Devere Anthony Weaver
COSC670 - Cryptocurrencies and Blockchain
Towson University - Spring 2024

I. Please write and submit this portion as a1p1.pdf. Some of the topics were discussed in lecture and now you will dive a bit deeper into a few and explore consensus across different chains. For any references used, please be sure to cite the urls in the footnotes

a. Cardano validates a block and transaction

Cardano uses a proof of stake method to validate blocks on its chain. Apparently it leverages the Ouroboros protocol which is a “family of proof-of-stake consensus protocols used in the Cardano and Polkadot blockchains. It can run both permissionless and permissioned blockchains” [1]. Of course this protocol is in contrast to Bitcoin’s proof of work method.

The paper for Cardano doesn’t really go into much detail about the protocol itself, just who created it and what it does, but from what I gathered a *very* simplified version of this uses what are known as slot leaders. Slot leaders are chosen based on their amount of Cardano at stake and they are responsible for validating blocks, similar to miners in Bitcoin. When a slot leader creates a block, it is then propagated throughout the network and then each node independently validates the block. Once the block is validated by the majority of stakeholders, then consensus is achieved and the block is added to the blockchain.

b. Solana validates a block and transaction

Solana uses a consensus mechanism called proof-of-history along with proof-of-stake as consensus mechanisms. Much of my understanding comes from reading [2]. At a very high-level, Solana uses proof-of-history as a way to achieve high throughput and scale by enabling parallel processing of transactions. With proof-of-history, Solana timestamps each transaction and ensures that all participants in the network can agree on the order of events without having to communicate with each other. Solana also combines this algorithm along with a proof-of-stake algorithm that is similar to how Cardano uses it mentioned above.

The other unique part of Solana’s validation process is its custom version of the Tower Byzantine Fault Tolerance consensus. It is a slightly more optimized variation on the standard Byzantine Fault Tolerance consensus algorithm to enable distributed nodes to agree on the state of the system. After the block is created, each network node validates the transaction and it is then placed on the chain.

c. Ethereum validates a block and transaction

Ethereum now uses a proof-of-stake mechanism for validation instead of proof-of-work. Ethereum's proof-of-stake works similar to the previous blockchain's proof-of-stake.

At a high-level, once a transaction is created, it is submitted to the Ethereum blockchain's execution clients, a validator, to verify validity of the transaction as well as confirming the proper amount of gas was sent. Validators stake their ETH into a smart contract on the Ethereum blockchain to become a validator. Currently a validator must stake a minimum of 32 ETH. These validators confirm the new blocks created while also creating new blocks that are propagated throughout the network to update Ethereum's global state.

Each execution client that receives this new block from the network then re-execute the transaction to confirm its validity. Once enough of these validators confirm the block to be valid, it is added to the chain.

d. In your own opinion, which out of the three seem the most efficient and scalable? Why?

Based on reading the technical details of how each of the previous consensus mechanisms works, from my understanding I'd posit Solana has the most efficient and scalable method. The ability to process transactions in parallel means by design it should theoretically have a higher throughput and faster confirmation times. This higher throughput should also reduce the amount of transaction fees and network congestion since propagating the blocks throughout the network, like the Cardano and Ethereum implementation, takes up bandwidth.

e. What does it take to become a validator node on each of these blockchains? Which would you pick to make the most profit and why?

To become a validator on Cardano you have to set up a registered server and deposit (at the time of this writing) about 500 ADA. As of March 2024 this is roughly $320 dollars, give or take due to general price fluctuation. Apparently there also is no risk of losing the stake, after deregistering the server you get the ADA back.

To become a validator on Ethereum, a validator must stake at least 32 ETH, which is approximately $113,305 as of March 2024. A validator must also run an execution client, validator client, and consensus client on their nodes.

To become a validator on Solana, the validator must pay 0.02685864 SOL, about $5 as of March 2024. This is simply to reserve a spot as a validator. A validator must also pay up to 1.1 SOL per day to participate in the validation process, which is significantly more than the reservation fee. That 1.1 SOL is about $200.

Solana appears to have the lowest startup and participation costs followed by Cardano. Ethereum clearly has the highest startup cost to become a validator. I suppose if I had the funding for it, I would choose Ethereum to make the most profit.

