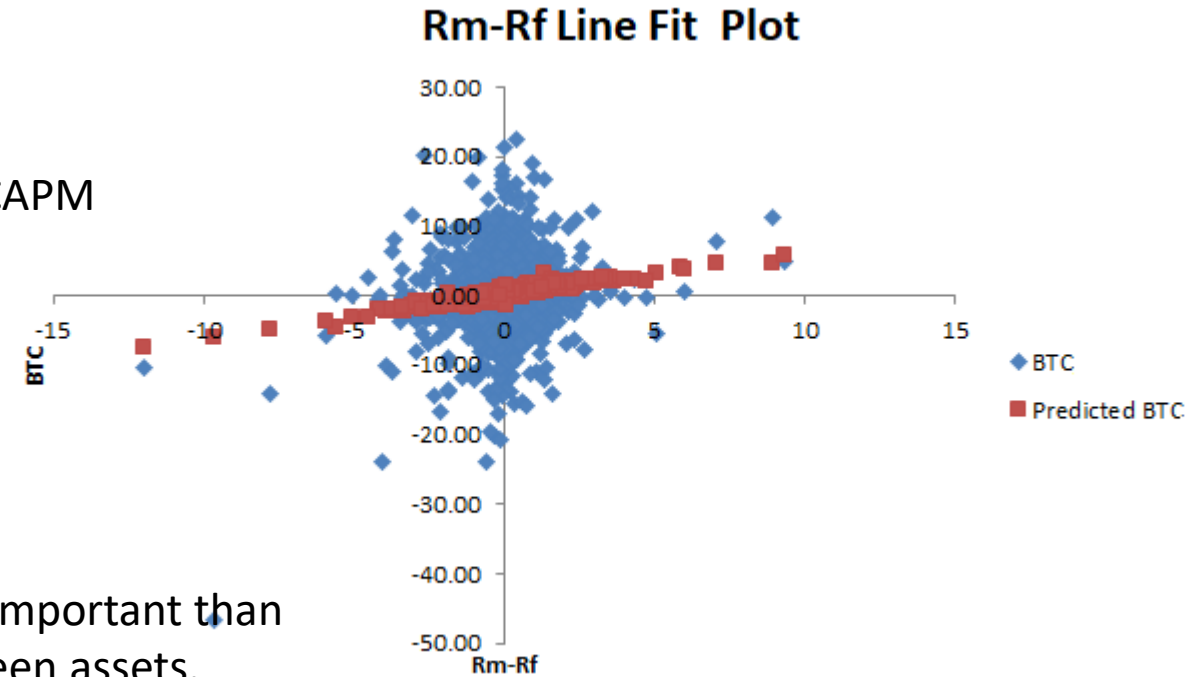
	BTC	ADA	Ethe
Alpha	0.23	0.37	0.40
β (Rm-Rf)	0.61	1.29	0.87

Alpha: excess return above expected by market return or CAPM

BTC: 2014-09-18 / 2021-10-22

ADA: 2017-10-03 / 2021-10-22

ETH: 2015-08-10 / 2021-10-22



Three cryptocurrencies have positive alpha. This might be more important than Sharpe ratio (SR) because SR does not consider covariance between assets.









Even though model follows the stock market trend, it has major daily variations.

β s of BTC and ETHE below 1.

