Task 1



Figure 1: Generated Identities for Parties A, B & C

The above image shows generated identities for 3 people, A, B and C. These include private keys and wallet addresses for making transactions and redeeming transactions. Once you have your private key, you can use the system to load your wallet and access your keys and address. Using your wallet, you can generate new transactions using the transaction IDs of the transactions you wish to use the outputs from, along with the public keys of the people you wish to send currency to. Transactions are stored in a compact form on the blockchain, making it space efficient, and every transaction output is marked with the relevant user’s public key.

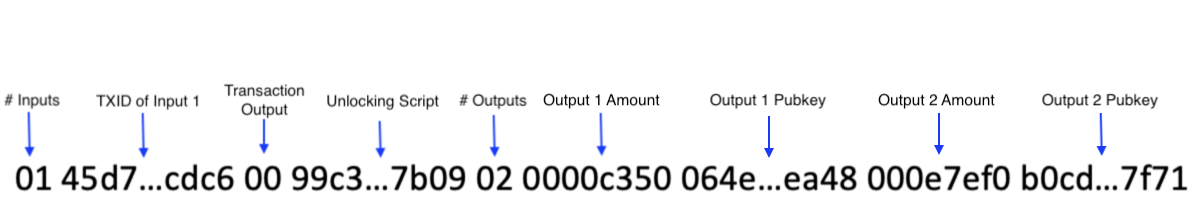


Figure 2: Structure of Transactions Stored on Blockchain

Transactions can only be redeemed with the correct private key using P2PK algorithms and ecdsa, meaning only the person with access to the relevant private key can spend the coins. All transactions are verified before being added to the blockchain to ensure double-spends and other invalid transactions cannot happen, ensuring all transactions are safe and secure. All transactions on the blockchain can be viewed by anyone, meaning they are transparent. Merkle hash trees are used to verify the integrity of transactions on the blockchain, so you can check that none of the transactions have been tampered with. Since these are stored in the block header, any changes to the Merkle root indicating changes to the transaction list would alter the hash of the block, automatically removing it from the chain.

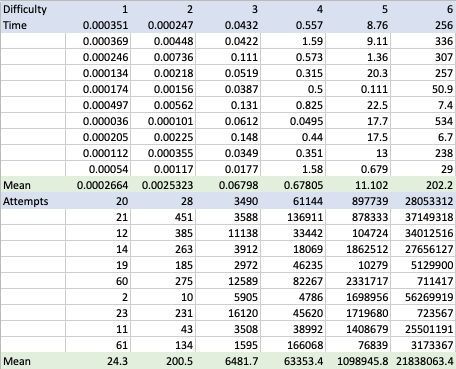
The results from the tests are shown in the table below.

Figure : Results from Testing Time and Attempts for Block Mining

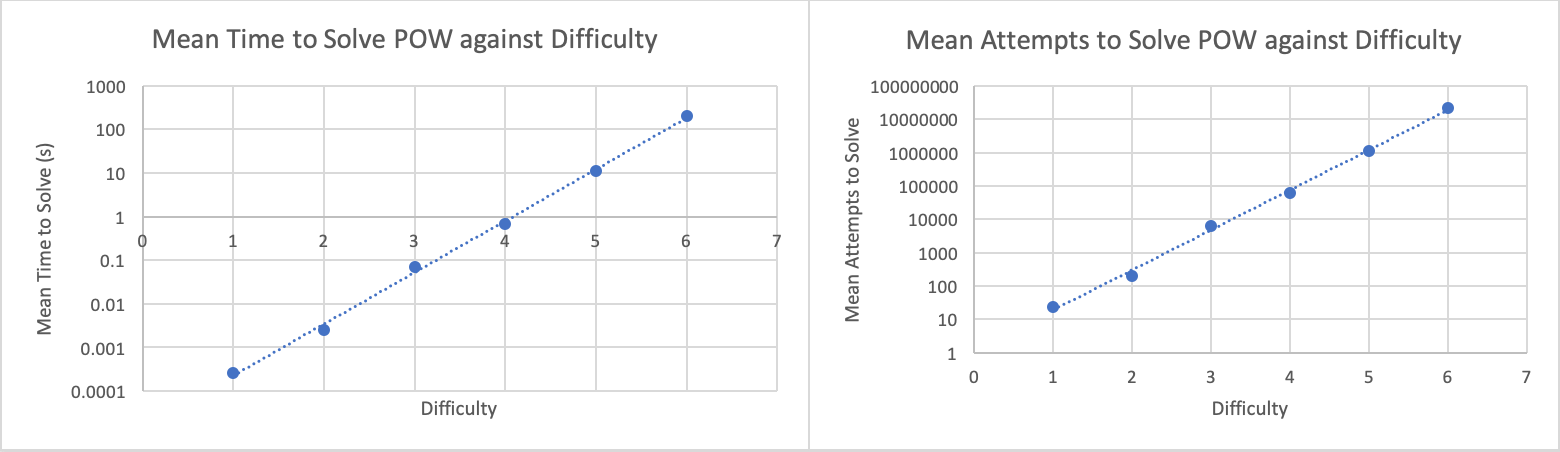
These results can also be seen plotted on the two graphs below. The Y-axis is logarithmic, to show the differences between each step more clearly, and a trendline has been added to show the time and attempts increase in a roughly exponential fashion as the difficulty increases. 

