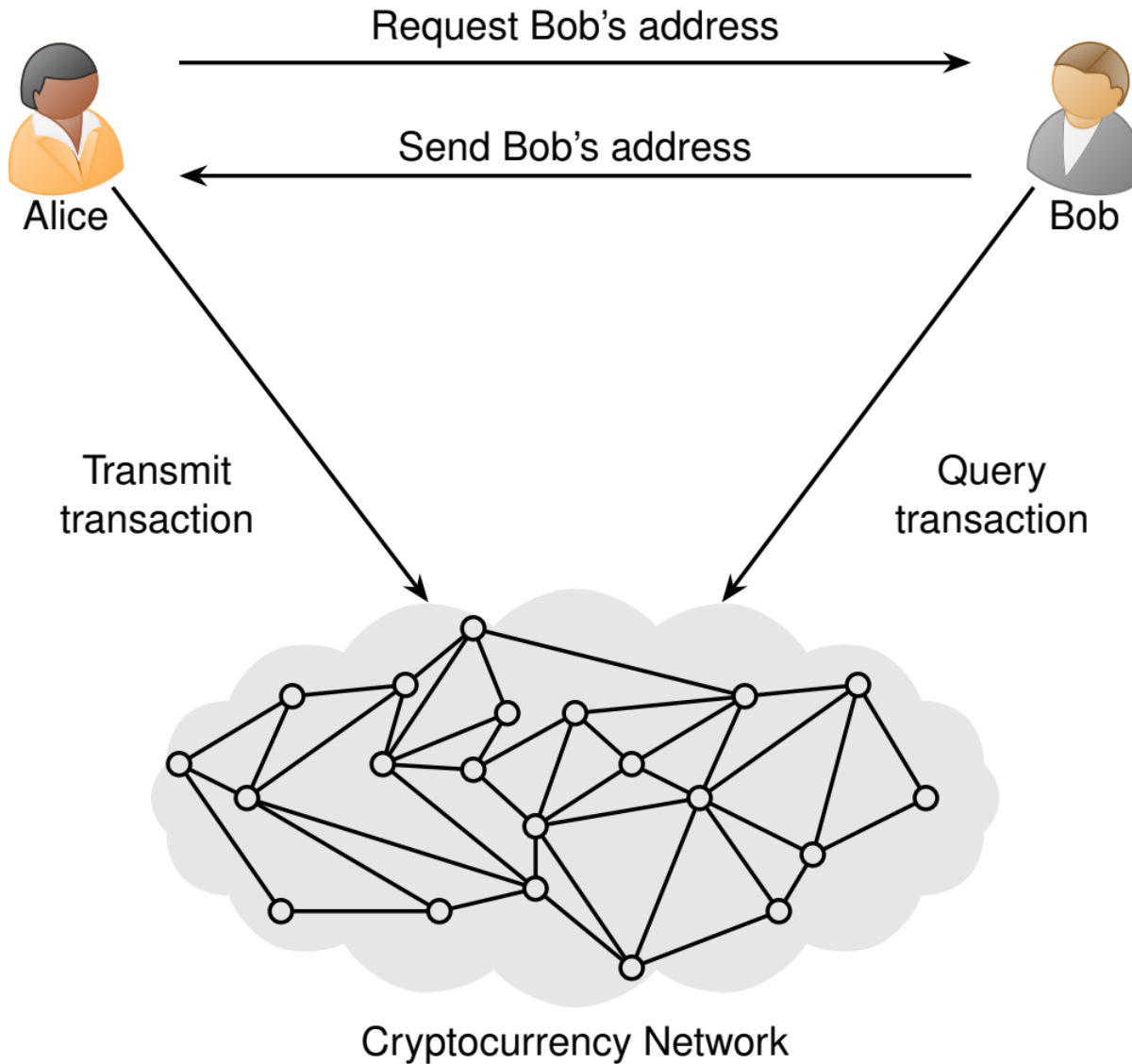


Bitcoin and other crypto currencies

Dhiren Patel

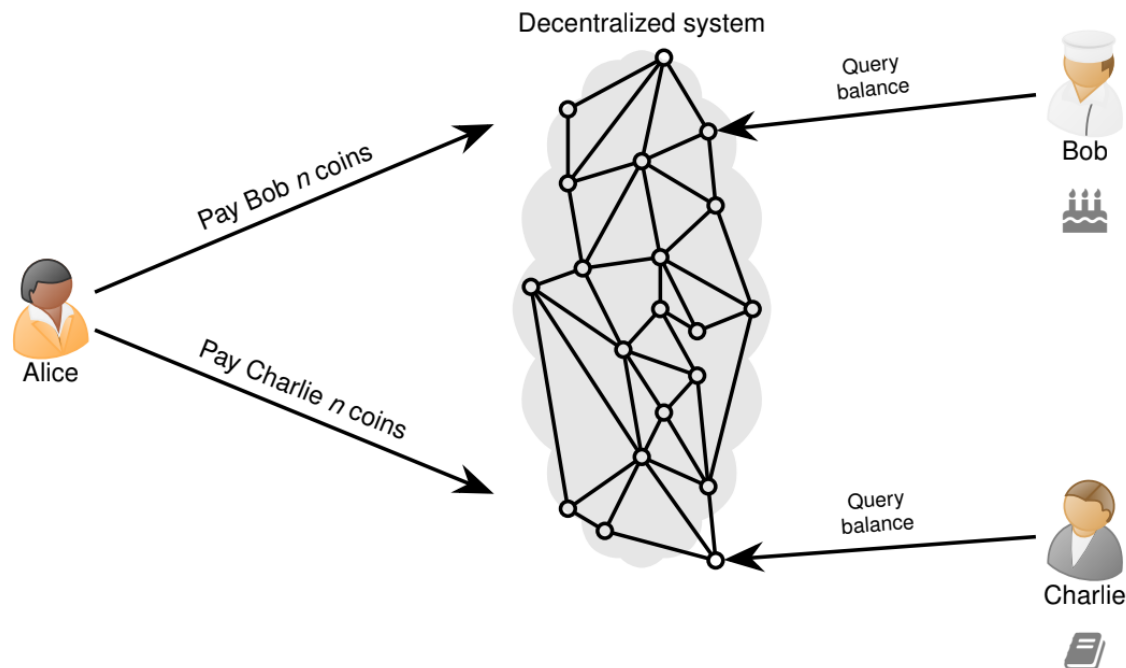
20 Feb, 27 Feb 2023

Transaction workflow

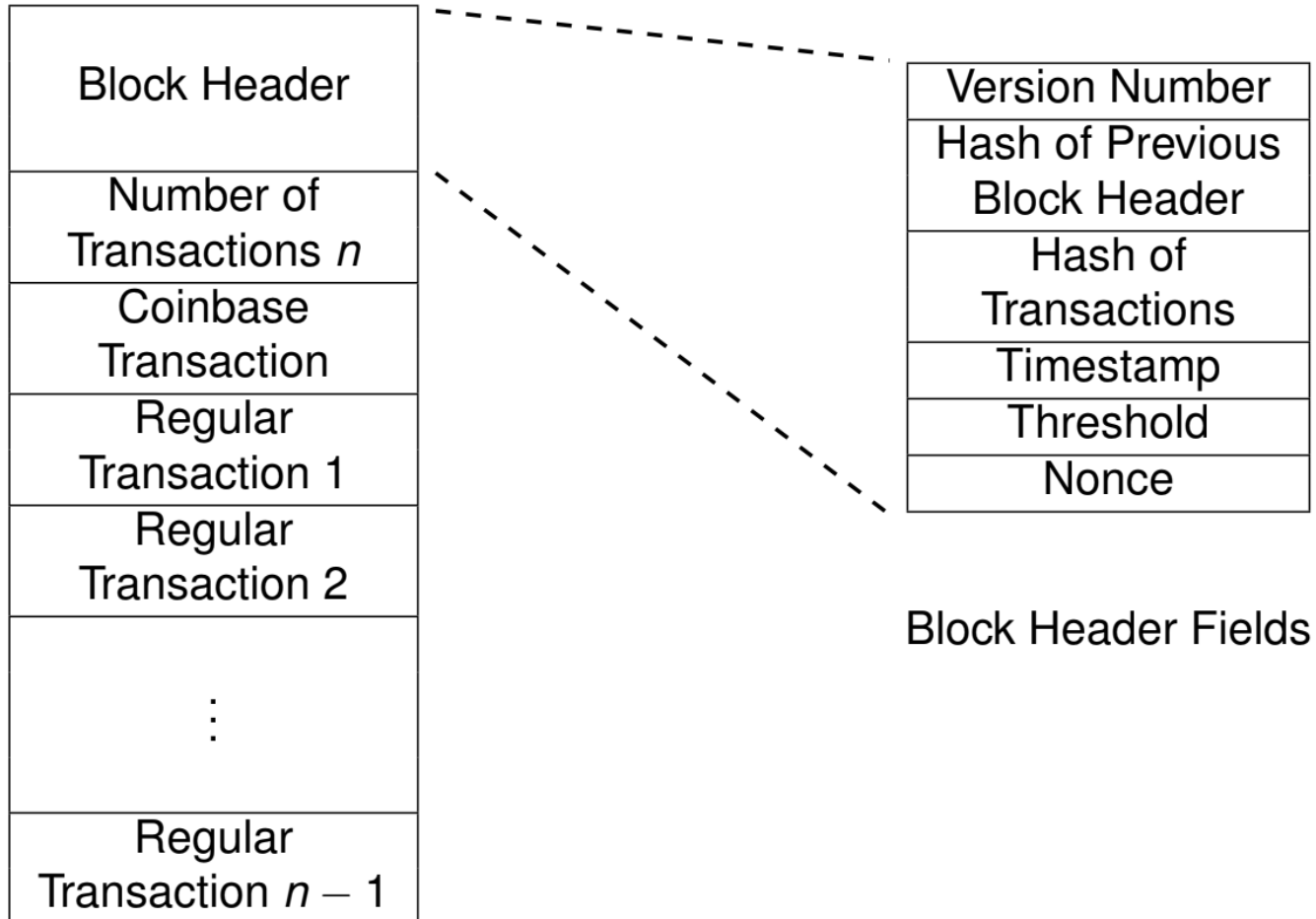


Challenges

- Counterfeiting
- Currency creation rules
- Double spending - Alice pays Bob n coins for a cake; Alice uses the same n coins to pay Charlie for a book



