Blockchain and Cryptocurrencies Coursework

pbqk24

March 22, 2019

1 Mining Puzzles

1.1 Proof of Work

The requested information for Proof of Work is as follows:

Index	Information	Value
1	User ID	pbqk24
2	Block hash target calculated (hex)	000003e7fc18000000000000000000000000000000000000000000000000000000
3	Nonce value (int)	2171906
4	Number of (double) hashes performed	2171907 (one per nonce tried, starting at 0)
5	Estimate for mining time for difficulty = 1 Estimate for mining time for difficulty = 7454968648263	58629 seconds $4.37 * 10^{17}$ seconds

Table 1: Mining Puzzles: Information Requested

The equations used for calculating the mining time estimates t are as follows:

$$target = \frac{target_{initial}}{difficulty} \tag{1}$$

$$h_q = \frac{h_{space}}{target} \tag{2}$$

$$t = h_q * t_h \tag{3}$$

Where h_q is the estimated number of hashes required to be performed to find a valid hash, $target$ is the target value, t_h is the estimated time per hash calculated by timing how long it takes to perform a large number of hashes (e.g. 10^9) and finding the average. t_h was computed as $1.365 * 10^{-5}$ and used for both calculations.

For difficulty of 1:

$$target = \frac{00000000FFFF0000000000000000000000000000000000000000000000000000}{1}$$

$$h_q = \frac{2^{256}}{00000000FFFF0000000000000000000000000000000000000000000000000000} = 4295032833$$

$$t = 4295032833 * 1.365 * 10^{-5} = 58629$$

For difficulty of 7454968648263:

$$target = \frac{00000000FFFF0000000000000000000000000000000000000000000000000000}{7454968648263} = 3.62 * 10^{54}$$

$$h_q = \frac{2^{256}}{3.62 * 10^{54}} = 3.2 * 10^{22}$$

$$t = 3.2 * 10^{22} * 1.365 * 10^{-5} = 4.37 * 10^{17}$$

Index	Information	Value
6	ECDSA public key (hex)	4f045a6cfacb3e67e7c5d4ddfb9f1acfe7d6ddda c29869734cce5218cdab24e2d2cc72601138d6f 324464df7691f819cd14e8b3752d9c463e5162a ad37393ca0
7	Signature of "Hello world" (hex)	eae12ab8fdbeb5635ac45edbfceb999907a5b090 42eeddbd9a07a744f656b3ac7e00124086256e5 caf86539e68186742d593e5e8b537b9f6d7ee055 57c2ef68a
8	Signature used in calculating hit (hex)	aa2974089248c51977f63350c3aad2757b935d68 a236dd777621c3ed879657d2c5e1f01d22ad16b b2d37f1c2567d1daeccd4e3f1a45201f53291e2e ba9e9bea3
9	Hit value (hex)	a135a0781dd3c0f6
10	Time (s) that you could forge a new block	394

Table 2: Mining Puzzles Information

1.2 Proof of Stake

The requested information for Proof of Stake is as follows:
The equations used for calculating the hit value are as follows:

$$hit_{full} = hash(sign(S_g)) \tag{4}$$

Where the hit value is the first 8 bytes of hit_{full}, and S_g is the generation signature for the previous block:

$$S_g = 9737957703d4eb54efdff91e15343266123c5f15aaf033292c9903015af817f1$$

$$sign(S_g) = aa2974089248c51977f63350c3aad2757b935d68a236dd777621c3ed879657d2c5e1f01d22ad16bb2d37f1 c2567d1daeccd4e3f1a45201f53291e2eba9e9bea3$$

$$hash(sign(S_g))[:8] = a135a0781dd3c0f6$$

The time in seconds when you would be able to forge a new block was calculated using the following equations:

$$T = T_b * B_e \tag{5}$$

$$t_{forge} = \frac{hit}{T} \tag{6}$$

Where T is the target value (independent of time passed), T_b is the base target value, B_e is your effective balance, and t_{forge} is the time when you can forge a new block (rounded up, in seconds):

$$T = 1229782938247303 * 24 = 29514790517935272$$

$$t_{forge} = \frac{11616367251628998902}{29514790517935272} = 394$$

2 Interacting with bitcoin-testnet

The requested information for Task 2 is included in Table 3 and 4 below.