Figure : Graph showing results displayed above. Exponential relationship is shown by trendline.

Unfortunately, my machine was only able to mine blocks up to a difficulty of 6. The machine I was using has an Intel Core i7-3520M, from 2012, and 8gb of RAM. If I were to continue the tests to difficulty 7 and the exponential relationship were to continue, it would probably have taken 8-10 hours to complete. With a given maximum nonce value of 100,000, you would expect the system to only be able to mine block up to difficulty 4. This is because 100,000 is 186A0 in hexadecimal, which is a 5 digit number. If we were to assume the hash value would be unique for every possible nonce, it is possible that we could exhaust all 100,000 possible nonce values and not find once which results in the hash having 5 leading 0’s, since if the first 5 values were unique for every nonce, we do not have enough nonces to cover every possibility for the first 5 digits.

Task 2

I studied block 93036 on the BTC block chain, which received 622,383 confirmations and was mined on 20/11/2010. The difficulty for mining this block was 6,866.90, whereas the mining difficulty on the date which I accessed the block (21/12/2021) was 24,195,286,980,613.62. This is 3,513,233,382.31 times more difficult, which shows that the hash rate of the BTC network has increased massively since November 2010. The log of this number in base 2 is approximately 31, meaning the difficulty has doubled 31 times in about 11 years. Compared to Moore’s Law, which posits that computing power should roughly double every year [1], this increase is clearly far larger than what should be attributed to increases in computing power alone. This shows how significant the increase in popularity of bitcoin has been since 2010: if we look at changes in price between these two dates, we see the price has doubled roughly 17 times, which confirms that most of this increase in difficulty can be attributed to increased popularity rather than advances in computing power. The block reward was 50 BTC, which would have been worth £8.88 at the time but would be worth £1,838,762.51 on the date accessed. Two transactions in this block were 650168cf2c0111fa4fd6589f621cd1980b3c439983c72dfed9946853124935ae (<https://www.blockchain.com/btc/tx/650168cf2c0111fa4fd6589f621cd1980b3c439983c72dfed9946853124935ae>) and 3356edd82fdeea8c7a57e1b828dcef558a0d36e092486bc9eb261075f43bd28b (<https://www.blockchain.com/btc/tx/3356edd82fdeea8c7a57e1b828dcef558a0d36e092486bc9eb261075f43bd28b)>. The block reward was sent to the address 1ENDYyEEXqdhKTM2pmhLghtq4NAkvgSNAU. The first transaction at this address was the coinbase transaction from the mining of the block with the hash da2cc47a9bd590b3e3741f730045b82513c28d49463a47622430d0b32627a7f8, receiving the block reward of 50 BTC. Another transaction involving this address happened on 01/02/2021 with hash 621a5b844bc602388adff93237cc86ee0bccd334d72ee8c0012c439b03f2f698, where they received 0.00000547 BTC from bc1qw7wg6mk352uetqyelcs35szqa9389hzg57qxkt. There were 314 recipients in this transaction, with 1.64234928 BTC being sent in total. The fee for this transaction was 0.00264275 BTC.

For John’s bitcoins, the ScriptSig script that can be used to redeem the transaction is <blockchain and cryptocurrencies>.