Bitcoin – Block and Header



Header

nVersion	4 bytes
hashPrevBlock	32 bytes
hashMerkleRoot	32 bytes
nTime	4 bytes
nBits	4 bytes
nNonce	4 bytes

Previous Block Header

nVersion
hashPrevBlock
hashMerkleRoot
nTime
nBits
nNonce

Double
SHA-256

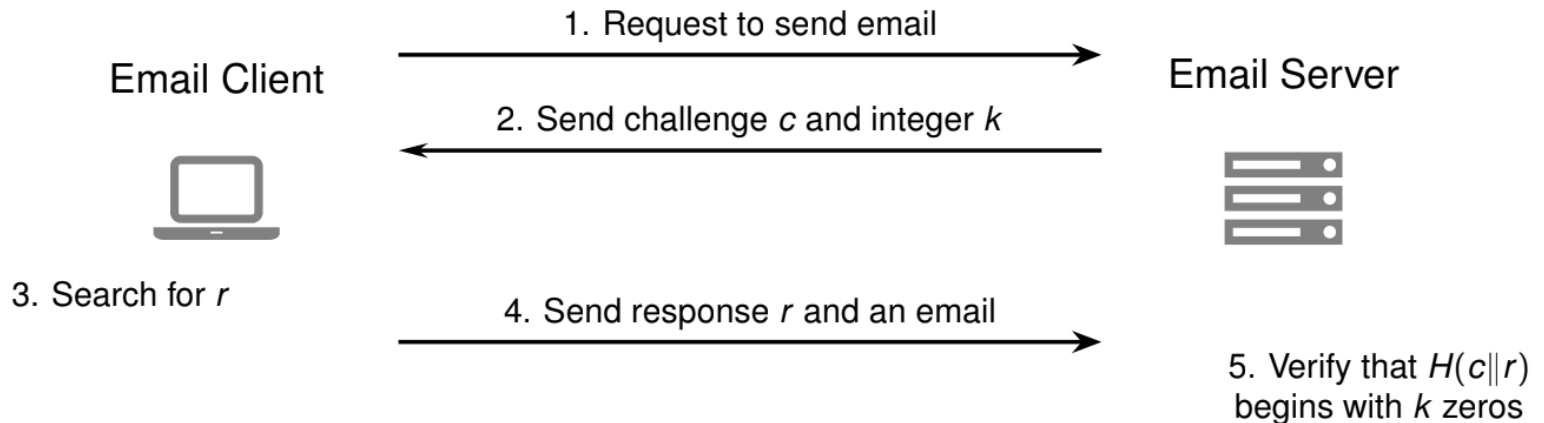


Current Block Header

nVersion
hashPrevBlock
hashMerkleRoot
nTime
nBits
nNonce

Hashcash (90's protocol)

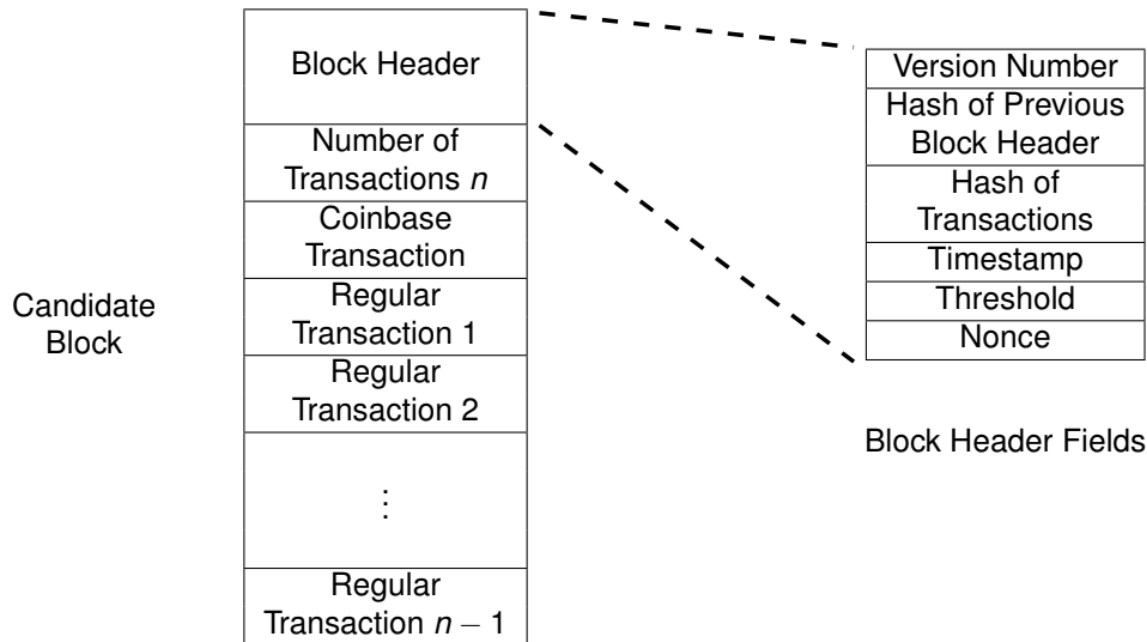
- A database you own where anyone in the world can add entries?
Your email inbox
- Hashcash was proposed in 1997 to prevent spam
- Protocol
 - Suppose an email client wants to send email to an email server
 - Client and server agree upon a cryptographic hash function H
 - Email server sends the client a challenge string c
 - Client needs to find a string r such that $H(c||r)$ begins with k zeros



- The r is considered **proof-of-work (PoW)**; difficult to generate but easy to verify

Mining

- Mining = Process of adding new blocks to the blockchain
- Nodes which want to perform transactions broadcast them
- Miners collect some of these transactions into a candidate block



- Threshold encodes a 256-bit value like $0x \underbrace{00 \dots 00}_{16 \text{ times}} \underbrace{\text{FFFF} \dots \text{FFFF}}_{48 \text{ times}}$
- Miner who can find Nonce such that

$$\text{SHA256}(\underbrace{\text{SHA256}(\text{Version Number} \parallel \dots \parallel \text{Nonce}))}_{\text{Candidate Block Header}}) \leq \text{Threshold}.$$

Mining

- Successful miner gets reward in bitcoins
- Miners also collect the transaction fees in the block
- Each miner specifies his own address as the destination of the new coins
- Every miner is competing to solve their own PoW puzzle
- Mining Farms are located in places with cheap power and cooling

How Block is added?

- Nodes broadcast transactions (mempool)
- Miners accept valid transactions and reject invalid ones (solves double spending)
- Miners try extending the latest block
- Miners compete to solve the search puzzle and broadcast solutions
- Unsuccessful miners abandon their current candidate blocks and start work on new ones
- What if two miners solve the puzzle at the same time?

PoW consensus

- Nodes will accept the first solution they hear and reject others
- Nodes always switch to the chain which was more difficult to produce
- Eventually the network will converge and achieve consensus
- This is called proof-of-work (PoW) consensus

Summary

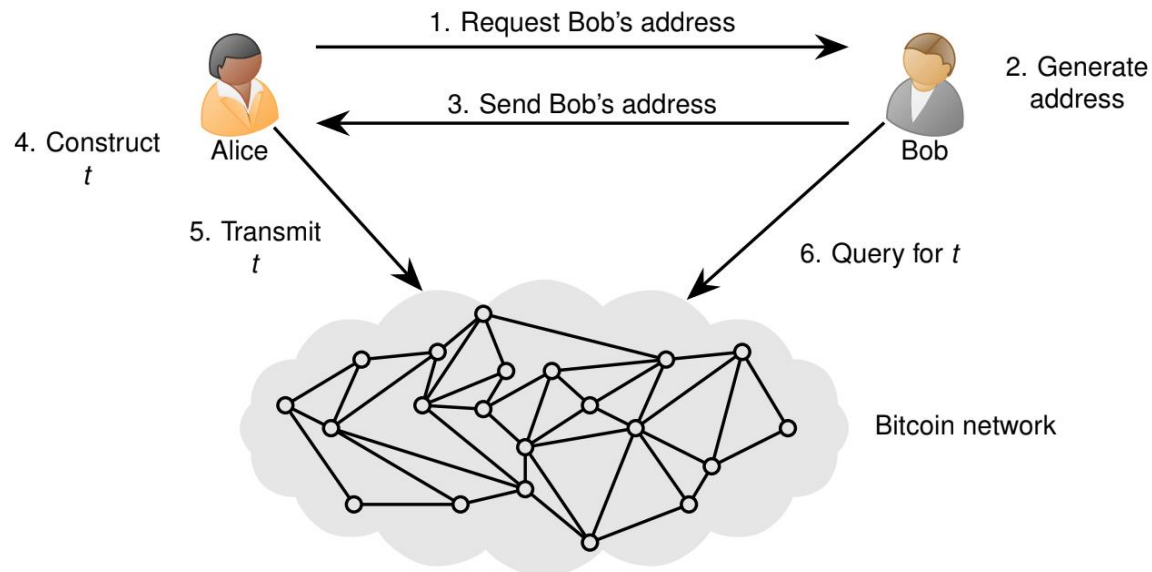
- Bitcoin's blockchain prevents double spending and tampering
- Secure only if nobody controls 50% or more of network hashrate
- Mining difficulty adjusted to regulate coin supply
- Miners incentivized by block reward
- Block subsidy halves every four years to cap total coin supply

