**EMCS2020: Advanced Topics in Computer Security**

Post-Work Assignment: How Bitcoin Works

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

***Suppose a glitch in your Bitcoin wallet software or device hardware flips (i.e., changes from 0 to 1 or from 1 to 0) a bit in the hash value associated with the address to which you are sending funds in a transaction. What happens to the funds you have sent? Will the intended recipient get them? If not, can you recover the funds or are they lost forever? Justify your answer.***

Sending Bitcoin to an address that you don’t control is impossible to “undo” and most likely will result in the loss of the coins. No, the intended recipient will **not** get funds and it cannot be reversed. Each BTC address is unique and exact. Each address also has a unique private key associated with it. Unlike bank accounts BTC cannot be stored in a secret place hidden from view. Furthermore, there is no equivalent of a bank administrator checking the transactions for accuracy. In a bank, if a wire comes in with details that don’t match any account the bank usually sends the funds back to the sender. With blockchain there is The only way to get the funds back would be if the person that owes the address to send the money back. Since there is no directory of addresses with contact information, the only hope one would have would be to send a message in a micropayment asking for funds back. Alternatively, if you are using a wallet that has a support team and you can prove that the error was not your fault the publisher of the wallet may eat the transaction.

***Explain why solving the puzzle associated with the creation of a new block in the Bitcoin blockchain is computationally expensive.***

There are two primary reasons the puzzle is computationally expensive. Firstly, the puzzle must be solved with brute force methods, which means guessing and testing millions and millions of answers before the right one is found. Second, the way BTC Blockchain mining was designed, the puzzle becomes incrementally harder ( by using bigger and bigger numbers ) with the addition of each block. Hashcash, the proof of work system, designed by Adam Beck, was designed to require computational energy from servers as a means of preventing DoS attacks and spam. “By requiring some work from the service requester, usually meaning processing time by a computer” the target service therefore makes DoS too expensive for any one server. The expense in this case is not only the computers processing time, but also the electricity necessary to execute said processing as the puzzle gets bigger and bigger.

***Argue why Bitcoin is not widely used today to pay for goods and services outside of the underground economy.***

I think the main reason Bitcoin is not widely used is that people don’t understand **what** it is, they don’t have enough money to enter the market and they don’t trust it. Most people in our modern times have come to understand and trust physical currency ( as opposed to ancient times when people traded in precious metals ). However, most of the developing world still do not use banks and by extension debit/credit cards. I worked for a company in Mexico called Payclip who offers a service . The World Bank estimates that out of 7.7 billion people on the planet 1.7 billion don’t have bank accounts. The number one reason cited was that they don’t have enough money.[[1]](#footnote-0)[[2]](#footnote-1)

Pivoting to BTC, there are very few reputable and safe ways to enter the BTC market without having a bank account. No bank account or credit card usually means no BTC wallet. This excludes the people who are relatively poor who are more populous and spend more money as a group. But it also excludes teenagers who spend a lot of money usually in cash. If businesses know that people who represent the lowest common denominator are most likely to use cash and not use BTC, they will not go out of their way to support it. The volatility of BTC and the gray area is occupies in the regulatory world poses a significant risk to business.

When it comes to organized crime and their underground activities, the lack of a bank is an advantage ( so they think ). Since all banks are regulated by federal government, banks are motivated to ( and required to ) report when their accounts are being used for criminal purposes. In the world BTC there is no oversight unless the criminals were dumb enough to use a US Based BTC wallet.

***In Bitcoin pool mining, what prevents a pool worker who has found the solution to the puzzle from taking the entire block reward themself?***

Miners in a pool communicate through a protocol called `getwork` that is confined to requesting work and sending back shares. The work in this protocol is just the Block “Header” not the entire Block. The encoded merkle root is not exposed to the miner. The merkle root requires the entire block hash. Since the miner doesn’t know the complete transaction details, just enough to contribute, they won’t be able to take the shares in the block. If the miner tries to change the transaction details they would invalidate the solution and thereby invalidate the block.

The only way to cheat would be to send back unrelated shares while withholding the real solution. In this case the miner would basically be “skimming” so they would never get away with the value of any whole block, but they would essentially have to “pay” for each block they stole. Any smart mining protocol would catch this over time.

1. Hodgson, C. (2017, August 30). The world's 2 billion unbanked, in 6 charts. Retrieved from <https://www.businessinsider.com/the-worlds-unbanked-population-in-6-charts-2017-8>. [↑](#footnote-ref-0)
2. Dinis Guarda. (April 27, 2017 Thursday). Global Findex, The World Bank's Financial Inclusion Data. IntelligentHQ. Retrieved from <https://advance-lexis-com.revproxy.brown.edu/api/document?collection=news&id=urn:contentItem:5NDP-FXM1-JCMN-Y0YC-00000-00&context=1516831>. [↑](#footnote-ref-1)