Password isn’t a secure way to store bitcoins, since to redeem the transaction the password will have to be put on the blockchain in plaintext, meaning it will be visible to anyone, so he cannot use the password more than once. Additionally, someone could guess the password by hashing strings until they match the locking script, which could be easy if his password is not very secure. P2SH would fix this security issue as a script is hashed, not a password. This script contains a public key with a corresponding signature using ECDSA. This would be much harder to brute force as a script involving signatures would be typically a lot less “guessable” than passwords, and since the private key is not revealed in the script it can be reused unlike the password.

The updated script for John’s bitcoins is a P2SH script using multisig, which requires 2 signatures from 2 private keys. John could keep 1 private key and give the other to a trusted third party, and when redeeming the transaction, he can ask them to send him the relevant signature. This means that if his private key is compromised, the attacker still can’t redeem his bitcoins.

Task 3

The first step is to install the Metamask browser extension. Links to versions for different browsers can be found at <https://metamask.io/download.html>. Metamask provides us with a wallet to store Ethers in so we can deploy contracts on the blockchain over the Ropsten test network. After installing the extension, it will walk you through creating a new wallet. After creating a wallet, we must switch from the Ethereum main network to the Ropsten test network, since we don’t want to spend actual Ethereum and waste space and resources on the blockchain when testing and developing contracts. To do this, navigate to Settings => Advanced and then toggle ‘Show Test Networks’. Once you have done this, you should be able to switch to the Ropsten test network, as shown in the series of images below.

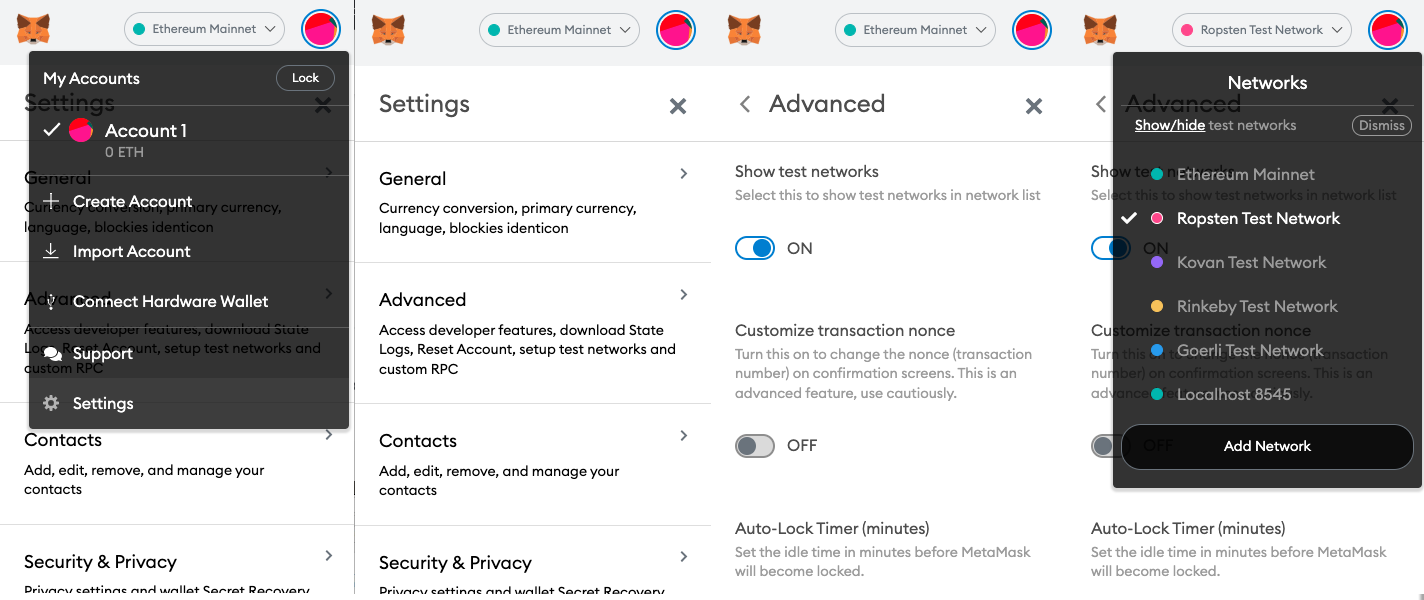


Figure 5: Steps to change from Ethereum Mainnet to Ropsten Test Network

Once you have a wallet, you can load test ethers into it by visiting a test ether faucet, such as the one at <https://faucet.metamask.io/>.