Bitcoin Blockchain Explorers

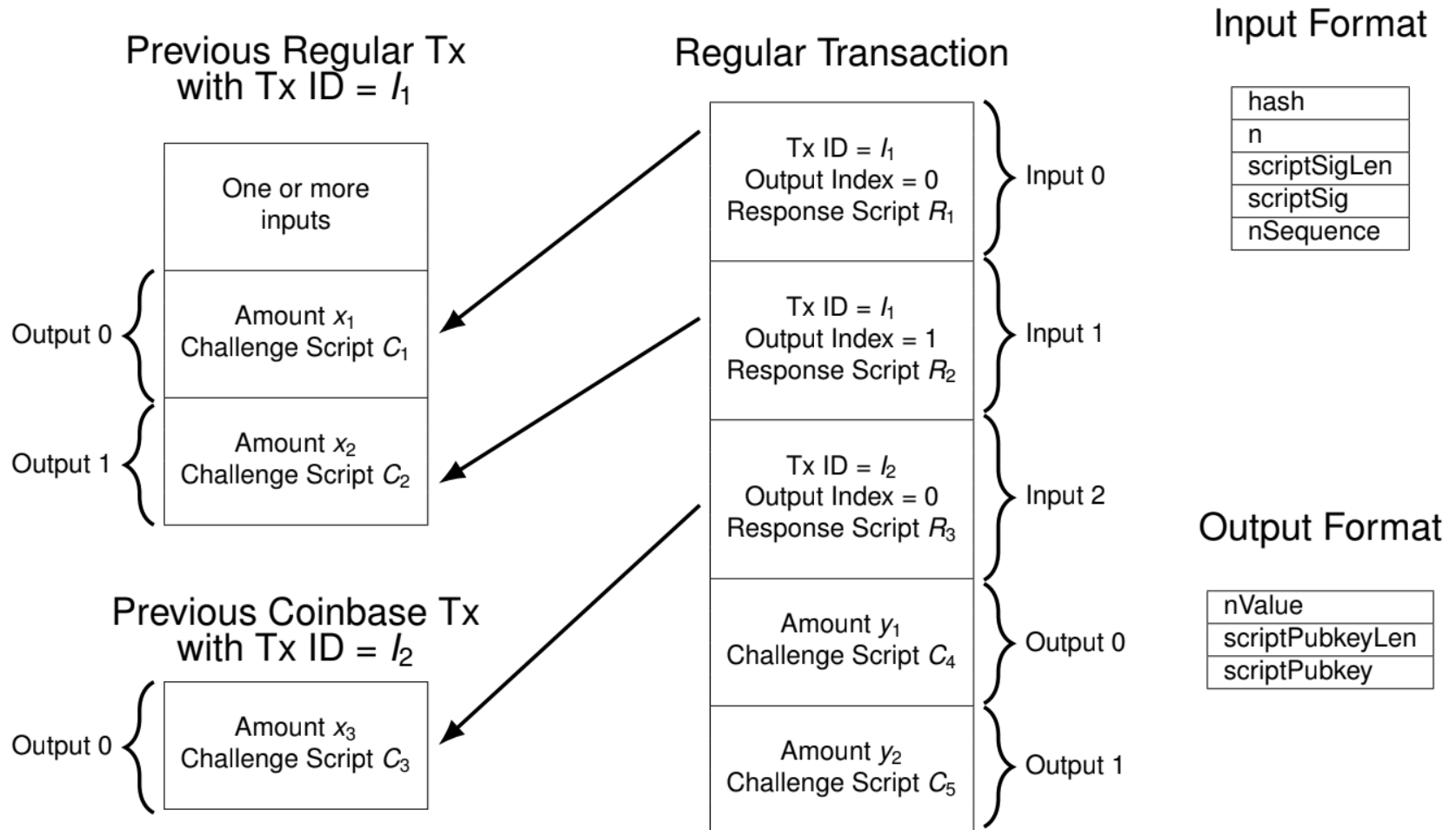
- Web interfaces to view current blockchain state
- <https://www.blockstream.info>
- <https://www.blockchain.com/explorer>
- Demo checklist
- List of transactions (coinbase, regular)
- Address generation in <https://www.bitaddress.org>
- Brainwallet generation at <https://brainwalletx.github.io>
- Bitcoin Testnet
- <https://live.blockcypher.com/btc-testnet/>

Bitcoin Payment Workflow

- Merchant Bob shares address, Customer Alice broadcasts transaction t which pays the address
- Miners collect broadcasted transactions into a candidate block
- One of the candidate blocks containing t is mined
- Merchant waits for confirmations on t before providing goods



Regular Transaction Format



Coinbase Tx format

Block Format

Block Header
Number of Transactions n
Coinbase Transaction
Regular Transaction 1
Regular Transaction 2
\vdots
Regular Transaction $n - 1$

Coinbase Transaction

Amount x_1 Challenge Script C_1	}	Output 0
Amount x_2 Challenge Script C_2		
	}	Output 1

Output Format

nValue
scriptPubkeyLen
scriptPubkey

Test and Assignment Test

- Blockchain Explorers
- BTC, ETH and others – Refer classroom website

Crypto Whales



Whales and Mega Whales

- **Bitcoin wallets holding over 1,000 BTC peaked in February 2021 (about 2,500)**
- There were 2,027 whales on Sunday, February 19, 2023
- mega whales, those holding more than 10,000 BTC, representing an investment of over \$250 million at current prices
- There are just 117 mega whales, fairly close to the historical highs of 123 in November 2022, and 126 in October 2018

Whales

- The number of wallets holding more than one BTC currently sits at 982,000, a solid rise from around 814,000 around this time last year, and 788,000 in February 2020.
- Bitcoin's price has risen from \$16,542 on January 1 to around \$24,900 (20 Feb 2023), an increase of over 40%

Speculation - Risk

- the speculative nature of digital currencies makes them a form of gambling
- The internet bubble was a speculative stock market bubble in which many internet-based companies experienced rapid growth in their stock prices, often without generating substantial profits or revenues. The bubble was fueled by hype and speculation, as investors poured money into companies with little regard for their underlying business models or financial fundamentals.
- Many dot-com companies relied on venture capital funding and initial public offerings (IPOs) to raise money, but many of these companies had no clear path to profitability. This speculative investment frenzy eventually came to an end in 2000. As the bubble burst, the stock market experienced a sharp decline, wiping out billions of dollars of investor wealth.

Issue?

- digital currencies may find a useful application in remittances if immediately converted into fiat currencies
- Web 3.0, as a way to give users control of their own data, including how it's accessed and stored.
- blockchain protocols are “too slow, too expensive and too public” whereas “personal data stores have to be fast, cheap and private.”

NFT

- NFTs are blockchain-based crypto tokens that prove ownership of a digital or physical asset.
- “the latest playful creations in this realm and the most appropriate means of ownership that exists.”

Nearly \$370 Billion in Bitcoin Has Gone 'Dormant'—Why? (22 Feb 2023)

- Bitcoin is largely not moving again, with the amount of dormant coins nearly at a new all-time high.
- Investors are keeping their coins still, with the amount of Bitcoin not budging nearing a new all-time high?
- According to blockchain analysis firm Glassnode, the number of Bitcoins that have not moved for at least six months—dubbed “old supply”—stands at 14.99 million, worth roughly \$370 billion at today’s prices.

Store of Value

- The Bitcoin community has clearly become more long-term oriented, focusing primarily on holding
- Other chains such as Ethereum have communities building tools and services where coins move significantly more, mostly in pursuit of profits
- Most Bitcoin buyers, entered the market during bull runs when the price was high, and these investors have largely sold for losses.
- “potentially signaling a perception that the market is oversold”—meaning it may be poised for a rebound.