BTC's β is 0.61: it may work as a hedge against the risk of the stock market

Currency Exchange Markets

bitcoincharts.com/markets/

Overview		Currencies		All Markets																			
All	KRW	NMC	IDR	RON	MYR	NGN	VND	GAU	PKR	VEF	ARS	AUD	BGN	BRL	BTC	CLP	CNY						
CZK	DKK	EUR	GBP	HKD	HUF	ILS	INR	JPY	LTC	MXN	NOK	NZD	PEN	PLN	RUB	SAR	SEK						
SGD	SLL	THB	UAH	USD	XRP	ZAR	CHF	CAD	VES														
Symbol		Latest Price		30 days	Average		Volume		Low/High		Bid		Ask		24h Avg.		Volume		Low/High				
▲	Kraken	52749.9		48888.71	85,501.04	34924.1	52736.9	52737	51912.00	4,010.61	49688.2	EUR	krakenEUR	0 min ago	3861.19 7.90%	4,180,035,964.27 EUR	67016.5	61520.06	61528.1	60355.66	4,205.96	56425	62524
▲	BitStamp	61640.02		56929.14	77,240.86	40750	61520.06	61528.1	60355.66	4,205.96	56425	USD	bitstampUSD	0 min ago	4710.88 8.28%	4,397,255,447.77 USD	67016.5	61520.06	61528.1	60355.66	4,205.96	56425	62524
▲	BitBay	242730.8		221788.49	7,814.23	162300.01	243137.1	244174.08	240801.08	308.15	231000	PLN	bitbayPLN	1 min ago	20942.31 9.44%	1,733,105,954.13 PLN	259355	243137.1	244174.08	240801.08	308.15	231000	246591.57
	Mercado Bitcoin	330158.00084		317409.84	3,867.33	223465.3	330158.00053	330750.99827	—	0.00	—	BRL	mrcdBRL	1 day, 5 hrs ago	12748.16 4.02%	1,227,529,348.02 BRL	370000	330158.00053	330750.99827	—	0.00	—	—
▲	CEX.IO	61576.6		56174.94	3,705.75	40825	61549.8	61570.9	60385.25	180.23	58100	USD	cexUSD	0 min ago	5401.66 9.62%	208,170,274.56 USD	66984	61549.8	61570.9	60385.25	180.23	58100	62388.9
▲	btcmarkets	81889.2		77064.73	3,613.22	56500	81689.01	81855.73	80232.02	153.93	77211.36	AUD	btcmarketsAUD	0 min ago	4824.47 6.26%	278,451,567.42 AUD	89193.41	81689.01	81855.73	80232.02	153.93	77211.36	83145.74
▲	BitBay	52622.24		47078.66	2,742.63	28000.01	52361.67	52991.65	52349.45	68.00	49623.01	EUR	bitbayEUR	7 min ago	5543.58 11.78%	129,119,356.59 EUR	57268.49	52361.67	52991.65	52349.45	68.00	49623.01	53200
▲	Zaif	7004995		6450952.11	2,060.98	4551320	6999985	7000000	6873731.01	72.26	6600000	JPY	zaifJPY	0 min ago	554042.89 8.59%	13,295,311,661.59 JPY	7630000	6999985	7000000	6873731.01	72.26	6600000	7043500

<http://bitcoincharts.com/markets>

[Buy bitcoins](#)[Sell bitcoins](#)[Post a trade](#)[Learn ▾](#)[Wallet](#)**QUICK BUY****QUICK SELL**

USD ▾

United States ▾

All online offers ▾

Search

Results for buying bitcoins online

Trader	Payment method	Price / BTC	Limits	
Julie_4426 (2; 100%) ●	Paypal	56,000.00 USD	50 - 52 USD	Buy
Mata_TD (1; 100%) ●	Other online payment: ❤️ WESTERN UNION 🚫 WHATSAPP ME +260979744359 🚫	60,826.10 USD	7 - 8 USD	Buy
dabaobaoa (2; 100%) ●	GreenDot Card	61,452.90 USD	100 - 419 USD	Buy
liqin0619 (38; 100%) ●	International Wire (SWIFT): SCBLSG22	61,452.90 USD	10,000 - 30,726 USD	Buy
Fxcrypto1 (13; 100%) ●	National bank transfer: United States	61,523.91 USD	7 - 7 USD	Buy
andimillan96 (250+; 98%) ●	Transfers with specific bank: Zelle	61,900.00 USD	350 - 351 USD	Buy

Bitcoin Exchanges

Market matches buyer and seller:

- Accept deposits of Bitcoins and fiat currency (\$, €, ...)