According to Coinbase, the estimated ETH reward rate APY is sitting at 2.61% as is actually up 3.99% within the past 30 days. If I were to stake even the minimum amount of ETH to become a validator, participate in the validation process only one time this year, and if I were to actually be lucky enough to win the reward, that one time reward would be worth a few thousand dollars.

I haven't seen anything that indicates the other two have the same level of rewards for validators.

f. **Do you see any flaws or potential dangers with any of the three blockchains? If yes, state and explain them. If not, explain how it is foolproof.**

For the proof-of-stake mechanism, the only real potentially glaring issue that could occur is the network validation could become centralized. This is due to the amount of currency that has to be staked to participate in the validation process.

For example, in the case of Ethereum, if a validator somehow gets their hands on a massive amount of ETH, they could gain control as the most influential validator on the network and have a disproportionate amount of leverage on the network when it comes to approving transactions.

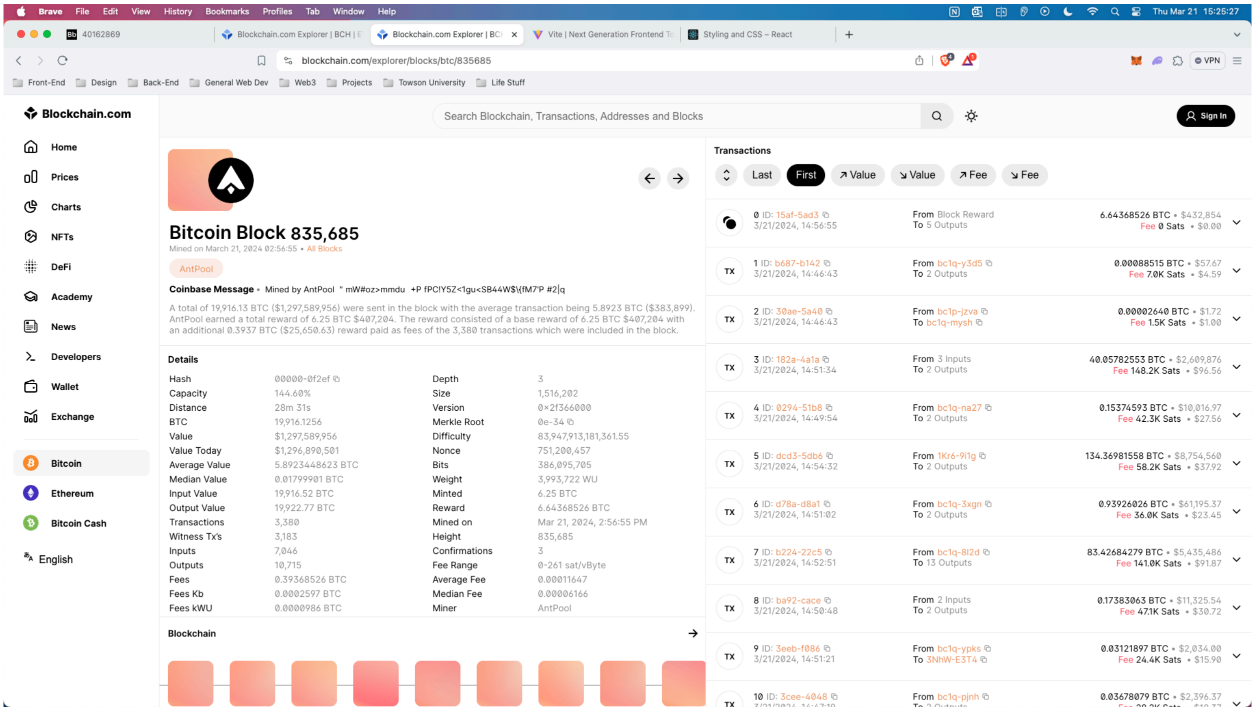
This would defeat the purpose of maintaining a decentralized network. It seems unlikely but it is still theoretically possible given how the proof-of-stake mechanism works.

References

[1] Wikipedia. *Ouroboros (protocol)*. https://en.wikipedia.org/wiki/Ouroboros_(protocol). (accessed 2024-03-25).

[2] Solana Foundation. *Proof of History: How Solana brings time to crypto*. https://solana.com/news/proof-of-history. (accessed 2024-03-25).