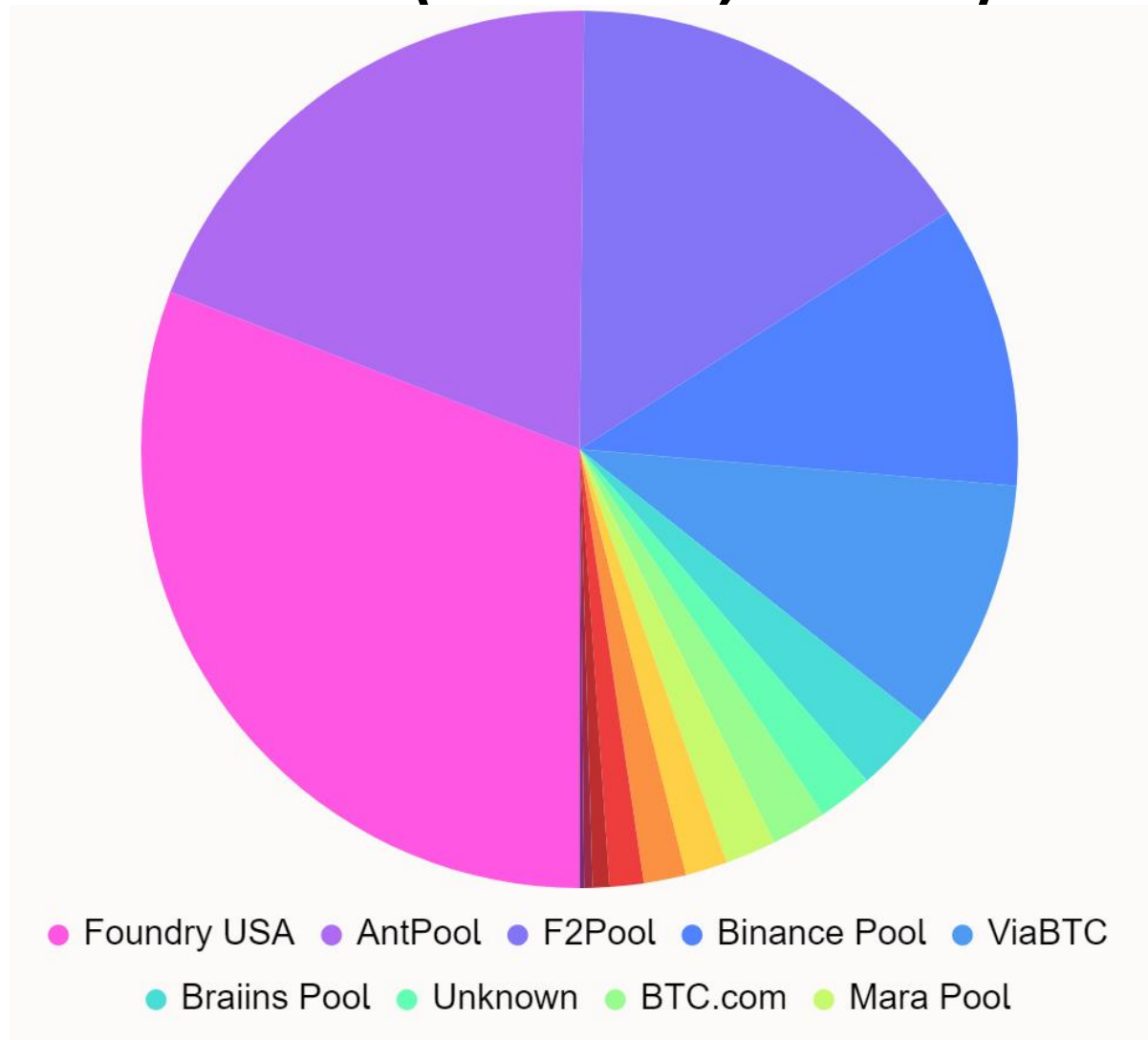
Ancient coins

- An ancient BTC address that has not transacted in over a decade came back to life on Wednesday (Feb 9, 2023)
- Since October 1 2012, address 1MMXRA held 412.12 BTC accumulated across four transactions, altogether worth just \$8 at the time. No coins went in or out of that wallet until February 8, when all but a sliver was emptied from the wallet at \$23,000 apiece.
- By today's prices, the moved coins represent \$9.6 million in value.

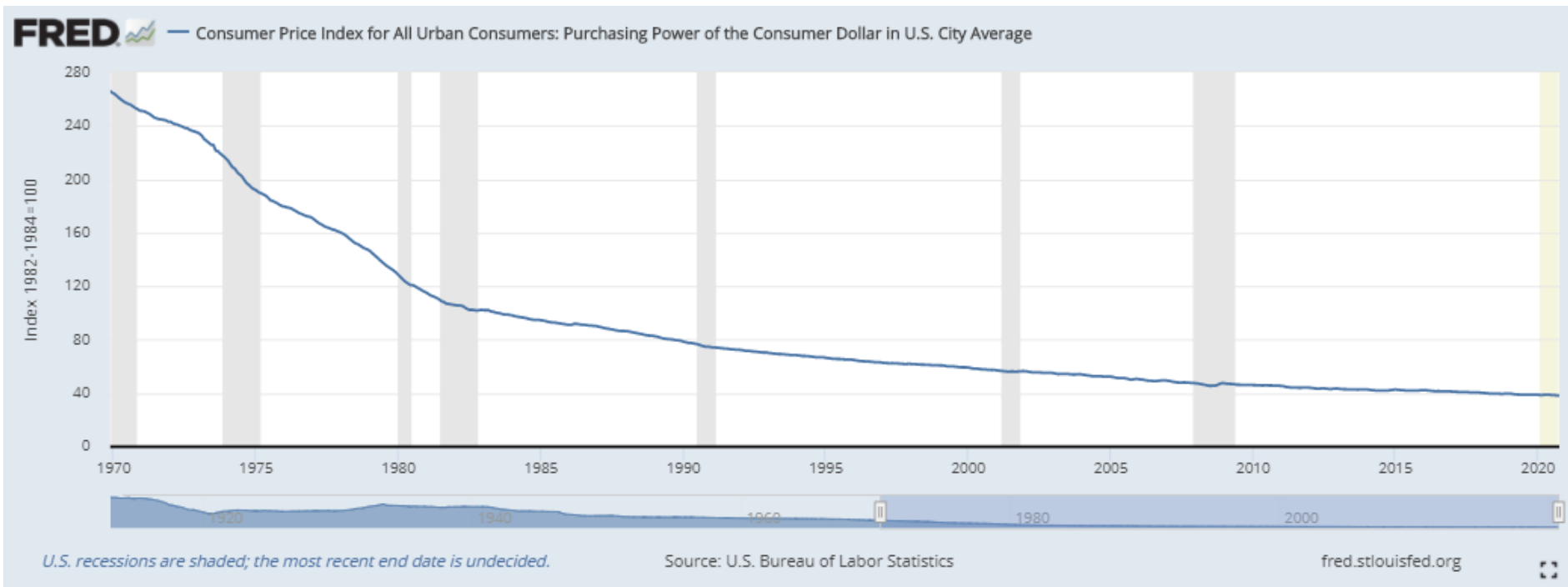
Satoshi coins

- Satoshi is suspected of holding as much as 5% of Bitcoin's entire supply due to mining in the network's early days, but many don't believe those coins will ever move again.

Bitcoin hash rate distribution (Feb 22, 2023)



Purchasing power of USD (over time 1970-2020)



FED - perpetual risk-taking as a forced substitute to saving

- a drug dealer that creates his own market by giving the first hit away for free.
- Drug dealers create their own demand by getting the addict hooked.
- That is the Fed and the financialization of the developed world economy via monetary inflation.
- By manufacturing money to lose value, markets for financial products emerge that otherwise would not.
- Products have emerged to help people financially engineer their way out of the very hole created by the Fed.
- The need arises to take risk and to attempt to produce returns to replace what is lost via monetary inflation.

Money and Investment

- money loses its value, opportunity cost is often believed to be a one way street.
- Spend your money now because it is going to purchase less tomorrow.
- While money is intended to store value, no one wants to hold it because the predominant currencies used today do the opposite.
- Rather than seek out a better form of money, everyone just invests instead!
- the quality of investment will actually be greater as both consumption and investment benefit

Bitcoin – scarce token

- there will only ever be 21 million and that alone is sufficiently powerful to begin to reverse the trend of financialization.
- While each bitcoin is divisible into 100 million units (or down to 8 decimal points), the nominal supply of bitcoin is capped at 21 million.
- Bitcoin can be divided into smaller and smaller units as more and more people adopt it as a monetary standard, but no one can arbitrarily create more bitcoin.

Ethereum – how many?

(27 Feb 2023 – Ref for Price etc.)

- **Ethereum** ETH – USD 1643,
- Market cap – 203 B,
- Latest block no. **16,189,079 → 16,716,843** (15m)
- circulating supply - **122,373,866**,
- Proof of Stake, **Algo – Ethash**,
- Genesis Block Date **30 July 2015**
- **Ethereum.org**
- Ethereum concept was introduced in 2013 by Vitalik Buterin with the release of the Ethereum whitepaper and in 2015 the Ethereum platform was launched by Buterin and Joseph Lubin along with several other co-founders.

Eth

- Ethereum is described as “the world’s programmable blockchain,” positioning itself as an electronic, programmable network that anyone can build on to launch cryptocurrencies and decentralized applications.
- Another difference between Ethereum and Bitcoin is how the networks treat transaction processing fees. These fees are known as “gas” on the Ethereum network and are paid by the participants in Ethereum transactions.

ETH - Utility token

- ETH acts more as a utility token than a token of value, its supply is technically infinite although this inflation curve slows dramatically over time.
- In theory, Ether will always be in demand, meaning inflation should never devalue the asset beyond use, thus Ether consistently enters circulation in the form of miner rewards.
- Miners get paid a transaction fee called “gas.” Gas is paid by the user initiating the transaction to the miner who validates the transaction- incentivizing future mining and network security.

PoW to PoS






- Instead of miners verifying transactions; Now, the network is using the owners of significant stakes to validate transactions.

Eth Block 16,716,843

- Mined on February 27, 2023 08:55:35 by Unknown Miner
- A total of 93.2410 ETH (\$153,197) were sent in the block with the average transaction being 0.6757 ETH (\$1,110.13).
- 0xda-8bc5 earned a base reward of 0.04 ETH \$65.72.
- The reward consisted of a base reward with an additional 0.3356 ETH (\$551.40) reward paid as fees of the 138 transactions which were included in the block.
- Now nonce is 0 (PoS not PoW)

Eth Block 16,716,843 (PoS)

Details

Hash	0×316-a99ed 	Mined	2/27/2023, 08:55:35
Parent Hash	0xcab-b266e 	Miner	0xda-8bc5 
Sha3Uncles	0×1dc-49347 	Transactions	138
State Root	0×7f6-f92b9 	Internal Txs	64
Nonce	0	Sent	93.240956
Depth	-16,716,842		153,197 USD
Capacity	12.48%	Internal Value	\$153,197
Distance	14m 6s	Value Today	\$153,237
Uncles	0	Average Value	0.67566 ETH
Uncle Reward	0.000000 ETH	Median Value	0.000000 ETH
	0.00 USD	Block Reward	0.03684 ETH
Difficulty	0.000000		60.54 USD
Total Difficulty	5.87500e+22	Minted	0.000000 ETH
Gas	17,107,252 57.02%		0.00 USD
Gas Limit	30,000,000	Fee Reward	0.33562 ETH
Size	196,226		551.44 USD






Ethereum Block10,000,000

Mined on May 04, 2020 06:52:13

- A total of 94.8397 ETH (\$19,283.76) were sent in the block with the average transaction being 0.9208 ETH (\$187.22).
- Ethermine earned a base reward of 2.00 ETH \$406.66. The reward also consisted of a base reward with an additional 0.0767 ETH (\$15.60) reward paid as fees of the 103 transactions which were included in the block.