- Promise to pay back on demand

Let customers:

- Make and receive Bitcoin payments

- Buy/sell Bitcoins for fiat currency

Large, liquid market reaches a consensus price

Price set by supply (of BTC) and demand (for BTC)

What happens when you buy BTC

Suppose my account at Exchange holds \$5000 + 3 BTC and I use Exchange to buy 2 BTC for \$580 each

Result: my account holds \$3840 + 5 BTC

Note: no BTC transaction appears on the blockchain

Only effect: Exchange is making a different promise now

Supply of Bitcoins

Supply = coins in circulation (+ demand deposits?)

Coins in circulation: fixed number, currently ~18.85 million (10/21)

When to include demand deposits?

When they can actually be sold in the market.

Demand for Bitcoins

BTC demanded to mediate fiat-currency transactions

Alice buys BTC for \$

Alice sends BTC to Bob

Bob sells BTC for \$

} BTC “out of circulation” during
this time

BTC demanded as an investment

If the market thinks demand will go up in future

Exchanges: Pros and Cons

Pros:

1. Connects BTC economy to fiat currency economy
2. Easy to transfer value back and forth

Cons:

1. Risk - same kinds of risks as banks

Financial Sector

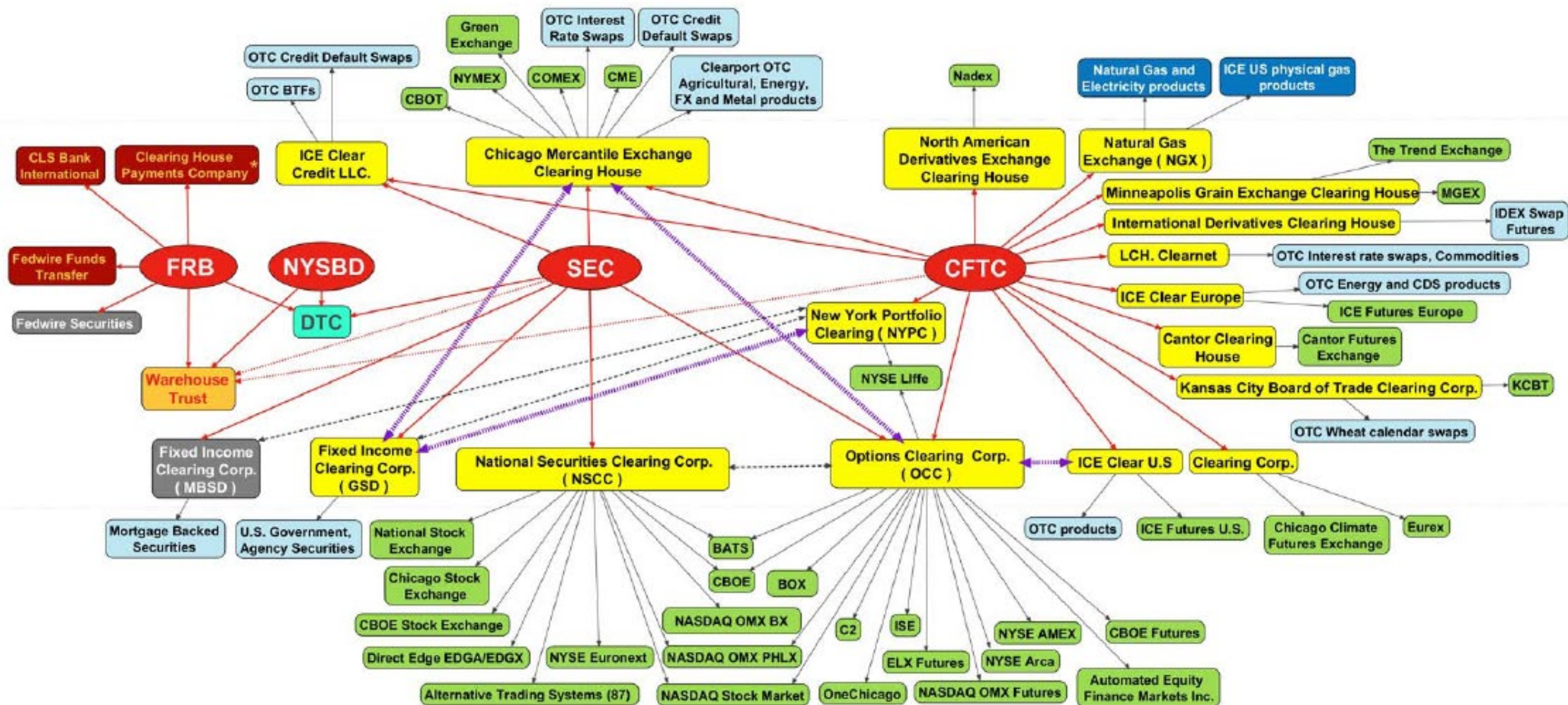
- Facilitate funds and assets' transfers
- Based on trust and system of ledgers
- Grows with technology, mostly IT