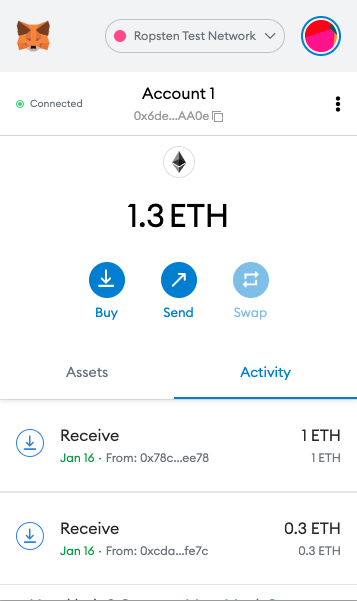


Figure : Wallet containing 1.3 Test Ethers.

Once we have some test ethers, we can experiment with deploying our smart contract on the blockchain. We can do that directly through Remix IDE or we can do it locally using Ganache by setting up a blockchain on our system. When doing it over Remix IDE, the gas cost for deploying the transaction was 466,033, which is 0.000466033 ether or 466,033,000,000,000 wei, compared to using ganache, where it was only 248,842 gas, which is 0.000248842 ether, or 248,842,000,000,000 wei. This could be because the ganache blockchain is hosted locally, so does not have to be deployed over the internet.

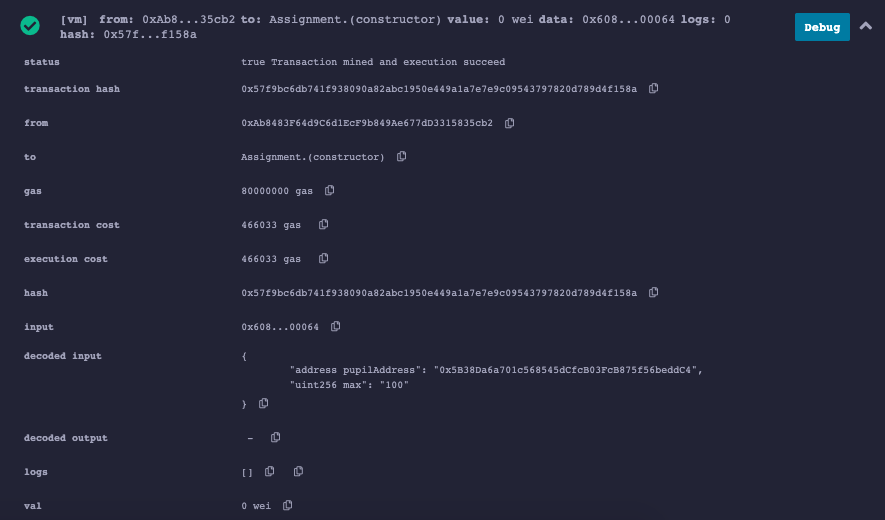


Figure : Transaction Details for Deploying over Remix IDE



Figure : Transaction Details for Deploying over Ganache

Task 4

My chosen cryptocurrency is Ada, the cryptocurrency related to the blockchain platform Cardano which was launched in 2017 by Charles Hoskinson, one of the co-creators of the Ethereum cryptocurrency. It was developed to be faster, more scalable and more efficient than existing currencies like Bitcoin, using a proof-of-stake consensus algorithm called Ouroboros as opposed to Bitcoin which uses a proof-of-work algorithm. This makes it significantly greener due to lower energy usage, and much like Ethereum, the Cardano system has the functionality to deploy smart contracts and dApps on the blockchain with its own turing-complete Plutus programming language, [2] making it useful as a platform as well as a currency. It is the largest cryptocurrency to use proof-of-stake, with a market cap of over $36 billion as of February 2022 [3].

It has clearly been successful in its aims: the average block time is 10-20s, meaning a transaction should only take 20s - 10 minutes, much faster than Bitcoin at 10mins – 1 hour [4]. It is far more scalable, too, since the consensus algorithm doesn’t require large amounts of computing power to be set up to mine blocks, it simply requires users to stake their currency to be given a chance of mining the next block. The faster block time also means transaction throughput is far higher, with max TPS (transactions per second) expected to reach 500-1000 in 2022 [5], and plans for a new Hydra scalability protocol which could in the future increase throughput up to 1,000,000 TPS [6], an enormous amount compared to Bitcoins 7 TPS [7]. In addition, its energy usage is significantly lower than bitcoin: in 2021, Cardano was estimated to use 6GWh of energy annually, less than 0.1% of Bitcoin’s enormous 110.53 TWh, with Cardano’s network using an estimated less than 1% of the energy per transaction than Bitcoin [8].

