Comments on Donation Platform Final Report (Draft) – 15 May 2020

(Page numbers refer to the PDF file.)

Title page - "Group 39" (otherwise it's not clear what the 39 is!)

p4 "Dr. Richard Piacentini, a DLT expert from Sharkaroo.com"

p 8 Format/indenting of Table of Contents is inconsistent
Chapter 5 should be "Conclusions"

p13 "In the real world, donors never know whether money that they transfer will reach the destination or the beneficiary."

p15 Remove the comment about "different currencies" from the scope (since right now it's just lumens/baht)

p19 Remove "Test result from users" since I don't think you will have time for this. (If you do plan to do this... need to hurry!)

p 22 I think you need to explain the term asymetric. For instance "'Asymetric' when applied to cryptography means unequal or non-equivalent. The term highlights the difference in visibility between the public key which everyone can see, and the private key which is secret." Put this after the first sentence in the second paragraph.

P 23 "Figure 2.3 shows the process of how the asymmetric cryptography works. "
"to do an identity verification by using **the receiver's own** private key to decrypt it."

p28-29 Please revise the paragraph below to be more clear. Part of the problem is that you are using the term "Byzantine Fault Tolerance" (I think) to refer to the row labeled "Consensus Fault Tolerance" - which gets confusing because Practical Byzantine Fault Tolerance is one of the concensus protocols!

"As shown in Table 2.1, each consensus algorithm has its own advantages and disadvantages. For instance, in Proof of Work even Byzantine Fault Tolerance is around 50% but the throughput from Proof of Work is less than 100 transactions per second compared to Practical Byzantine Fault Tolerance Consensus Fault Tolerance is only 33 percent they need around 66 percent of agreement between node in order to confirm the transaction (see Section 2.3.5.3) but Practical Byzantine Fault Tolerance provide a very high rate of throughput. In order to consider which consensus algorithm is good or bad will depend on these characteristics like Byzantine fault tolerance, throughput, etc. Therefore, in order to create a good consensus protocol all of these characteristics from table 2.3 need be considered."

p29 "Every node in blockchain network will hold a pair of public and private keys."

Really? If the private key is stored in the block, how can it be private???

p 31 "(iii) Private Permissioned network - Permission in the network are kept centralized to a certain extent by a company. The company may only let some of the known or trusted nodes to gain permission in the network. [17]"

~~Always a company? Maybe you should say "company, authority or organization"~~

~~p33 "SHA-256 is a cryptographic hash function designed by the NSA (National Security Agency)~~ **~~of the United States."~~**

p 34 "The body of block will hold t**he count of transactions and the actual transaction information that has been collected by the Miner.**"

~~p36 "(SHA (SHA256(Merkle root || timestamp || prev || version || nonce)) < target)."~~

~~Is the || supposed to be "or"? Since this is bitwise OR, not logical OR, should only be one vertical bar (according to most programming languages).~~

~~Why is the target called "nbits"? Who determines the target for each block?~~

~~P 37 "If Sam has a multiple accounts and votes for Transaction B and most of validator believe that B is the valid transaction, Transaction A will be invalid and Jane won't get $5."~~

~~I don't understand how this benefits Sam. Doesn't he still have to send $5 to the other account?~~

~~Can you explain a bit more?~~

~~P 38 - This process is like throwing a dart~~ **~~while blindfolded~~**~~.~~

"When it went live in [what year?] the network contained a total of 103.78B XLM due to the design of the protocol."

~~"The validation in Stellar achieved by Stellar Consensus Protocol or SCP~~ **~~which will be discussed in detail in Section 2.3.5.3."~~**

~~p 39 Overlay is a component t~~**~~hat is used to flood messages to the network and fetch~~** ~~needed data in order to accomplish consensus from its peers.~~

~~P 40~~ **~~"For anyone running a node in the Stellar~~** ~~network, Stellar will provide benefits~~ **~~for users~~** ~~such as~~ **~~providing~~** ~~a Horizon instance (see section 2.3.5.4) and allowing for customization of business logic or APIs, etc. [22]. "~~

~~p41 "In a pBFT system there must be a recommended validator list that is defined by a central authority~~ **~~which can define it as a centralized system~~**~~.~~

P 42 " as stated in the **Stellar Consensus Protocol white paper [need reference]"**

~~"There are three properties that a consensus protocol needs, which are safety, liveness, and fault tolerance."~~

~~Please fix the formatting of the following list, which is inconsistent and very hard to read. Also note the period after "tolerance" above.~~

~~"anymore messages" ==> "any more messages"~~

p 43 “In theory (FLP impossibility result)” ==> need a reference for this theory.

P 45 “So, in order to guarantee safety that the two quorums will consistently **validate** a statement, the **SCP** requires quorum intersection.” I am not sure what this means. Requires in what sense? If a quorum is disjoint, will it be ignored?