Ethereum Block10,000,000 (PoW)

Details

Hash	0xaa2-97dbe 	Mined	5/04/2020, 18:52:13
Parent Hash	0x966-f9c4c 	Miner	0xea-8ec8 
Sha3Uncles	0x1dc-49347 	Transactions	103
State Root	0x744-2e05d 	Internal Tx	19
Nonce	0	Sent	94.839695
Depth	6,716,921		19,283.76 USD
Capacity	1.94%	Internal Value	\$19,283.76
Distance	2y 9m 24d 14h 20m 34s	Value Today	\$155,814
Uncles	0	Average Value	0.92077 ETH
Uncle Reward	0.000000 ETH	Median Value	0.000000 ETH
	0.00 USD	Block Reward	2.000000 ETH
Difficulty	2.38503e+15		406.66 USD
Total Difficulty	1.52733e+22	Minted	2.000000 ETH
Gas	9,970,867 99.81%		406.66 USD
Gas Limit	9,990,236	Fee Reward	0.07667 ETH
Size	30,515		15.59 USD

Privacy coins

- Bitcoin's pseudonymity
- Government regulators, blockchain analytics firms and others began surveilling the Bitcoin public blockchain
- Can we embed privacy into the protocol rather than making it an optional feature?

Monero (XMR) – Private, decentralized cryptocurrency

- Monero is the leading cryptocurrency focused on private and censorship-resistant transactions (launched April 2014)
- The majority of existing cryptocurrencies, including Bitcoin and Ethereum, have transparent blockchains. Transactions can be verified and/or traced by anyone in the world.
- This means that the sending and receiving addresses of these transactions could potentially be linked to real-world identities.
- Monero, on the other hand, uses various privacy-enhancing technologies to ensure the anonymity of its users.

Monero








- Coin that hides the sender, receiver and amount
- Monero makes no attempt to comply with know-your-customer/anti-money laundering (KYC/AML) procedures and values privacy above all else
- Untraceability: This means it's impossible to determine where something came from
- Unlinkability: This refers to the inability to establish a connection between people involved in a transaction or to prove various transactions were sent to the same person.

Monero (151.4 USD – 27 Feb 2023)

- Monero transactions are confidential and untraceable
- The sender, receiver, and amount of every single transaction are hidden through the use of three important technologies: Stealth Addresses, Ring Signatures, and RingCT.
- The underlying technology is so effective that, in 2020, the Internal Revenue Service called upon experts to help crack Monero's privacy features; issuing a \$625,000 reward to anyone who could successfully do it.


Block # 2,830,875

Transactions included in this block


Hash	Is coinbase?	Signers	Payment Id	Fee total	Output total	Size
22c4b50cec 	Yes	0	-	0 XMR · 0 USD	0.60974756 XMR · 92.32 USD	97 B
feb560e3a6 	No	16	9cd6870637742eb7	0.008888 XMR · 1.35 USD	** XMR · ** USD	2,222 B
3419af37af 	No	16	b6b1abee940cde0f	0.00070944 XMR · 0.11 USD	** XMR · ** USD	2,217 B
2a5cb b748d 	No	16	be09b9ebd44cf769	0.0000307 XMR · 0.00 USD	** XMR · ** USD	1,535 B
700c880e7d 	No	16	aff1aca24f7cfe96	0.0000444 XMR · 0.01 USD	** XMR · ** USD	2,220 B
dc1d17a32f 	No	16	ca8cdadbe452fcbf	0.00003064 XMR · 0.00 USD	** XMR · ** USD	1,532 B
1313a6eda4 	No	16	107dde571e7326e3	0.00004438 XMR · 0.01 USD	** XMR · ** USD	2,219 B

All time		Mempool	
Blocks	2,830,876	Transactions	13
Transactions	28,472,730	Size	30.69 kB
Difficulty	375,594,309,060	Suggested transaction fee	20 piconero per byte
Latest block	2,830,875 · 3 minutes ago		


Blocks

 Difficulty


375196667713

 Height

2830881





 Hashrate



3126.6 Mh/s

 Emission

18245726

 Block [◀ 2830880 ▶](#) 6eaa3778fce081f4a275b006a0d33896827b591083d8f6043f6aea67f254720a

 Height	2830880
 Timestamp	2023-02-27 04:31:07 UTC
 Block difficulty	375196667713
 Block size (bytes)	3166

 Cumulative Difficulty	261237931740804417
 Total Generated Coins	18245726.083596594632
 Transactions	2

Tx

⇌ Transaction 27e722cf06437d401fbacb7bac17731488bd0b5520e8bc598784c81c1746862b

✔ Confirmations	2
📦 From Block	2830880
🕒 Timestamp	2023-02-27 04:31:07 UTC
🏧 Output total	confidential
🏛️ Fee	0.000793000000 XMR
↔ Size	1530 B
🔗 Ring Size	16

RingCT

- RingCT, short for Ring Confidential Transactions, is how transaction amounts are hidden in Monero.
- Ring CT was implemented in block #1220516 in January 2017.
- RingCT introduces an improved version of ring signatures called "A Multi-layered Linkable Spontaneous Anonymous Group signature", which allows for hidden amounts, origins and destinations of transactions with reasonable efficiency and verifiable, trustless coin generation. (Refer Shen Noether's paper)

RingCT

- One is a Multilayered Linkable Spontaneous Anonymous Group (MLSAG) ring signature, which obscures the amounts, origins, and destinations of transactions;
- the second is confidential transactions, which uses a cryptographic technique called the Pederson commitment to obscure transaction amounts.
- The Pedersen commitment allows cryptography to be performed on a transaction such that the transaction can be verified while only the sender and receiver see the amount being exchanged.
- the true amounts aren't visible except to the parties involved

stealth address

(automatic one time address for every transaction)

- Stealth addresses essentially create burner addresses – or one-time public keys – for each transaction, with a sender generating a new address to send XMR tokens with a bit of additional data attached.
- Stealth addresses allow and require the sender to create random one-time addresses for every transaction on behalf of the recipient.
- The recipient can publish just one address, yet have all of his/her incoming payments go to unique addresses on the blockchain, where they cannot be linked back to either the recipient's published address or any other transactions' addresses.
- By using, only the sender and receiver can determine where a payment was sent.

Keys

- When you create a Monero account you'll have a private view key, a private spend key, and a Public Address.
- The spend key is used to send payments, the view key is used to display incoming transactions destined for your account, and the Public Address is for receiving payments.
- Both the spend key and view key are used to build your Monero address.
- When using the Monero Wallet all this is handled by the software.

Bulletproof and Dandelion

- Bulletproofs (2018) weren't about adding new privacy functionality, they were key to speeding up Monero transactions while lowering the fees associated with them.
- in 2020 Monero implemented Dandelion ++, a feature for hiding the IP addresses associated with nodes (computers that help to validate the Monero blockchain), so that it cut down the risk of such identifying information being used to deanonymize transactions. - It essentially finds a proxy node to broadcast from and then spreads "fluff" information symmetrically, such that adversaries looking to track transactions are unable to do so.

Prove to someone that you have sent them Monero in this transaction:

Recipient's Monero address

Tx private key

Prove payment

- Monero is electronic cash that allows fast, inexpensive payments to and from anywhere in the world.
- With Monero, there are no wire transfer or check clearing fees, no multi-day holding periods, and no fraudulent chargebacks. Because Monero is decentralized, it is not constrained by any particular legal jurisdiction and provides safety from capital control.

Supply

- **Emission curve**
- To make sure there will always be an incentive to mine Monero and keep it safe, the emission is infinite.
- There are two main emissions: first, main curve: ~18.132 million coins by the end of May 2022,
- then, tail curve: 0.6 XMR per 2-minute block, kicks in once main emission is done, translates to <1% inflation decreasing over time (Tail Emission).

Block

- A new block is created every ~2 minutes.
There is no maximum block size, but instead a block reward penalty and a dynamic block size, to ensure a dynamic scalability.

Challenges

- **Poisoned outputs** pose a serious threat to the privacy of Monero users because they present a human-based, rather than a technology-based, problem.
- Essentially, poisoned outputs involve two colluding parties that target a third party and attempt to learn about them by sending outputs and then analyzing their transaction graphs.
- the **Janus attack** allows an incoming transaction to appear to be addressed to one wallet subaddress while having actually been addressed to a different wallet subaddress (The goal of the attack is not to steal XMR, but to compromise the address owners' privacy by tricking them into revealing control of the two subaddresses)

XMR

- The very fact that XMR is best known as the currency of the dark web is, in itself, a testament to its success as a privacy coin. If it didn't do such a good job of protecting its users' identities, it would have been abandoned by those users.
- the trade-off with these sorts of open-access technologies is that anyone can use it, for good or bad

Other privacy coins

- **Zcash (October 2016) :**
- Heavily influenced by Bitcoin (and featuring the same 21 million coin cap), Zcash implements zk-SNARKs to ensure that all needed conditions are met for a valid transaction without exposing any personal, confidential data.
- Zcash offers multiple transaction types ranging from fully public to fully private, so it's potentially more regulatory-friendly than Monero, and fully shielded transactions can include private memos, as well.

Zcash ((**Price** 45 USD – 27 Feb 2023))

- It protects users' data by encrypting transaction information using zero-knowledge proofs.
- This technology enables transactions to be verified without having to see specific details like wallet addresses or the amount being sent.
- *zk-SNARKS* * – Zcash uses a form of zero-knowledge proofs known as 'Zero-Knowledge Succinct Non-Interactive Argument of Knowledge'.
- They enable a user to prove he has the correct money and authorisation, without having to actually show it. Similar to Wax seals used for messengers to know letters were authentic without having to actually open and check.

zk-SNARKS

- zk-SNARKS currently takes up a lot of computational power
- The strong privacy guarantee of Zcash is derived from the fact that shielded transactions in Zcash can be fully encrypted on the blockchain, yet still be verified as valid under the network's consensus rules by using zk-SNARK proofs

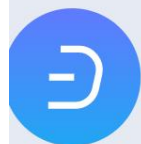
Other privacy coins

- **Dash (March 2015):** Forked from Bitcoin with the aim of improving upon the original cryptocurrency, Dash can mix multiple transactions with CoinJoin (called PrivateSend) to obscure potentially identifying details.
- Dash similarly makes its privacy features optional, and also has an InstantSend option for rapid transactions that are confirmed within two seconds.
- Anyone can become a masternode by holding 1,000 Dash in a wallet. These nodes can perform special features regular nodes can't and receive higher transaction fees as a result. Additionally masternodes get to vote on improvements to the network.