Major challenges:

- Legacy of costly & numerous softwares and platforms
 - Risk management:
 - Centralized and concentrated in certain products or clients
 - Counterparty risk
 - Systemic risk: financial crisis
 - Economic rent more difficult to justify
-
- 7 ½ % of U.S. GDP: Financial sector costs
 - ½ - 1 % of Global GDP: Payment system costs

Can cryptocurrencies or blockchain technology address any of the above issues?

U.S. Regulatory Authority over Payment, Clearing and Settlement Systems



Current* as of April 09, 2012
 Source: Federal Reserve Bank of Chicago
 Financial Markets Group
 * Derived from publicly available information

Financial Sector: blockchain projects

- Australia – ASX CHESS project with Digital Asset system (2016 – 21)
 - Estonia – Tallinn Stock Exchange Exploring Proxy Voting & Registration (2018)
 - India – SEBI, Blockchain Technology exploration announced (1/2018)
 - Japan – Japan Exchange Group – Post Trade Matching Test (2017-18)
 - US – NADAQ Linq private securities platform (2015) & Mutual Fund project (2018)
-
- Australia, Estonia, India, Japan, US

Central banks research on Central Bank Digital Currency (CBDC)

Similar to paper money:

Digital Base Money: claim on central bank

Different from paper money:

Digital Base Money: digitalized debts of central bank

Other initiatives:

- **El Salvador: BTC official legal tender**
- Dubai (emCash)
- Iran (Indigenous Cryptocurrency)
- Senegal (eCFA)
- Tunisia (e-Dinar)
- Uruguay (Digital Uruguayan Peso)

Did not advance for political reasons:

- Ecuador (Dinero Electrónico)
- Venezuela (Petro)

Many other blockchain projects: Australia, Estonia, India, Japan, US

Central banks of major economies devoted to research on digital currency

China	E-RMB
Bank of England	<ul style="list-style-type: none">• Core studies in 2015. Focus on impact of CBDC on macro economy. Released The Macroeconomics of Central Bank Issued Digital Currencies in 2016.• Research on DLT to support technical aspects of CBDC.
Bank of England	<ul style="list-style-type: none">• Add CBDC to research agenda.• Initiated Project Jasper in mid-2016.• Experimented to apply DLT in high value payment system.
Bank of Canada	<ul style="list-style-type: none">• Announced a two-year project in Nov 2016.• Will decide on whether to issue CBDC by end-2018.• Current studies on technical, policy and regulatory aspects.
Riksbank (Sweden)	<ul style="list-style-type: none">• Studied on design and technical issues of CBDC since Jan 2017.• Joint Project Stella with BOJ since Dec 2016 to test DLT application in financial infrastructure.
ECB	<ul style="list-style-type: none">• Current research on CBDC stays at technical level. Vice Governor of BOJ said to learn more about new technologies including DLT in Nov 2016.• Joint Project Stella with ECB since Dec 2016.
Bank of Japan	<ul style="list-style-type: none">• Joint Project Ubin with R3 since Nov 2016 to study on using CBDC in payment and settlement on a distributed ledger.• In 2nd phase of Project Ubin, MAS cooperated with Accenture in 2017 to explore whether DLT can realize certain RTGS functionalities.
Monetary Authority of Singapore	

