TABConf 2024
BitDevs Socratic Village:

Hardcore Trivia

Brought to you by:
Localhost Research

Rules

1. 30 questions, a mix of multiple choice and free-response.
    a. 1 point per question
    b. ½ point for bonus questions
2. Questions span cypherpunk and Bitcoin history, as well as cover a variety of technical questions. Sometimes technical and history questions are blended.
3. Teams of 4. Pick a team name.
    a. **No more than one OG per team.** OG is defined as someone who has been in the space for >=10 years.
4. Don’t shout the answers, no internet access.
5. Winner takes all. Prize: $350 in sats. Paid via lightning.

Question 1

In 1993, these two researchers wrote a paper called "Pricing via Processing or Combatting Junk Mail." It is generally recognized as the first description of using a "moderately hard, but not intractable, function in order to gain access to [a] resource."

A. Cynthia Dowk, Moni Naor
B. Victor Miller and Mark Wegman
C. Whitfield Diffie and Martin Hellman
D. W. Scott Stornetta and Stuart Haber

Question 2

Name one of the two researchers who coined the term “proof of work” in a 1999 paper. Half point for partial answers (e.g. just first or last name)

Question 3

This mobile wallet has a "Local Trader" function within it. It is the successor to the BitcoinSpinner project. The project seems borderline defunct, but is still available for download in the Play Store.

Question 4

This biblical message was embedded in block 666,666

A. Peter 3:9 Do not repay evil with evil or insult with insult. On the contrary, repay evil with blessing, because to this you were called so that you may inherit a blessing.
B. Romans 12:21 Do not be overcome by evil, but overcome evil with good
C. Proverbs 25:21 "If your enemy is hungry, give him food to eat; if he is thirsty, give him water to drink.
D. None of the above

Question 5

This domain was registered one day before bitcoin.org

A. timechain.org
B. webcoin.org
C. bytecoin.org
D. None of the above

Question 6

What is Rusty Russell's first name? (not a DOX, it's on the wikipedia page)

A. Robert
B. Paul
C. Michael
D. None of the above

Question 7

Len Sassman maintained this piece of software (hint: randseed)

Question 8

In 2018 there was a supply chain attack against BitPay's Copay Wallet. Name the library that was compromised

A. duplexer
B. split2
C. ua-parser-js
D. event-stream

Question 9

This company was behind ASICMiner, known for producing the first ever USB powered ASIC (the Block Eruptors).

A. Butterfly Labs
B. Avalon
C. Bitfountain
D. BIOSTAR

Question 10

Theymos, the administrator of Bitcointalk, has a popular nickname. Hint: it's a handheld item.

Question 11

In the pre-release version of the Bitcoin source code, 1,000,000 sats was given a specific moniker. What was it?

A. CENT
B. BIT
C. COIN
D. NOTE

Question 12

This individual scammed users of Moolah and Mintpal exchanges. Provide his legal name.

A. Trendon Shavers
B. Ryan Kennedy
C. Zhou Tong
D. Peter Vessenes

Question 13

Bonus point: Provide the fake name he operated under.

Question 14

Stefan Thomas infamously has 7,000 BTC locked in an "armored" USB device. What is the model name of this device?

A. Secudrive
B. IronClad
C. JumpDrive
D. IronKey

Question 15

How many segwit versions can there be?

A. 62
B. 17
C. 2^{32}
D. None of the above

Question 16

Ilja Gerhardt and Timo Hanke's Homomorphic Payment Addresses and the Pay-to-Contract (P2CH) Protocol paper was inspiration for which Bitcoin soft fork?

A. Taproot
B. Segwit
C. P2SH
D. BIP-62

Question 17

In the Great Script Restoration project, a new "budget," similar to sigops is proposed. What is it called?

A. memops
B. hashops
C. varops
D. txops

Question 18

Bonus question: This budget is calculated by multiplying this number by the transaction weight.

Question 19

Name the BIP that prevents the Block 1,983,702 Problem

Question 20

Which opcode changes the number of elements on the stack?

A. OP_CHECKLOCKTIMEVERIFY
B. OP_NEGATE
C. OP_SIZE
D. OP_SWAP

credit: sipa

Question 21

How many blocks were reorged during the 2013 berkleyDB incident?

A. 24
B. 6
C. 17
D. None of the above

Question 22

This is a hash function that takes a message, a pubkey, and a random value. The function is designed so that it works as a strong hash function but the holder of the corresponding private key can produce free collisions.

Question 23

This coin was the first to implement demurrage

Question 24

What is the max_htlc_cltv value that will produce an "expiry_too_far" error in a lightning payment

A. 2016
B. 4032
C. 144
D. None of the above

credit: carlaKC

Question 25

What is the size of the payload in a Sphinx onion packet?

A. 512
B. 1300
C. 65
D. None of the above

credit: carlaKC

Question 26

Bonus question: What is the lightning network's path length limit (maximum number of hops)?

Question 27

In BOLT 8, what handshake was chosen for authenticated key exchange?

A. Noise_IK
B. Noise_IX
C. Noise_XX
D. Noise_XK

credit: carlaKC

Question 28

How many historical blocks older than its tip do network-limited (pruned) nodes serve to their peers?

A. 550
B. 2016
C. 1008
D. None of the above

credit: mzumsande

Question 29

Satoshi left which of the following quotes in the satoshi codebase

A. Never go to sea with two chronometers; take one or three.
B. Better three than two, better two than one
C. Two is one and one is none
D. The rule of three: one's none, two's one, three's two

credit: mzumsande

Question 30

Who wrote “A Declaration of Independence of Cyberspace”

A. Eric Hughes
B. Timothy May
C. John Perry Barlow
D. Adam Back