Dash (73.50 USD on 27 Feb 2023)

- Dash is a privacy focused cryptocurrency that can process transactions more quickly and cheaply than Bitcoin.
- the average block mining time is 2.5 minutes
- It's become popular in countries like Venezuela and Zimbabwe, where fiat currencies are experiencing extreme inflation.
- Privacy coins are banned in Japan and South Korea

Dash – block (<https://blockchair.com/dash>)



Explorers

Dash

API

73.53 USD ^ 3.47%

1 satoshi per byte
recommended transaction fee

Circulation 11,168,388 DASH

Market cap 820.835 million USD

Dominance 0.07%



Blocks
1,828,919



Transactions
46,586,358



Outputs
155,547,901



Addresses
1,523,750

All time

Blockchain size 28.55 GB

Network nodes 4,225

Latest block 1,828,918 • 53 seconds ago

Difficulty 118,920,655

Hashrate 3.27 Ph/s (X11)

Mempool

Transactions 9

Transactions per second 0

Outputs 73

Fees 0.02 USD

Size 0 MB

Suggested transaction fee 1 satoshi per byte

Bitcoin types – how many?

- Do it in class

Ethereum types – How many?

Different Crypto token?

Market Summary > Basic Attention Token

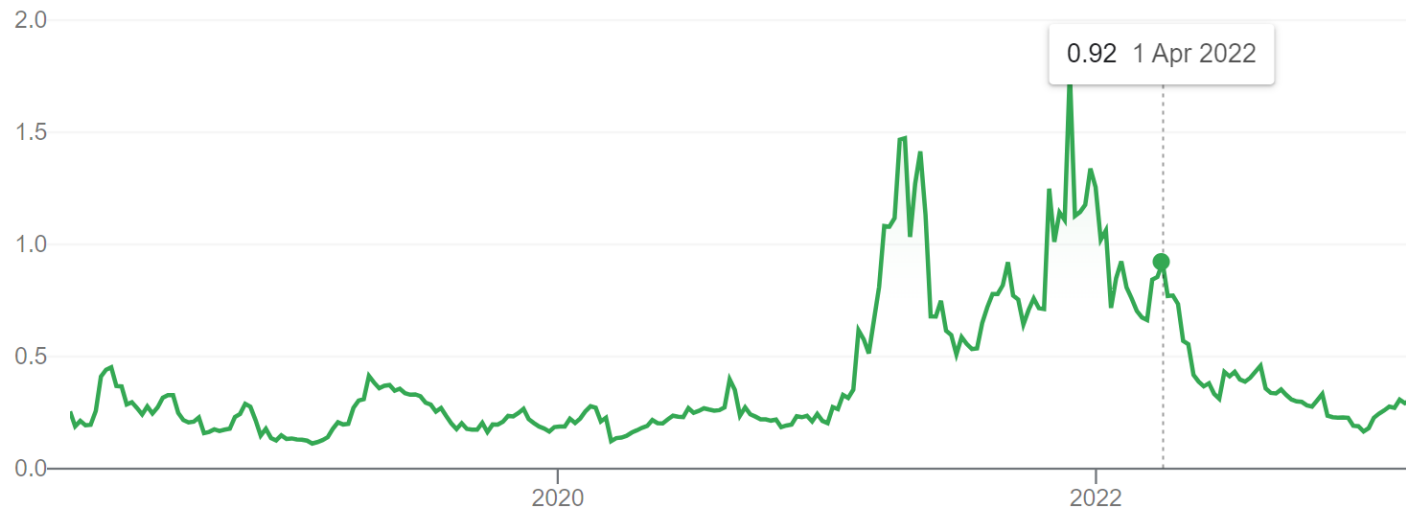
0.30 USD

+ Follow

+0.05 (19.14%) ↑ past 5 years

27 Feb, 8:17 am UTC · [Disclaimer](#)

1D | 5D | 1M | 6M | YTD | 1Y | 5Y | Max



1

BAT ▼

0.30

USD ▼

The Basic Attention Token (BAT)

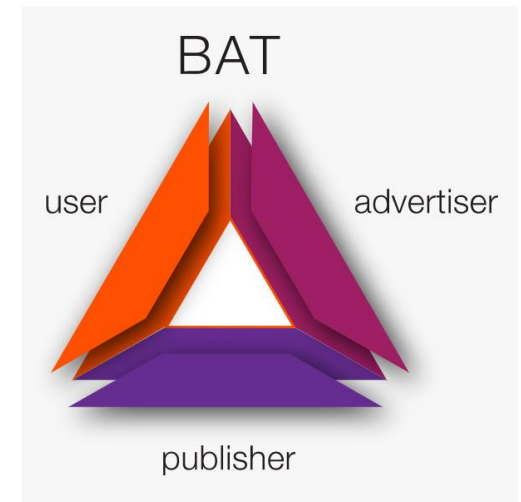
- The Basic Attention Token (BAT) was developed to address the broken digital advertising market
- BAT is an ERC20 token built on top of Ethereum, is the unit of exchange in a decentralized, open source and efficient blockchain-based digital advertising platform

BAT ecosystem

- In the ecosystem, advertisers will give publishers BATs based on the measured attention of users.
- Users also receive some BATs for participating.
- They can use them on the platform or donate them back to publishers.
- This transparent system keeps user data private while delivering fewer but more relevant ads.
- Publishers experience less fraud while increasing their percentage of rewards.
- Advertisers get better reporting and performance

BAT - basic attention token

- BLOCKCHAIN-BASED DIGITAL ADVERTISING
- Basic Attention Token radically improves the efficiency of digital advertising by creating a new token that can be exchanged between publishers, advertisers, and users. It all happens on the Ethereum blockchain.
- The token can be used to obtain a variety of advertising and attention-based services on the BAT platform.
- The utility of the token is based on user attention, which simply means a person's focused mental engagement.



Prolouge

- Attention has been widely recognized as a commodity
- Beginning with radio, each new medium would attain its commercial viability through the resale of what attention it could capture in exchange for its 'free' content.
- The promise of advertising technology (“ad-tech”) was to create a more efficient marketplace for attention. The hope was that the Internet would arrive with a transparent and efficient ad marketplace.

Advertising Technologies

- Ad tech would “get marketers closer to their users via data analysis, immediate valuation and distribution.”
- Data would be used to “accurately identify audiences, determine the value of those audiences, and deliver the right messages to them instantly.”
- That didn’t happen. Instead, the ad-tech ecosystem that has evolved over the last two decades is a bewildering variety of middlemen and complexity.

What went wrong?

- Worse, ad-tech introduced a host of correlated problems for publishers, advertisers and users.
- Users have lost their privacy, users are facing increasing malware, and suffer slow speeds.
- Publishers have lost billions in revenue while fraud has skyrocketed.
- And advertisers face poor reporting and targeting.

Electronic pollution

- Users suffer a form of “electronic pollution” consisting of
 - threats to security, threats to privacy,
 - costs in inefficient download times,
 - financial costs in extra data (bandwidth) fees,
 - excessive costs to their attention
- //Neurons can and do learn to ignore ad slots (banner blindness)
- //While most users may be willing to pay some price for access to the publisher’s information, user attention is mispriced when we sum up the growing negative externalities imposed by the present advertising ecosystem

Definition(s)

- attention is focused mental engagement on a particular item of information.
- Items come into our awareness, we attend to a particular item, and then we decide whether to act.
- Advertising, throughout history, has been used as the primary mechanism to capture Attention, raise it to a level of Interest to incite some Desire that can then translate it into Action
- Advertising evolved around - print form, radio, tv
- Internet brought the development of a new level of advertising technology with the promise of higher speed and better information

Attention market place

- the advertising ecosystem has become more complex and crowded, with many more players taking a piece of the advertising pie, either directly or indirectly
- Sales planners currently budgeting for brand advertising - are required to account for an excessive number of intermediaries that stand between the ad and the end user.
- Agencies, trading desks, demand side platforms, desktop and mobile network exchanges, yield optimization, rich media vendors and partnered services often consume significant portions of creative and delivery ad budget.