II. Explain the following fields (1-2 sentence per field) for BTC:


Brave File Edit View History Bookmarks Profiles Tab Window Help
Thu Mar 21 15:25:27
40162869
Blockchain.com Explorer | BCH | E
Blockchain.com Explorer | BC
Vite | Next Generation Frontend To
Styling and CSS – React
blockchain.com/explorer/blocks/btc/835685
VPN
Front-End
Design
Back-End
General Web Dev
Web3
Projects
Towson University
Life Stuff
Blockchain.com
Search Blockchain, Transactions, Addresses and Blocks
Sign In
Home
Prices
Charts
NFTs
DeFi
Academy
News
Developers
Wallet
Exchange
Bitcoin
Ethereum
Bitcoin Cash
English

Bitcoin Block 835,685

Mined on March 21, 2024 02:56:55 • All Blocks

AntPool

Coinbase Message • Mined by AntPool " mW#oz>mmdu +P fPC!Y5Z<1gu<SB44W$\{fM7'P #2|q

A total of 19,916.13 BTC ($1,297,589,956) were sent in the block with the average transaction being 5.8923 BTC ($383,899). AntPool earned a total reward of 6.25 BTC $407,204. The reward consisted of a base reward of 6.25 BTC $407,204 with an additional 0.3937 BTC ($25,650.63) reward paid as fees of the 3,380 transactions which were included in the block.

Details

Hash	00000-0f2ef	Depth	3
Capacity	144.60%	Size	1,516,202
Distance	28m 31s	Version	0×2f366000
BTC	19,916.1256	Merkle Root	0e-34
Value	$1,297,589,956	Difficulty	83,947,913,181,361.55
Value Today	$1,296,890,501	Nonce	751,200,457
Average Value	5.8923448623 BTC	Bits	386,095,705
Median Value	0.01799901 BTC	Weight	3,993,722 WU
Input Value	19,916.52 BTC	Minted	6.25 BTC
Output Value	19,922.77 BTC	Reward	6.64368526 BTC
Transactions	3,380	Mined on	Mar 21, 2024, 2:56:55 PM
Witness Tx's	3,183	Height	835,685
Inputs	7,046	Confirmations	3
Outputs	10,715	Fee Range	0-261 sat/vByte
Fees	0.39368526 BTC	Average Fee	0.00011647
Fees Kb	0.0002597 BTC	Median Fee	0.00006166
Fees kWU	0.0000986 BTC	Miner	AntPool

Blockchain

Transactions

	0 ID: 15af-5ad3 3/21/2024, 14:56:55	From Block Reward To 5 Outputs	6.64368526 BTC • $432,854 Fee 0 Sats • $0.00
TX	1 ID: b687-b142 3/21/2024, 14:46:43	From bc1q-y3d5 To 2 Outputs	0.00088515 BTC • $57.67 Fee 7.0K Sats • $4.59
TX	2 ID: 30ae-5a40 3/21/2024, 14:46:43	From bc1p-jzva To bc1q-mysh	0.00002640 BTC • $1.72 Fee 1.5K Sats • $1.00
TX	3 ID: 182a-4a1a 3/21/2024, 14:51:34	From 3 Inputs To 2 Outputs	40.05782553 BTC • $2,609,876 Fee 148.2K Sats • $96.56
TX	4 ID: 0294-51b8 3/21/2024, 14:49:54	From bc1q-na27 To 2 Outputs	0.15374593 BTC • $10,016.97 Fee 42.3K Sats • $27.56
TX	5 ID: dcd3-5db6 3/21/2024, 14:54:32	From 1Kr6-9i1g To 2 Outputs	134.36981558 BTC • $8,754,560 Fee 58.2K Sats • $37.92
TX	6 ID: d78a-d8a1 3/21/2024, 14:51:02	From bc1q-3xgn To 2 Outputs	0.93926026 BTC • $61,195.37 Fee 36.0K Sats • $23.45
TX	7 ID: b224-22c5 3/21/2024, 14:52:51	From bc1q-8l2d To 13 Outputs	83.42684279 BTC • $5,435,486 Fee 141.0K Sats • $91.87
TX	8 ID: ba92-cace 3/21/2024, 14:50:48	From 2 Inputs To 2 Outputs	0.17383063 BTC • $11,325.54 Fee 47.1K Sats • $30.72
TX	9 ID: 3eeb-f086 3/21/2024, 14:51:21	From bc1q-ypks To 3NhW-E3T4	0.03121897 BTC • $2,034.00 Fee 24.4K Sats • $15.90
TX	10 ID: 3cee-4048	From bc1q-pjnh	0.03678079 BTC • $2,396.37

- **confirmations -** A confirmation represents the given block being added to the BTC network. Certain BTC transactions require a certain number of confirmations before the entity considers the transaction settled, the higher the number of confirmations, the more sure they can be that the transaction is legitimate on the network.