Ada is mined through a proof-of-stake algorithm, which requires users to “stake” coins from their wallet for the chance to mine blocks. The more currency a user stakes, the larger the chance of them being allowed to mine the next block and receiving coins as a reward. Users can also ‘pool’ their currency together to have a larger chance of being selected, sharing the rewards between themselves [9]. Security is kept through consensus, with at least half of users currently staking having to agree on a block for it to be mined, and its security is ‘mathematically verifiable’ [9]. However, this does mean that it is still vulnerable to the 51% attack, like Bitcoin.

Despite this, no major security flaws have been identified within the Cardano system. They have adopted a bug-bounty system, with people being encouraged to report any bugs found to Cardano’s parent company, Input Output Hong Kong, where they may be rewarded up to $10,000 [10], and with their design mantra of letting formal theory precede practise (the Cardano foundation has produced over 40 academic papers since 2015 [11]), it is likely it will continue to be a reliable and secure cryptocurrency platform.

Bibliography

[1] Britannica, The Editors of Encyclopaedia. "Moore's law". Encyclopedia Britannica, 26 Dec. 2019, <https://www.britannica.com/technology/Moores-law>. Accessed 23 December 2021.

[2] Anthony Cuthbertson. “What is Cardano? The “Green” Crypto that Defied Musk’s Bitcoin Crash – and Hopes to Surpass Facebook and Netflix”. Independent, 18 May 2021, <https://www.independent.co.uk/life-style/gadgets-and-tech/cardano-crypto-bitcoin-elon-musk-b1849021.html>. Accessed 01 February 2022.

[3] CoinMarketCap, <https://coinmarketcap.com/currencies/cardano/>. Accessed 01 February 2022.

[4] Capital.com Research Team. “Cardano vs Bitcoin: Which is the Better Asset to Buy in September 2020?”. Capital.com, 04 September 2020. <https://capital.com/cardano-vs-bitcoin>. Accessed 01 February 2022.

[5] Siamak Masnavi. “Cardano ($ADA) Whale: ‘Transactions per Second Should Scale to 500-1000 this year’”. Cryptoglobe.com, 19 Jan 2022, <https://www.cryptoglobe.com/latest/2022/01/cardano-ada-whale-transactions-per-second-should-scale-to-500-1000-this-year/>. Accessed 01 February 2022.

[6] Cardano Team. “Hydra: The Multi-Headed Scalability Protocol”. summit.cardano.com, <https://summit.cardano.org/sessions/hydra-the-multi-headed-scalability-protocol>. Accessed 01 February 2022

[7] Jeffrey Craig. “What is Transactions Per Second (TPS): A Comparative Look at Networks”. Phemex.com, 02 Nov. 2021, <https://phemex.com/blogs/what-is-transactions-per-second-tps>. Accessed 01 February 2022.

[8] Jonathan Ponciano. “Cardano Surges During $300 Billion Crypto Crash as Musk Eyes Sustainable Bitcoin Alternatives”. Forbes.com, 13 May 2021, <https://www.forbes.com/sites/jonathanponciano/2021/05/13/cardano-surges-during-300-billion-crypto-crash-as-musk-eyes-sustainable-bitcoin-alternatives/?sh=57a9d273259e> . Accessed 01 February 2022.

[9] The Cardano Team, “Ouroboros”. Cardano.org, <https://cardano.org/ouroboros/>. Accessed 01 February 2022.

[10] King kamsi, “ADA Security Flaws Are Being Investigated by The Cardano Foundation”. Dogecoinnewshub.com, 04 Sept. 2021, <https://dogecoinnewshub.com/crypto/ada-security-flaws-are-being-investigated-by-the-cardano-foundation/>. Accessed 01 February 2022

[11] Undersearcher, “How Secure is Cardano?”. Medium.com, 26 Jan 2019, <https://medium.com/@undersearcher/how-secure-is-cardano-5f1e076be968>. Accessed 01 February 2022