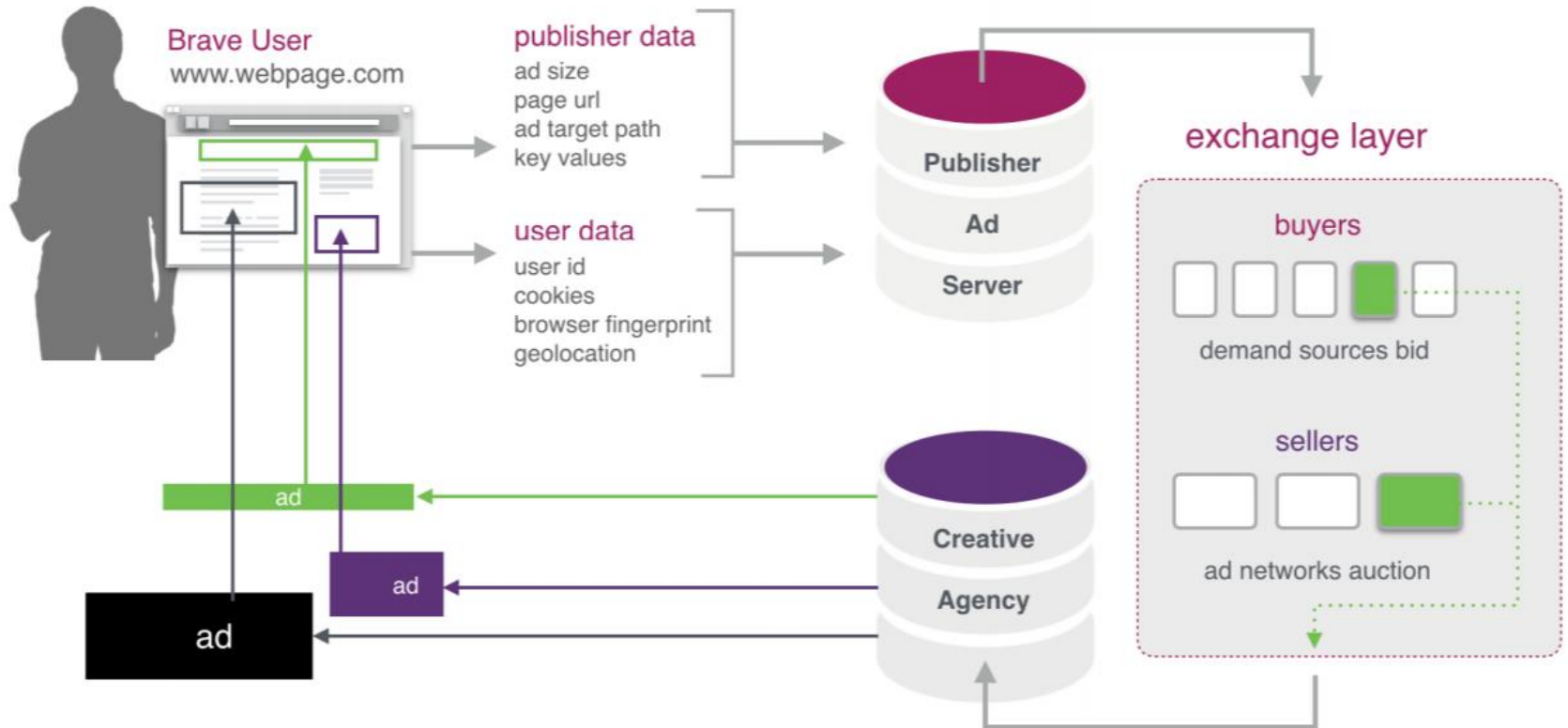
Attention market place

- It is also common for agencies in charge of packaging brand campaigns to use data aggregators, data management platforms, data suppliers, analytics, measurement and verification services to fight fraud, enhance targeting, and confirm attribution.
- These factors add up to a high transaction cost on the efficient provision of attention to brand ad campaigns.

Social cost - clickbait

- the violation of user privacy exacts a significant social cost; economists have compared violations of user privacy as analogous to environmental pollution
- government should do more to regulate advertisers - regarding how they use and store personal information

Typical Digital Ad flow



Effects

- the data used by advertising resulted in significant download times and costs across 50 top publishing sites
- removing ads saved “more than five seconds of loading time over a typical cell connection”
- The data to load the ads came with a financial cost as well – the price for the advertising content often outweighs that of editorial material...
- On one extreme, www.boston.com took 30.8 seconds for advertising and 8.2 seconds for editorial.

Publishers' losses

- Publishers pay ad serving fees, operational fees for campaign setup, deployment and monitoring, publisher analytics tools
- The sum total of malvertisements, load times, data costs, battery life, and privacy loss has driven users to adopt ad-blocking software.
- users of ad blocking software prefer the simplicity of navigation of ad-free or nearly ad-free content
- This further reduces publisher revenues and leaves the remaining ad-viewing audience even harder to target.

Existential threat

- This “perfect storm” for publishers has only gotten worse over the last few years as Google and Facebook have taken more and more share of advertising revenues!!!
- While Facebook Instant Articles, Google AMP project and Apple News delivery channels were initially presented to publishers as opportunities to extend reach and visibility, they ultimately diminish publishers’ control of their brand narratives and reader relationships, and divert direct attention away from publisher sites over the long run.
- Marketing budgets continue to climb, yet publisher revenues are static or shrinking

Why BAT?

- Gatekeeper companies such as Google and Facebook control the entire online marketing budget with publishers powerless to control their revenues
- Users face unprecedented levels of malvertisements and privacy violations.
- Mobile advertising results in as much as \$23 per month in data charges on the average user's data plan, slow page loads, and as much as 21% less battery life. (March 2018 - USA)
- Publishers face falling revenue, users feel increasingly violated, and advertisers' ability to assess effectiveness is diminished.
- The solution is a decentralized, transparent digital ad exchange based on Blockchain...

Attention-based Economics on Blockchain

- user attention is valuable, but it hasn't been properly priced with an efficient and transparent market system
- information consumes the attention of its recipients
- Hence a wealth of information creates a poverty of attention and a need to allocate that attention efficiently among the overabundance of information sources that might consume it!!

Design rationale



- The first phase involved the roll-out of a new browser, Brave, a fast, open source, privacy-focused browser that blocks invasive ads and trackers, and contains a ledger system that anonymously measures user attention to accurately reward publishers.
- The next phase involves the introduction of Basic Attention Token or BAT. It is a token for the decentralized ad exchange.
- BAT connects advertisers, publishers, and users, creating a new, efficient marketplace. The token is based on Ethereum technology

Online privacy by default: Brave vs. other browsers



Full Protection



No protection



Limited protection

Built-in features



Brave



Firefox



Safari



Google
Chrome

Invasive ads blocked



Cross-site trackers blocked



Cookies blocked



Fingerprinting blocked
(cookie-less trackers)



Malware & phishing protection*



Design rationale

- The token is derived from – or denominated by – user attention. Attention is really just focused mental engagement – on an advertisement in this case.
- Attention be measured as viewed for content and ads only in the browser's active tab in real time. The Attention Value for the ad will be calculated based on incremental duration and pixels in view in proportion to relevant content, prior to any direct engagement with the ad..

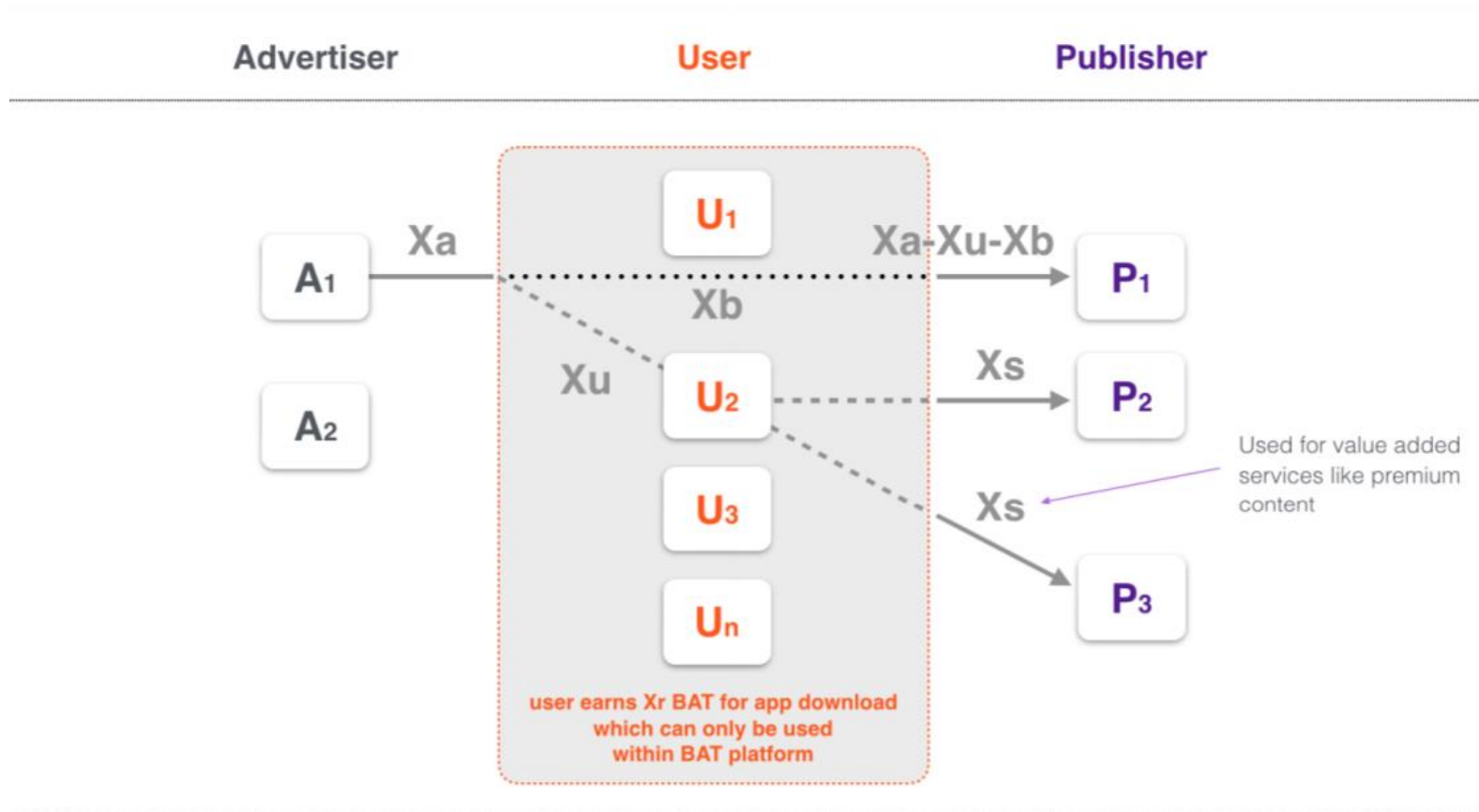
How?