- **height -** The height is simply the number of previous blocks on the blockchain. For example, the height for the block in the image is 835,685. That means there are 835,684 blocks on the chain before this one (i.e. this guy is the 835,685th BTC block).

- **difficulty -** Difficulty is a relative measure of how computationally “hard” it is to compute a hash for the given block. It is a dynamic measurement and exists to help ensure blocks aren’t mined too fast, which could possibly cause issues on the network.

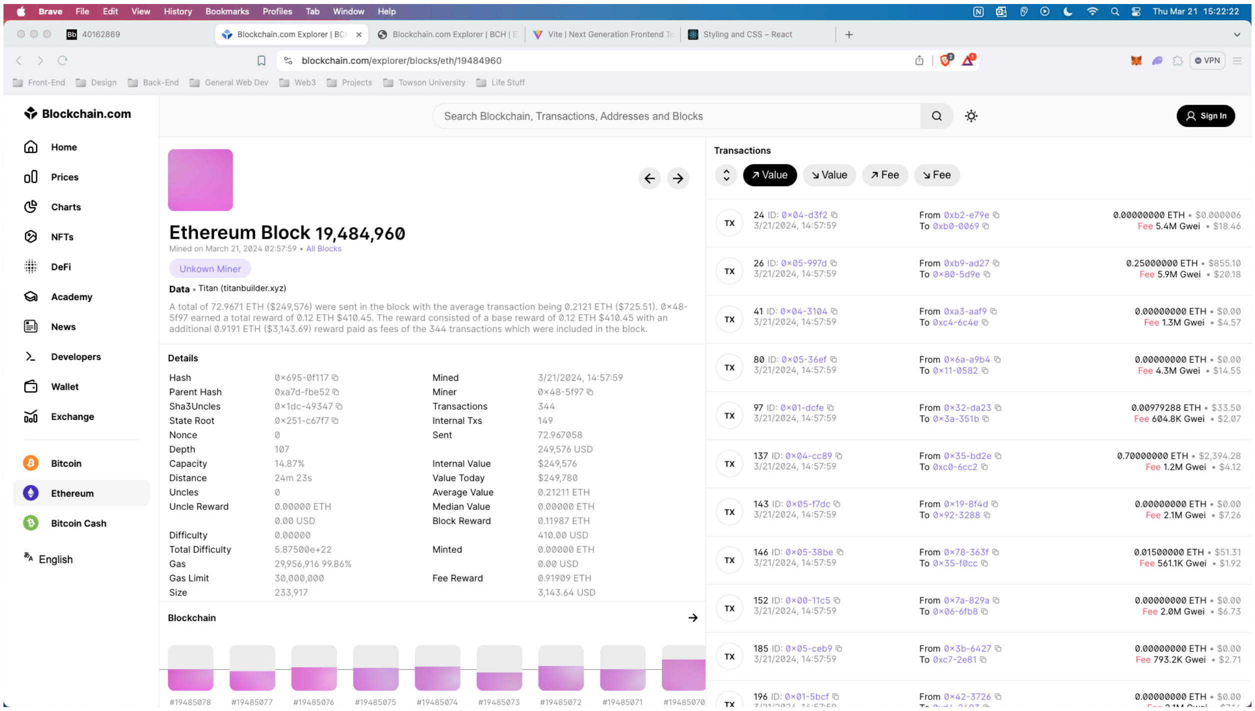
- **weight -** A block weight is a relative measure of size between blocks. It is computed as a function of the transaction size and the complexity of the transaction. The measure helps increase transaction capacity.

- **size -** The size field is just a measure of the size of the given block measured in MB.

- **nonce -** The nonce is a random number that network miners need to compute to verify a BTC block. The first miner to compute this receives the block reward.

- **depth -** The depth appears to simply be the total number of confirmations on the chain. As stated previously, the higher the number of confirmations, the better the chance the block and transactions are legitimate on the network and won't get reversed.

