Hypothetical Problems concerning the Theory of Relativity on Cryptographic Currency Implementations

Abrahim Ladha
Computer Security
Armstrong State University
abrahimladha@protonmail.ch

***Abstract*—this is my abstract section**

I. What is bitcoin?

History Bitcoin was invented by someone using the psuedonym Satoshi Nakamoto. In his original whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System", he introduces the concept of a decentralized and crytpographically secured monetary system. He also covers topics on proof-of-work, transactions, mining, privacy, and attacks on the network. [1] It was implemented as free software and released in January 2009. Unlike gold, bitcoin has no attachment to any sort of industry, so the price day to day price fluctuation is really based on nothing but speculation. It has been as high as 1000 USD per bitcoin. [2]

Units There can only ever exist a maximum of 21 million bitcoins. Each bitcoin can be broken up into a hundred million pieces, much like a single US Dollar can be broken up into one hundred pennies. The smallest unit of bitcoin is called a satoshi, which is 10^{-8}th of one bitcoin

Ownership Since bitcoin has no central authority, transactions are made user to user. A user can only send bitcoins to another user if they can digitally sign the transaction with their private key. Without the private key, a malicious user cannot sign the transaction and the coins cannot be spent.

Transactions A transaction is a data structure with a source of funds for the input and a destination, or the output. A bitcoin transaction is just 300 to 400 bytes of data. Once a bitcoin transaction is sent, it will be validated by that node. If valid it will propogate through the nodes to which it is connected sending a confirmation to the sender. The propogation grows exponentially across the network until everyone has received the message. To prevent spamming and denial of service attacks, each node independently validates each transaction before propogating it further. A bitcoin transaction has what is called *unspent transaction output*, or UTXO. These are indivisble units of bitcoin with an associated owner. These are recognized as currency units by the rest of the network and recorded into the blockchain. an owners bitcoin amount would be scattered UTXO from many transactions and many blocks.

mining Verifying transactions take computation power which takes time, money and electricity. Mining is the incentive. Mining is the process in which new blocks are added to the money supply. Miners are the ones to validate transactions and record them on the ledger. A new block containing the transactions since the last block is mined 10 minutes on average adding those transactions to the blockchain and considered confirmed. After coins are confirmed, this allows the new owners of those bitcoins to engage in transactions. This is how the problem of double-spending coins is prevented.

II. The Theory of Relativity

history Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Postulates Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

lorentz equations Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

time travel Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Example Problem To demonstrate some of this material, we present a famous example problem. There are two planets known to be hostile towards one another, A and B which are 4.0×10^8m apart. You are in a rocket traveling at $0.98c$ relative to A and B. Your rocket follows a straight line, first past A, then B. You detect a high energy microwave signal from A and then, 1.10s later, an explosion on planet B. Clearly A has attacked B. Should you prepare for a confrontation? First we set up our reference frame. We let the rocket be stationary and the A-B planetary system moving at $0.98c$ relative to the rocket. We could have chosen another equivalent reference frame but this will make calculations simpler. let x_A and x_B denote the position of the signal from A and the explosion on B respectively, and t_A and t_B the times. Therefore $\Delta x = x_B - x_A = +4.0 \times 10^8$m, and $\Delta t = t_B - t_A = +1.10$s. We now transform the reference frame to that of A-B and calculate $\Delta t'$ and $\Delta x'$. with $v = 0.98c$, $\gamma = 1/\sqrt{1-(v/c)^2} = 1/\sqrt{1-(0.98c/c)^2} = 5.0252$. Therefore $\Delta x' = \gamma(\Delta x - v\Delta t) = 3.86 \times 10^8$m, and $\Delta t' = \gamma(\Delta t - v\Delta x/c^2) = -1.04$s. Well $\Delta t'$ is negative. What does this mean? Well $\Delta t' = t'_B - t'_A = -1.04$ seconds. This tells us that $t'_A > t'_B$ which implies that the signal happened 1.04 seconds *after* the explosion. But we witnessed the signal first, then the explosion, so which is it? If there is a relationship between these events, then information must travel from one to the other. If we check the speed of this information, we see $v_{info} = 4.0 \times 10^8$ meters / 1.10 seconds $= 3.64 \times 10^8$ m/s. But this speed is impossible since it exceeds c. Therefore neither event is dependent on the other, and these are unrelated events.

REFERENCES

[1] N. Satoshi. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System* [Whitepaper] Available: https://bitcoin.org/bitcoin.pdf

[2] M. Farrell. (2013). *What Bubble? Bitcoin Tops $1000* [Online]. Available: https://blogs.wsj.com/moneybeat/2013/11/27/what-bubble-bitcoin-tops-1000/

[3] J. K. Author. (year). *Title* (edition) [Type of medium]. Available: https://www.example.com