P 48 “The situation discussed above is just an ideal scenario. **In fact, it is not easy for nodes to reach an agreement because of node failures. “**

p 49 “In summary on how **the behavior of t**hese types of node will have an effect on the system. **As a first example**, if every quorum in the network depend**s** on an ill-behaved node (failed node) that **is a** quorum intersectio**n, th**e ill-behaved node can send one message to one quorum and another to another quorum which will drive the system into divergent states. This will cause well-behaved node to failed (**become a d**ivergent node) and can’t guarantee safety. **As a s**econd example, suppose each of a node’s slices in quorums contains ill-behaved nodes which might not agree to anything or crash. and **T**hese ill-behaved nodes can drive the system into blocked states. This will cause well-behaved node to **become** failed (blocked node) because the well-behaved node would never be able to hear unanimously from one of its quorums and never make progress.”

p 50 “●Ledger header consists of these following fields:
● Version: the protocol version of given ledger
● Previous Ledger Hash: A hash value from previous ledger. This hash value will form a ledger that chained together.”

Please fix the format of this list so that the hierarchy is clear. It looks now like these items are all at the same level, when everything after “these following fields” should be further indented.

Are all these items part of the ledger header? If so, you should have a separate list item, at the same level as “ledge header”, for the transactions – even if you don’t provide details. Currently this is quite confusing because of the format.

P 53-54 This material is very confusing because it’s not well organized. I think you need to provide numbered headings and subheadings to guide the reader about the relationships among these concepts. This might help with the issue on p50 as well. What is the logical structure here? Make it clear!

P 55 “Being a stateless protocol means each request-response cycle is unrelated to other cycles [28]. **The server doesn’t have any representation of a continuing interaction or session. “**

p 57 “**Web applications can be structured as** one tier, two tier, three tier and N-tier architectures. The following paragraphs will discuss three layers that involved in each type of software architecture **The definition of the application architecture is based on the existence of and location of different functional layers:”**

p 58 “These are some benefits of a web app...”
Move this to be the second paragraph in this section, before you talk about layers and architectures.

“In addition, JavaScript can make interaction smoother and faster **by providing client-side routing. JavaScript can change the organization of the page (the DOM, or Document Object Model) without making a server request,** thus changing the contents you are viewing.”

I have never heard the term “client side routing”. Please provide a citation. Also, there are really two ways that JS makes pages more interactive. One is the ability to change the DOM. The other is the ability to send an HTTP request and get specific data back without having to re-render the page (“Ajax” style requests). You should probably mention both. Are you sure that “client side routing” doesn’t mean the Ajax capabilities?

P 59 Give HTML and CSS their own sections. They do not belong in the JS section.

P 59 Section 2.3.9.2.

Java is NOT free and open source (although Oracle provides free use to many categories of users).

Java did NOT develop from C++.

You have missed many of the most important characteristics of Java:
- Write once, run anywhere – executable code can be transferred from one machine and OS to another
- Automatic memory management, highly structured error handling
- Native networking – Java was built to be used with the Internet
- Native internationalization – uses Unicode by default, multi-language
- Rich set of class libraries provide for code reuse
- Can be used for client-side, server-side, mobile and embedded applications.

You should mention what aspect of your system will be developed with Java.

Section 2.3.9.3 (TypeScript) is a good explanation!

P 60 - “Angular, supported by Google, is ~~**an**~~ open source software”

“A framework is a set of tools that allows us to develop software and build an application.” Very vague, not a good definition. A framework provides a reusable abstract structure for an application. It makes application development easier because the overall organization is defined by the framework. The developer just needs to fill in the details.

I am very confused by this paragraph because you talk about both AngularJS and Angular8. Are they similar except for underlying language?

It would also be helpful to explain more about the form of the framework. I mean, what is the reusable abstract structure like? How do you develop a website in Angular? Your “benefits” list does not make much sense without a more complete explanation of what an Angular project looks like from a code/architecture perspective.

P 62 - “Spring boot is used to create a production-grade application.” What does this mean? Sounds like marketing hype, not technical. Also, be sure you capitalize correctly with every reference.

Section header for PostgreSQ: – fix format (don’t indent). It would also be good to mention that PostgreSQL has been around for nearly two decades and that it supports standard SQL.

“Docker is the OS-level virtualization platform service that allows applications to be packaged with all the dependencies installed and **run** wherever wanted.”

Need to explain more about the Docker architecture, and contrast with more familiar/older virtual

machine approaches (such as VMWare, VirtualBox). What do you need to do to get an application running in a container? How do you deploy it?

P 65 – I think you should move the detailed Use Case Narratives to an appendix, then reference that appendix in this section. Keep the Use Case Diagram, and add a short discussion/list of the different use case goals.