Explain the following fields (1 sentence per field) for ETH:



Ethereum Block 19,484,960

Mined on March 21, 2024 02:57:59 • All Blocks

Unkown Miner

Data • Titan (titanbuilder.xyz)

A total of 72.9671 ETH ($249,576) were sent in the block with the average transaction being 0.2121 ETH ($725.51). 0×48-5f97 earned a total reward of 0.12 ETH $410.45. The reward consisted of a base reward of 0.12 ETH $410.45 with an additional 0.9191 ETH ($3,143.69) reward paid as fees of the 344 transactions which were included in the block.

Details

Hash	0×695-0f117	Mined	3/21/2024, 14:57:59
Parent Hash	0xa7d-fbe52	Miner	0×48-5f97
Sha3Uncles	0×1dc-49347	Transactions	344
State Root	0×251-c67f7	Internal Txs	149
Nonce	0	Sent	72.967058
Depth	107		249,576 USD
Capacity	14.87%	Internal Value	$249,576
Distance	24m 23s	Value Today	$249,780
Uncles	0	Average Value	0.21211 ETH
Uncle Reward	0.00000 ETH	Median Value	0.00000 ETH
	0.00 USD	Block Reward	0.11987 ETH
Difficulty	0.00000		410.00 USD
Total Difficulty	5.87500e+22	Minted	0.00000 ETH
Gas	29,956,916 99.86%		0.00 USD
Gas Limit	30,000,000	Fee Reward	0.91909 ETH
Size	233,917		3,143.64 USD

Blockchain

Transactions

TX 24 ID: 0×04-d3f2 3/21/2024, 14:57:59 From 0xb2-e79e To 0xb0-0069 0.00000000 ETH • $0.000006 Fee 5.4M Gwei • $18.46

TX 26 ID: 0×05-997d 3/21/2024, 14:57:59 From 0xb9-ad27 To 0×80-5d9e 0.25000000 ETH • $855.10 Fee 5.9M Gwei • $20.18

TX 41 ID: 0×04-3104 3/21/2024, 14:57:59 From 0xa3-aaf9 To 0xc4-6c4e 0.00000000 ETH • $0.00 Fee 1.3M Gwei • $4.57

TX 80 ID: 0×05-36ef 3/21/2024, 14:57:59 From 0×6a-a9b4 To 0×11-0582 0.00000000 ETH • $0.00 Fee 4.3M Gwei • $14.55

TX 97 ID: 0×01-dcfe 3/21/2024, 14:57:59 From 0×32-da23 To 0×3a-351b 0.00979288 ETH • $33.50 Fee 604.8K Gwei • $2.07

TX 137 ID: 0×04-cc89 3/21/2024, 14:57:59 From 0×35-bd2e To 0xc0-6cc2 0.70000000 ETH • $2,394.28 Fee 1.2M Gwei • $4.12

TX 143 ID: 0×05-f7dc 3/21/2024, 14:57:59 From 0×19-8f4d To 0×92-3288 0.00000000 ETH • $0.00 Fee 2.1M Gwei • $7.26

TX 146 ID: 0×05-38be 3/21/2024, 14:57:59 From 0×78-363f To 0×35-f0cc 0.01500000 ETH • $51.31 Fee 561.1K Gwei • $1.92

TX 152 ID: 0×00-11c5 3/21/2024, 14:57:59 From 0×7a-829a To 0×06-6fb8 0.00000000 ETH • $0.00 Fee 2.0M Gwei • $6.73

TX 185 ID: 0×05-ceb9 3/21/2024, 14:57:59 From 0×3b-6427 To 0xc7-2e81 0.00000000 ETH • $0.00 Fee 793.2K Gwei • $2.71

TX 196 ID: 0×01-5bcf From 0×42-3726 0.00000000 ETH • $0.00

- **gas -** For the Ethereum blockchain, gas is the term for the unit the blockchain uses to measure computation for actions on the blockchain. It measures the amount of computational steps needed per transaction and also exists to reward miners and DoS.

- **gas limit -** The gas limit is the amount of gas by all the transactions on a given Ethereum block, it helps determine how many transactions will be allowed on the block. If the block reaches the gas limit, then it is considered full and no further transactions can be processed on that block.

- **block reward -** A block reward is the set amount of ETH that is given to a miner/validator on the network once they have computed the solution to the PoW/PoS problem.

- **internal txns -** The number of transactions or interactions between contracts in the processed block. Some don't consider these to be real transactions as they apparently aren't recorded on the blockchain and are simply transfers of some value between the contracts.