China: e-RMB

- In April 2020, China's central bank introduced “digital yuan” across four cities: world's first major economy to issue a national digital currency.
- Digital currency:
 - Most convenient tool to translate a central bank's zero and negative interest rate policy into commercial banks.
 - Will be pegged to the national currency
 - Decline in cash usage is expected to continue → people avoid physical contact
- Digital yuan (e-RMB) may replace cash in circulation, likely interfacing with popular payments platforms such as AliPay and WeChat Pay and the existing banking system.
 - Alibaba's Alipay and Tencent's WeChat Pay: 1.7+ billion active Chinese accounts
 - Alipay publicized five [patents](#) related to China's official digital currency between January 21 to March 17, 2020.
- China's plan to implement e-RMB among countries:
 - Involved in its Belt and Road initiative (new Silk road).
 - Participating in its development programs.

China electronic currency: Major player in international finance

China's digital currency poses no more of a threat to the US-based financial system than the RMB itself: if RMB will displace the USD, it will have little to do with the form of China's currency but rather with its economic and political choices.

1) A digital version of the RMB (renminbi) lets China interoperate between different currency contexts where the USD may start to fade.

2) China is in a technological battle to define standards with emerging technologies: 5G

3) Using digitization and decentralization to a nominal degree helps blunt China's international weakness — perception around its totalitarian domestic system: digital currency that is more acceptable to local populations than a raw form version of the Chinese RMB

Digitization of currency is inevitable: — cryptocurrency prevails: determine whether that will be at the hands of nation-states battling with one another, or a set of independent peers cooperating with one another

Conclusions – Blockchain & Bitcoin

- Blockchain technology: new paradigm of peer-to-peer system without a central authority
- Solves problems of verification, double spending, merchant acceptance, decentralization, and networking costs (i.e. trading network) that led to failure of previous crypto experiments.

Valuation and investment:

- Bitcoin is a currency that does not have value by itself; however, it has value as a medium of exchange, store of value, and channel for online (offline) transactions.
- Value in a diversified portfolio because of low correlation with other assets: hedge and/or risky alternative investment.

Investment and trading with cryptocurrencies: Summary

- Cryptos show a positive alpha, so they can improve the return of a market portfolio.
- Sharpe ratio's cryptos very similar to the rest of the market. Only since 2020, they improve significantly. How long will this last?
- High cryptos' return observed since 2020 is associated with high volatility. So, even though there are many profit opportunities, ADA and ETHE have lost value more than half of the days at least until 2020.
- As BTC's return is skewed to the right (positive), there are days of extraordinary returns while many days returns are very low or negative.
- Cryptos' return do not follow a normal distribution and they also have a lower correlation with the rest of financial assets. So, even though they might be very risky for short term trading, they can be a hedge for other risky assets or bad economic periods.

Investment and trading with cryptocurrencies: Summary

- Portfolio allocation decisions depend on the level of risk aversion of the investor and the efficient frontier: if the objective is to minimize risk (minimum variance portfolio), it is not recommended to include BTCs in the portfolio.
- Using the most typical group of ETFs, a tangent portfolio may suggest about 3% of BTCs. This is consistent with the suggestion of financial advisors. A larger weight, may increase significantly the volatility of the portfolio.
- Every trader or investor should start with a very small amount invested on cryptos. As they become more familiar increase their weights until a pre-established limit (<3-5%).
- Cryptocurrency and markets depend on technological innovation. As the economy improves and cryptocurrency is accepted as a medium of exchange, then its demand and price may increase.

Conclusions – Blockchain & Bitcoin

Financial technology:

- Major challenge for payment systems as credit cards who are developing their own digital solutions.
- Opportunities to address major challenges of financial sector: Legacy of IT systems, risk management and financial intermediation role
- System architecture:
 - Permissionless: open for anyone to participate
 - Permissioned: limited only to designated participants: alternative for incumbents that want to control a product (i.e. financial sector applications)

Observations:

- Cryptocurrencies and derived products are exposed to market manipulation or fraud because of very limited regulations.
- Implementation of a blockchain/crypto solution must be addressed not only from a technical perspective; should include clear policies of operation with a commercial and financial perspective
- Great opportunities for change