Index	Information	Value
1	User ID	pbqk24
2	blockchain.com links	This is included in Table 4 below
3	Transaction explanations	This is included in Table 4 below
4	bitcoin-testnet address	mvcM9NV5hesnSUNpZGZ9Pyt3PK8xDFmCTp
5	100 Satoshi Tx ID chain.so hyperlink	bfb4090faca08fe0f1ca46883cef1bf7e7860a4df6637acb7962741db0206f29 https://chain.so/tx/BTCTEST/bfb4090faca08fe0f1ca46883cef1bf7e7860a4df6637acb7962741db0206f29
6	Proof of Burn Tx ID chain.so hyperlink	611186bc95e29fc70127fce35bd9c8a7f86c46f00aecd9df4765731d27f64d31 https://chain.so/tx/BTCTEST/611186bc95e29fc70127fce35bd9c8a7f86c46f00aecd9df4765731d27f64d31
7	Hex used as script Explanation of hex script	6a067062716b323 This script is equivalent to 'OP_RETURN 06 7062716b323'. This causes the transaction to always be marked invalid, as OP_RETURN always outputs *fail*. The '06' signals that the next 6 bytes are to be pushed onto the stack, and '7062716b323' is the result of converting 'pbqk24', my USER ID, from ASCII to hex.

Table 3: Bitcoin-Testnet Information

Tx	Aspect	Explanation
1	blockchain.com link	https://www.blockchain.com/btc/tx/6c260da65fe98b08b27b80f8481c6f0ae34252921f6c34d327172472c5b419d7
	Input scripts	There is no input script since the coins are newly generated.
	Output scripts	There are three output scripts: one specifying the receiver of the mined bitcoin, one using OP_RETURN to push data onto the blockchain (not decodable as text), and one that seems to have produced an error when decoding the script (but similarly to the second one, it transfers no coins).
	Inferences from structure	This is a transaction claiming the mining reward of (at the time) $\sim$ 12.6BTC (including transaction fees). This can be inferred as there is no input script, thus this transaction is the miner's claiming their reward.
2	blockchain.com link	https://www.blockchain.com/btc/tx/4a3751b29128bea458f7f07d4f92b29322ba1900bbc364130bf2648e73f8cfad
	Input scripts	There is a single input script, which includes a witness.
	Output scripts	There are a large number of output scripts, most simply checking the hash of the receiver's address is valid, and a few additionally verifying and checking the signature.
	Inferences from structure	As this transaction has a single input, multiple outputs, and pays a large sum ($\sim$ 1.7 BTC), I suspect that this is payout from a mining guild, or possibly a sale of bitcoin by an exchange.
3	blockchain.com link	https://www.blockchain.com/btc/tx/496cda9b0f4083b7775822f07a1541176866947b9f93006752de029489e1abd6
	Input scripts	This transaction contains a large number of input scripts. Most of these have a small input amount, with three being notably large: $\sim 1, \sim 4.3$, and $\sim$ 25 bitcoin. All input scripts are from the same address.
	Output scripts	The transaction contains two output scripts. One claims $\sim$ 13.2 BTC, and the other 22.5 BTC.
	Inferences from structure	Due to the amounts involved, and the exact payment of 22.5 BTC to the second output address, I suspect that this transaction is a user selling BTC to an exchange. This is supported by investigating the recipient address of the 22.5 BTC, which shows it being involved in numerous high-value transactions, where the address seems to mainly be used as a middle man, often transferring the exact input amount onwards to another address.

