Book Chapter 4 Review

Overall it was a good introductory text, but in the interest of being accurate, I've listed the following items. Items in each section are ordered based on their appearance in the chapter.

0.1. **What parts are not clear?** Page 3, "The authority to confirm has been given to an incorruptible entity: the time itself." While this sentence has a poetic sense to it, I think it would be inaccurate to say this. It would be more accurate to mention that the authority to confirm has been given to the whole network, a transaction is confirmed only if the majority of the network agrees on it.
Page 3, Bitcoin properties seem out of place, it would be nice to have an introduction before it.
Page 3, "The system cannot require every node to obey these rules to function properly." I'm not sure what is meant by this sentence. I would rewrite this paragraph as: "Each entity in Bitcoin assumes a common set of rules to be obeyed. But since there are no regulations to enforce these rulesets and there are misbehaving entities in the network, lawful users should easily identify those who do not follow the rules and ignore them. Furthermore, disobeying the rules is costly and therefore the rational user would see there is more financial gain in following the rules than breaking those."
Page 9, there is a question about P2SH transactions, I consulted the code base, basically, the receiver of a P2SH doesn't do anything upon receiving it, the scriptPubKey is stored in the output on the blockchain. When the user wants to spend the output of a P2SH, they have to provide all of the inputs as well as the script itself in the scriptSig field, other nodes hash the script to ensure that it matches the scriptPubKey and then run it to ensure the user has the right to the coins.

0.2. **Are there any mistakes in the text?** Page 3, "If a fully connected network was possible, users would communicate with each other about how many coins they own, and balance information could be confirmed by asking everyone in the network", I think this is misleading, although the text is technically correct, there are still many problems in such networks, since this is a trust-based system, i.e., there aren't any proof of fund presented. Nakamoto's white paper briefly touches upon these troubles. I think it would be better to include the fact that their transactions could be broadcasted, and a transaction and fund could be confirmed by asking everyone in the network. One possible problematic scenario would be when a user A claims that user B must send him funds and half of the network agrees and half disagrees, possibly due to user B being mischievous, with transaction information provided the network would look at the signature and approve/disapproves.
Page 5, "Public/private key generation is a cheap process that can be done easily by using services online", I believe this to be misleading since public/private key generation could be even done on paper, CLI, or GUI tools without access to any online service.
Page 5 claims the addresses are unique, they are pseudo unique, the author's next sentence correctly explains why they are pseudo unique, but a false name is given to them.
Page 7, I think it was meant to say M/0/0, ..., M/0/11 and M/1/0, ..., M/1/4 (both major and minor for second range should change). In case it is meant to have a zero-based number followed by a one-based number, the second range's major number should still be different, otherwise, it would be address-reusing which is a discouraged practice.
Page 18, "miners change the hash of previous block with hash of b, and resume their mining efforts", this is inaccurate as miners also update their transactions in case they are included in the mined block

0.3. **Are there anything missing from the discussion?** Page 2, Would be better to mention what a ledger is before calling blockchain a distributed ledger. I would show the difference between a database and ledger, "Traditionally ledgers are books used to total the economical transactions. In a software sense, a ledge is a type of software for storing data, similar to a database, where the data could only be appended and there are no delete or update operations allowed."

Page 4, the hash analogy to personal names could be improved by providing an example that is a more clear hash. First of all, technically speaking names are varying lengths so they aren't hashes unless they are padded with whitespace or shortened to a fixed length. A better example would be using the first letter of everyone's name or their initials. The collision is more apparent, and the length criteria are also met.

Section 4.8 would benefit from including incentives for including a transaction with zero or low transaction fees, as covered in the Kaldoner paper in week 1.