- The first component is Brave, a fast, open source, privacy-focused browser that blocks third party ads and trackers, and builds in a ledger system that measures user attention to reward publishers accordingly.
- Brave will now introduce BAT (Basic Attention Token), a token for a decentralized ad exchange. It compensates the browser user for attention while protecting privacy.
- BAT connects advertisers, publishers, and users and is denominated by relevant user attention, while removing social and economic costs associated with existing ad networks, e.g., fraud, privacy violations, and malvertising.
- BAT is a payment system that rewards and protects the user while giving better conversion to advertisers and higher yield to publishers.

Value Proposition

- BAT as a token of exchange in a secure, anonymous, opt-in advertising system based in the browser and the mobile app webview.
- The BAT system provides:
- Users: strong privacy and security when viewing advertisements, improved relevance and performance, and a share of tokens.
- Publishers: improved revenue, better reporting, and less fraud.
- Advertisers: less expensive customer attention, less fraud, and better attribution.

Value flow of BAT



Publisher Revenue

$$\boxed{X_a} - \boxed{X_u} - \boxed{X_b} = \boxed{X_p}$$

Advertiser buy-in User share Brave placement share Publisher Revenue

System

- Publisher payment will be through the BAT system - all payments in BAT must have a publisher endpoint.
- For the first deployment of BAT, the transactions in BAT will take place through the Brave Ledger system, allow Brave users to make anonymous donations to publishers using bitcoin as the medium of exchange.
- A fully distributed ledger is desirable, both for public accountability and potential scalability reasons
- Publishers, advertisers and users of the BAT token will have incentive to use such a system to keep track of payments within the BAT system

USP - a fully distributed micropayment system

- free and open source infrastructure
- the transactions in a fully distributed BAT system will almost always be one to many and many to one
- private, secure and well-engineered
- the privacy of the browser customer is of primary importance; publishers and advertisers have fewer privacy concerns

BAT eco system

- Content may also be bought for friends using the token; if someone likes a premium article, they can make a micropayment to send it to three of their friends
- Higher quality content may also be offered to users for a BAT transaction
- Comment votes backed by BAT may be given more credibility due to the fact that someone cared enough to back the comment with what would be a limited supply of token, as well as the fact that a token transfer can be verified as coming from real people rather than robots.
- The right to post comments may also be purchased for some minimal payment, to cut down on abusive commenters

BAT applications

- BAT may be used within the Brave ecosystem to purchase digital goods such as high resolution photos, data services, or publisher applications which are only needed on a one-time basis
- Custom news alerts may be offered as a service by news providers for a small payment of BAT within the ecosystem

Browser as platform/BAT

- transfer and verification process entirely distributed on Ethereum using a state channel scheme
- **Competitors**
- Reddit (home to thousands of communities, endless conversation, and authentic human connection – one can get award on the post or comment – spend for good comment, turn off ads, additional comment filters)
- Steem (social-media and blogging platform - users earn revenue when they receive upvotes)
- Blendle (a kind of iTunes for journalism - offering micropayments on a per-story basis)
- Google (search engine company that makes most of its revenue from digital advertising - Users are unaware of how their privacy is compromised)

BAT advantage matrix

Present ecosystem	BAT token ad payments
User frustration over loading time	Fast loads
Walled gardens	Free software, open source infrastructure
Bandwidth wasted	Low bandwidth overhead
Screen clutter	Uncluttered screen
Irrelevant ads	Ads tuned to user interests
Security issues	No malware
Viewability problems/attribution	Secure attribution/attention score
Advertiser uncertainty about delivery	Perfect delivery certainty
CPM/click based	Attention-based
Reader attention not valued	Reader is paid for attention
Publisher revenues lowering	Larger publisher revenues
Expensive ad buys due to middlemen	Efficient ad buys
Complex/expensive viewability metrics	Simple/free viewability metric
User's privacy violated	Perfect user privacy

Brave Browser - tokens for viewing privacy-respecting ads

- Brave is more than a browser: it defends your data on your devices and synchronizes your personal and private browsing profile across devices using client-side encryption.
- Your data, studied and abstracted by on-device-only machine learning, provides you with private and anonymous options to get compensated for your attention.
- Brave cuts out all third-party trackers and middle-players, eliminating data leakage, malware risk, and excessive fee-taking.
- Brave does this while providing publishers with a substantially larger revenue share than they are receiving in existing inefficient and opaque marketplaces.
- Brave thus aims to reset the online ad-based Web ecosystem, giving advertisers, publishers and customers a win-win solution whose components and protocols can become future Web standards.
- When you use Brave Rewards, you earn Basic Attention Tokens (BAT) for each privacy-respecting ad Brave shows you. A typical, engaged person who uses Brave as their everyday browser can expect to earn about **\$5 of BAT a month**

BAT - Token milestones

- Launch date and time: 8AM PST May 31, 2017
block number 3,798,640
- Exchange rate: 1 ETH = 6,400 BAT (2017)
- Token launch time-frame: 30 days (based on Blocknumber 3,963,480).
- Token launch completion: Token launch will end when either the maximum number of ETH are raised or block number 3,963,480 is reached. If less than the minimum ETH are raised, ETH can be retrieved by holders of BAT.
- (Today) 1 Eth = 1701 BAT ~0.22 USD

Token Distribution

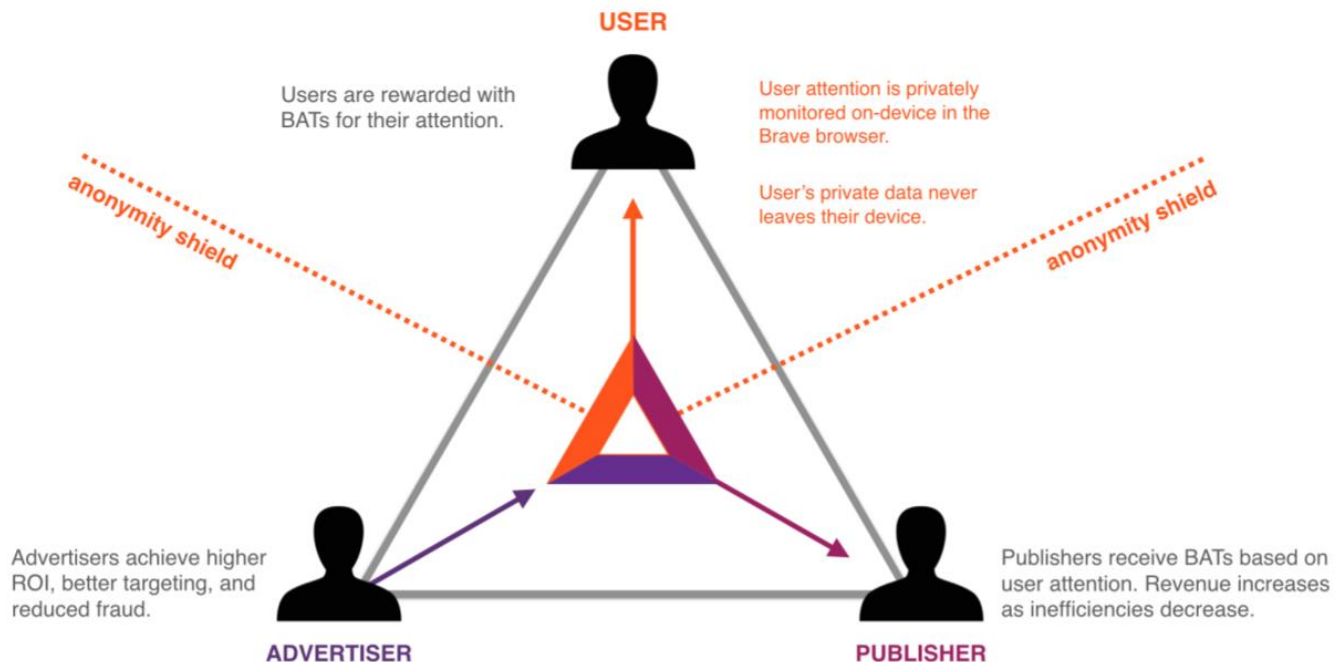
- Brave: 13.3% of max; 200 million BAT.
- User growth pool: 300 million BAT.
- Token available to public at launch: 1 billion (corresponding to the ETH raised at token launch)

User Growth Pool

- User growth fund is used to incentivize users to participate in the BAT ecosystem.
- A 300 million endowment is for early adopters of Brave and the BAT at up to 5 BAT/user.
- BAT received as a reward can only be used within the BAT ecosystem for value added services.
- Unused BAT after 6 months will be sent back to the user growth fund which can then be used for new users.
- Existing Brave users can get tokens by updating their app and verifying phone number.
- No new tokens will be created once the user growth pool is exhausted.

Summary

- The BAT, a token based on the Ethereum technology, is a unit of exchange in a new Blockchain based digital advertising system. User attention is anonymously monitored in the Brave browser and publishers are rewarded accordingly with BATs. Users also get a share of BATs for participating.



Midsem

(next week – 6 to 12 March 2023)

- Introduction: Blockchain, Bitcoin, Crypto currency, Mining, Consensus,
- Money reimagined – currency evolution, price fluctuation
- Stocks, Fiats, Crypto... exchanges – centralized, decentralized
- Blockchain explorer – tx, block, difficulty, blockheader, parameters
- Market cap, dominance – top 20 crypto currencies
- Security and Trust – Bitcoin, Ethereum
- Privacy coins – Monero, Zcash, Dash
- Advertising – BAT, Ethereum and Bitcoin varieties
- Foundation – Math - ECC – ECDSA, ECDH, Crypto primitives, Hash function SHA256, Merkel Tree,
- Smart Contract programming – Ethereum basics, Ganache, Truffle, Smart contract implementation

Ref. Books

- Bitcoin and Cryptocurrency Technologies By Narayanan, Bonneau, Fleten, Miller, Goldfeder
- Princeton University Press (2016)
- Mastering Bitcoin By Andreas M Antonopoulos
- O'Reiley (2017) – second edition
- Ref papers/sites – e.g., Satoshi Nakamoto – bitcoin whitepaper, Ethereum white paper, PPTs, Blockchain explorers