Table 4: Bitcoin-Testnet Transactions Details

3 Investment Advice: Bitcoin, NXT or Gold

The judgment of what to invest in depends on your reasons for investing. Firstly, if you are investing to maintain value then gold would be the best candidate. The value of gold rarely fluctuates, and it has some value as a material outside of being used as currency. It is also the most durable of these options, as it is not reliant on any technology or network in order to have worth and be useable. Even in extreme circumstances such as financial collapse, gold will maintain value as a currency, while any cryptocurrency may see its value plummet or become invalid due to collapse of its network or userbase.

If you are investing for short-term returns, then NXT is a good candidate. Over the past few months both Bitcoin and NXT have started to increase in value [1]. Out of these two NXT has risen faster, and due to its technical advantages over Bitcoin, such as using Proof of Stake rather than Proof of Work making it less wasteful to operate and more expensive to attack, and its ability to trade any asset on its network, it has more utility than Bitcoin. This theoretically gives NXT an edge over Bitcoin, meaning it should steal market share and users from it over time. However, will not necessarily happen due to the popularity of Bitcoin. Even though Bitcoin is an inefficient and outdated cryptocurrency, the fact that it was the first to gain widespread popularity and support cannot be ignored. It currently holds the largest market cap of any cryptocurrency, and is unlikely to lose popularity quickly [1].

Additionally, there is a large number of cryptocurrencies available, most of which have at least some technical merits over Bitcoin, and some of which are improvements on NXT, which NXT is competing with as well. This means it is extremely unlikely for NXT to become a true Bitcoin equal, and its value is likely to stay volatile. This means that investing in NXT could see short-term profits, but these are unlikely to be sustainable in the long-term.

The popularity of Bitcoin may also be a detriment when it comes to investment, however. Due to its technical shortcomings, Bitcoin can only process a handful of transactions per second, with long delays before a transaction is confirmed. This means that the more popular the cryptocurrency becomes, the more expensive transactions will become due to fees needed to ensure the transaction is confirmed within a reasonable time period. This will likely cap the potential market cap and value of Bitcoin in the future, which limits its investment opportunities. Even worse, this effect may result in people becoming aware of its technical shortcomings, and moving to other cryptocurrencies, leading to a massive crash in users, market cap, and value.

Because of the reasons outlined above, I would recommend investing in Bitcoin for potential profit, and gold for maintaining value. Due to the large number of competing cryptocurrencies, and small current market cap, I would not recommend investing in NXT [1].

4 An analysis of XRP (Ripple)

4.1 Idea and Justification for Creation

XRP, commonly referred to as Ripple, is a decentralized cryptocurrency used as part of the XRP Ledger. It was initially released in 2012, intended as a currency exchange and transfer system for financial institutions [2]. Ripple Labs Inc., the developer of XRP, uses it as part of their solutions and offerings to financial institutions. The idea behind its creation was to allow fast, cheap, and reliable international transactions, which currently can take up to 5 business days and cost as much as 6% in commission fees [3]. Any currency beyond XRP can be represented and traded on the XRP Ledger as 'issued currencies,' which can be traded for each other or for XRP, and can represent any item, not just traditional currency.

4.2 Technical Differences to Bitcoin

XRP differs significantly from Bitcoin in many regards. Firstly, unlike in Bitcoin and many other blockchain technologies, nodes do not need to store the entire history of the blockchain in order to track its current state. XRP uses a ledger system, where each ledger stores the entire current state of the system [4]. This means that the cost in terms of storage for each node is reduced. Every ledger is produced by a set of transactions that are applied to the previous ledger. The new ledger is then summarized using a hash tree and compared across the nodes [5]. A consensus is reached using the XRP Ledger Consensus Protocol (XRP LCP), which ensures that all nodes agree on the set of transactions, and a transaction processing protocol that is followed by each node to produce the same ledger based on this set [6]. The XRP LCP is designed to ensure that all users of the XRP Ledger reach an agreement on the state of the ledger, all valid transactions are processed, transactions can be processed even if some participants are missing or behaving nefariously, and to avoid requiring large amounts of resources to be spent [4]. This is a key difference from Bitcoin, which requires massive amounts of processing power (and thus energy) to be spent for each new block to be produced.