Also, I think you need to update (and simplify) the use case diagram to reflect the system as implemented. You do not have an admin and superadmin (do you?) There is no separate "non-profit organization" role, just regular users and beneficiaries. You no longer have third party wallet support. I don't think anonymous/non-anonymous deserves to be broken out in the Use Case diagram. Get rid of Request Receipt (just keep View Receipt). Edit campaign and update blog are the same thing.

You should note in the text that the use case diagram has been updated. However, I do not think you need to update the narratives; just move them. Once the system has been implemented, the narratives become history.

P 98 – I don't really want you to have to recreate all your sequence diagrams. However, Figure 3.5 does not seem to reflect your current implementation. You do not check any sort of financial information when a user creates a campaign. Also, I don't know if you check privilege level. Maybe you do, but right now only beneficiary type users have access to the create campaign functionality. Please review and correct this if necessary. (AND the text....)

The text talks about a transaction object. However, Stellar does not show up in the sequence diagram. Does creating a campaign create a Stellar transaction? (I would guess not...)

p 100 – Fix capitalization in the diagram (Spring Boot, Stellar,...) Always capitalize "Java".

P 101 – Either here, or in Chapter 4, you should discuss the fact that you're using a Test Stellar Core instance. Explain the actual deployment details.

P 102 – I don't think this reflects your system as implemented. For instance, I didn't notice a "Contact Beneficiary" option. You don't have two options one for Edit, one for Update. You're also missing some pages, such as Beneficiary History, Identity Verification, Activate/Inactivate campaigns, etc. Maybe you need three different diagrams, for the three different roles.

P 103-126 – To avoid reader confusion, and boredom, I think you should move the UI design details to a second appendix, and just put a reference in Chapter 3. (I am assuming Chapter 4 has the actual UI as implemented.)

p 127 – Please include a comment that this is the schema as originally designed, and that some changes have been made during implementation. Then include a forward reference to Section 4.2.

P 135 – Are there any significant UI features that you have NOT implemented? I would take out the "so far"!

P 146 – I thought that Report was mostly to report suspected fraud... not "inappropriate content".

P 147 "This field is **used** to specify some basic information."

p 152 "Users must provide their information in given fields for our admin to verify. **Specifically**

they should provide an image or scan of their ID card or passport, and a scan of their signature. After the admin verifies the user then the user **can access features for beneficiaries.**

P 143 – You DO have both Edit and Update??? So what is the difference? Is Edit for editing the text and update for modifying the cover image? If not, you need to explain this better. I didn't notice this when I was looking at the website.

P 156 – If a user deletes a campaign, what happens to the campaign history? Can another user still see donations? What about the donation history of individual users. Maybe "delete" shouldn't be allowed, just inactivating.

P 158 – Okay … Update looks just like Edit! This needs to be clarified (both in the report and in the website).

P 161 – PDF is not useful without the government charity number, official organization name, official organization address.

P 162 – How does an account become an admin account? Is this set directly into the database? Do you protect this in any way, using Stellar, encryption or anything else?

P 163

"navigate the user" This is not valid English since "navigate" is not a transitive verb.
I recommend that do a search and replace to change to "bring the user".

3. Activate Campaign - This option will navigate the user to the Activate Campaign page which is used **to** activate suspended campaigns.
4. Identity Verification - This option will navigate the user to the Identity Verification page which is used to verify the user account.
5. Sign out – this option will sign out and clear current session. After that the system will navigate user to normal home page

p 164 "The number of reports t**hat have been submitted about the campaign**. (For further report detail the user can click on the number that displays in the block)."

"This block is used **to** inactivate the campaign."

p 166 - **Figure 4.31 displays** a table that contains users **who have requested** identity verification. Each row in this table will consist of

p 169 "(**as described** in 4.2.1)" (multiple cases)

p 170 - "We add a **new** table **called VerificationToken.** This table will operate with the email system. This table will be used during operation that dealing with email system like "Reset user password" and "Email Verification"

p 171 – Fix the table format so that all data are readable and do not get split! I suggest reducing the font size.

P 172 "but we've changed to the second approach. We decided to use WYSIWYG quill editor

(what you see is what you get). It uses HTML markup to create content of campaign detail when the campaign is created or edited. Then we will store the markup in the database. When requested we will display said content as rendered HTML."

(Good explanation!)

p 173 - "There are several operations that deal with Stellar Horizon which are Donate, Register New User, Review Own Donation history, and Review Campaign's History of receiving donations.

"the Stellar network." PLEASE do a global replace to make sure Stellar is always in upper case.

P 183 – Section 4.4. This is well-explained. However, you don't say when or how this sort of checking will be executed. It seems that you should do this validation at least nightly.

Please think about this and add some discussion. (And the implementation.)

For your defense presentation, I want to SEE you hack the data base and then discover the fraud using Stellar!

P185 – Table 5.1 – why are some rows gray and some not? Does this mean something?

P 188 - "Finally, as we've already said that this is our first time with a big project like this. It is really important to understand the scope of what we are trying to do."