In Bitcoin, anyone can set up a system to begin mining and be a part of creating the next block. XRP differs from this in that it uses validated servers to reach the consensus to produce the next ledger. Only trusted servers, those present in a participant's Unique Node List (UNL) are considered when determining if a given transaction or ledger is valid. While participants can freely choose which servers are in their UNL, Ripple Labs publishes a recommended UNL. This presents a barrier to entry for any party wanting to join the consensus system, and makes XRP much less decentralized than Bitcoin and other cryptocurrencies.

Another major difference between Bitcoin and XRP is in the transaction fees. In Bitcoin, transaction fees are voluntarily added by the source of the transaction, and any fees included in transactions in a mined block can be collected by the miner in full. In practice, transaction fees are mandatory if a user wants their transaction included within a reasonable amount of time. The typical transaction fee is completely controlled by market forces and varies with the network congestion. For reference, the estimated fee for a transaction to be included in the next block at the time of writing was $\sim$ \$0.30 [7]. On the other hand, XRP has a mandated minimum transaction fee of 0.00001 XRP per transaction built into the protocol (at the time of writing this was equivalent to $\sim$ \$0.0000031). Additionally, this fee is burned, rather than being collected as in Bitcoin. The minimum transaction fee scales with the current load on the network. In XRP, this transaction fee serves two purposes: firstly, it discourages attacks on the network attempting to overload it with transactions, both intentional and unintentional. Secondly, in burning the XRP paid for the fee it makes all remaining XRP more valuable [8]. This makes XRP a deflationary currency, as there is a finite supply of the coin.

In addition to the differences above, XRP is also much faster and has a higher throughput than Bitcoin. The XRP Ledger is one of the fastest blockchains currently, being able to confirm a transaction in under four seconds [9]. Bitcoin, on the other hand, can take longer than an hour before a transaction is considered confirmed, as a transaction is usually only considered to be completed when it has been present in several consecutive blocks. XRP can currently handle up to 1500 transactions per second, giving it a much higher transaction capacity than Bitcoin, which can only process $\sim$ 7 transactions per second [10]. This makes XRP much better suited as a transaction processing system and currency than Bitcoin. Additionally, according to Ripple Labs XRP has the capability to scale to handle as many transactions per second as Visa (50000) [11].

4.3 Mining Ripple

Unlike Bitcoin, Ripple is not designed to be mined, and no reward is given to nodes for helping produce the next ledger [12]. 100 billion XRP were initially created by its creator, Ripple Labs, and no new XRP can ever

be created. Out of these, roughly 38 billion are currently available with the rest being held by Ripple Labs, most of them in escrow to be released at a rate of 1 billion per month [2]. This also means that there is no financial incentive to operating a validator server, as there is no reward in XRP for doing so. Instead, the reward given to validators is in being a part in controlling the network, and deciding on the future evolution of the network. Ripple Labs' justification for this being a viable system is that the only cost to running a server is the electricity it consumes, which is extremely low compared to a Bitcoin mining rig - roughly equivalent to running an email server [13]. In addition to this, institutions or individuals that rely on the XRP Ledger, for example for financial transactions, are incentivised to operate servers in order to ensure its reliability and stability. If already runnning a server, the additional cost to run a validator is negligible [13]. However, this design also further reduces the extent to which XRP is decentralized.

4.4 Performance

Despite its technical advantages over Bitcoin, XRP has failed to outperform the more popular coin. It briefly held a price of $\sim$ \$0.2 per XRP for the second half of 2017, before rapidly climbing to a peak value of \$3.84 in early 2018, and rapidly falling down to just below \$1. Since this peak, the price of XRP in USD has been on a slow but steady decline. Bitcoin has similarly been declining after a massive peak in price around the same time, but has seen a small increase in the last month which XRP has failed to mimic. XRP currently holds a fairly stable market cap of $\sim$ \$13 billion, while Bitcoin is at nearly \$80 billion [1].

While XRP is not performing as well as Bitcoin recently, compared to the general cryptocurrency market it is performing favourably. It remains at the number 3 spot in terms of market cap, being only \$1 billion behind Ethereum at number two, and comfortably $\sim$ \$9.5 billion ahead of Litecoin at number four. Additionally, most cryptocurrencies have seen a small slump over the past few days, which XRP has begun to recover from faster than many others.

4.5 Notable Attacks and Events

Ripple has so far mostly managed to stay out of the limelight and has not been the victim of any major attacks. According to Ripple Labs' CTO David Schwartz, this is because of the consensus protocol used in the XRP Ledger, which makes it immune to '51%' attacks that many other cryptocurrencies have suffered from [14]. However, this does not mean that XRP is without controversy. One common source of worry is the fact that Ripple Labs owns $\sim$ 60 billion of the 100 billion XRP in existence. Most of these ($\sim$ 55 billion) are locked in escrow accounts, scheduled to be released 1 billion per month over the next 55 months. Ripple Labs have stated that the reason for their holding this many XRP is to incentivize the company to continue development of XRP Ledger to the best of their ability [13], but many users worry that this gives them extreme powers over the cryptocurrency, breaking the principles of decentralization. For example, Ripple Labs have the ability to drastically affect the price of XRP by releasing a large amount of their holdings, at any time [9]. Another source of worry is the design choices limiting decentralization discussed previously, such as most validated servers being controlled by financial institutions. This goes against a common drive behind interest in cryptocurrencies and blockchain: independence from banks and governments.

A major event that affected XRP occurred in May of 2018, when Ripple Labs was named in a lawsuit filed in the state of California, USA. This lawsuit alleged that Ripple Labs ran a scheme to collect hundreds of millions of dollars by generating XRP and trading them in unregistered sales in a "never-ending initial coin offering" [15]. The lawsuit is based on the idea that XRP tokens act more like stock for Ripple Labs than a traditional cryptocurrency, and as such should be subject to more strict controls and regulations [16]. As of November 2018, the lawsuit is still ongoing.

4.6 Assessment of XRP and Conclusion

While XRP has many technological advantages over Bitcoin, such as drastically faster transaction confirmation speeds and higher transaction throughput, many design choices that contribute to these feats may severely restrict its potential as a cryptocurrency. Although XRP technically is a decentralized cryptocurrency, in practice this ideal is violated by the fact that Ripple Labs control $\sim$ 62% of all XRP, and that ledger consensus is carried out by a select few parties, and there are large barriers to becoming one of these parties. Lastly, while many see XRP's connection to Ripple Labs and their financial services as a positive regarding its feasibility and stability, XRP is not necessary to the operation of the XRP Ledger due to the issued currencies mentioned earlier. Thus, this connection has no impact on the utility and value of XRP as a cryptocurrency.

References

[1] CoinMarketCap, "Top 100 cryptocurrencies by market capitalization," 2019.

[2] Finder.com, "What is ripple? a step-by-step guide to XRP," 2018.

[3] J. Bushmaker, "The top 50 cryptocurrencies," 2018.

[4] R. Labs, "Intro to consensus," 2013.

[5] S. Gordon, "What is ripple?," 2018.

[6] B. Chase and E. MacBrough, "Analysis of the XRP ledger consensus protocol," *CoRR*, vol. abs/1802.07242, 2018.

[7] C. Lizarraga, "Bitcoin transaction fees," 2019.

[8] R. Labs, "Transaction cost," 2018.

[9] J. van Zwanenburg, "What is ripple (XRP)?," 2018.

[10] Blocksplain, "Blockchain speeds & the scalability debate," 2018.

[11] R. Labs, "XRP: The digital asset for payments," 2019.

[12] cointelegraph.com, "Ripple vs. bitcoin: Key differences," 2019.

[13] R. Labs, "Technical faq," 2018.

[14] N. Chong, "Ripple CTO claims XRP eliminates PoW risks seen in Ethereum Classic's 51

[15] L. Katz, "Ripple hit with class-action suit over 'never ending ICO'."

[16] B. Brown, "Why is ripple in court over XRP? (the lawsuits, explained)," 2018.