Explorable Explanation for Explaining the Working of Blockchain Technology

Akshay Khanna
University of Washington
Seattle, USA
akshay21@uw.edu

Naga Soundari Balamurugan
University of Washington
Seattle, USA
nagabala@uw.edu

***Abstract*—This paper is an attempt to explain how we have implemented an 'explorable explanation' to explain the concept of working of a simple Blockchain. This interactive model is developed using the concepts of web development. We have tried to explain the Blockchain concepts like shared ledger, the information inside a block, how a chain is formed, the concept of block tampering and peer to peer networks using interactive visualizations supported by text explanation. This paper discusses the motivation and rationale behind this topic, related work, detailed methodology used for the development, results and scope of future work for further development of this model.**

Keywords—explorable explanation, blockchain, working, shared ledger, proof-of-work, interactive visualization,

I. INTRODUCTION

Explorable Explanation is a reactive document that aims to explain a complex concept to an active reader (Victor, 2011). This reactive document allows the user to get a better understanding of a concept intuitively and understand the complex working of a system or a concept. The reader is able to play with the nuances of the concept through visualizations that are interactive in nature. Through these interactions the user is able to challenge the underlying assumptions and analyses and see the consequences. The contextual information alongside the interactive information helps the reader learn the related material just-in-time (Victor, 2011).

We have used explorable explanation to explain the concept of working of the Blockchain technology. Blockchain technology is the underlying technology of the working of cryptocurrencies like Bitcoin. However, the applications of the Blockchain technology are not limited to bitcoin and can be extended to a several concepts including, but not limited to, storing medical records, creation of a digital notary or even collecting taxes.

In our explorable explanation we have tried to explain the following concepts related to Blockchain in an interactive manner:

- The Shared Ledger
- The contents of a "block"
- The formation of "chain"
- Proof-of-work
- The concept of distributed Blockchain and peer-to peer network

Identify applicable funding agency here. If none, delete this text box.

II. RELATED WORK

During the search for our topic for explorable explanation we came across several interactive explanations of various concepts in Physics, Art, Biology, Philosophy, Math and Programming. However, Blockchain, given its novelty, was not explained interactively unlike several other topics.

Given its complex working, videos explaining Blockchain are more abundant. We noted that lack of an interactive text and the abstract nature of the concept made it difficult for the average person to learn from a video, this motivated us to develop an explorable explanation for this topic.

However, the explanation of the key concepts related to Blockchain is derived from a number of sources; the most prominent being from the works of a Belgian developer, Xavier Decuyper, more popular by his pen-name: Savjee.

III. METHODOLOGY

The first step towards creation of this explorable explanation was to come up with a low fidelity story-board to identify the main topics to be covered in the project.

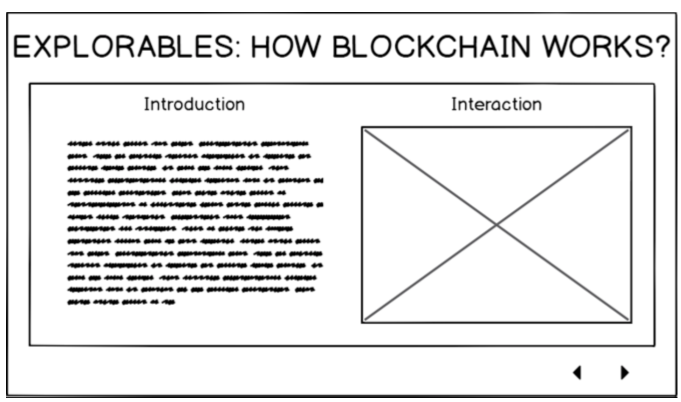

Figure 1 A Low-Fidelity wireframe of the web-application project

An animated story-board in PowerPoint was also created to understand the basic functionality of the various interactive visualizations and to assess the overall 'look' and 'feel' of each of the element within the project. The tools used for the development of this visualization include:

- Javascript as the primary scripting language along with an extensive use of its library: D3. D3 was primarily used owing to the functionalities it offers for drawing data driven visualizations.
- HTML as the primary scripting language for the development of the web page.
- CSS rules for overall aesthetics of the visualization
- Web Storm text editor for writing the code. This was chosen because it automatically creates a local server on the user machine, eliminating the need to manually build one.

Below is an assessment of each of the concept identified for this project.

A. *The Shared Ledger*

This concept is visualized using a simple animation implemented through JavaScript and HTML. On the click of a button a number of transactions take place between the nodes; which is represented by arrows. Each of these transactions are further recorded in four different ledgers, belonging to each node in the network.

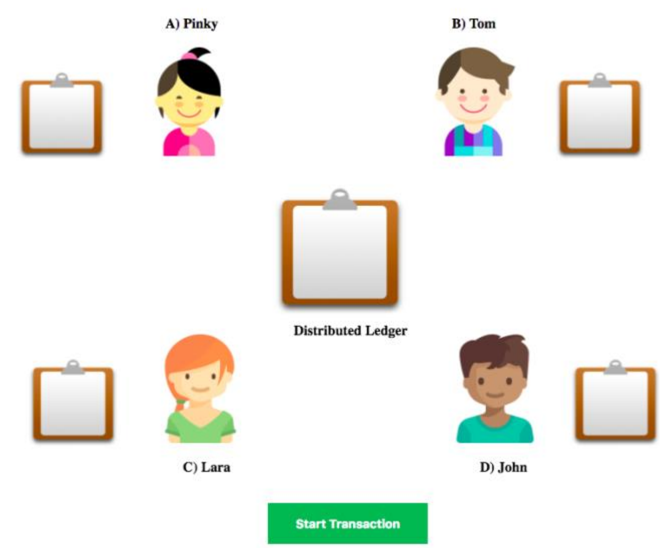

Figure 2 Concept of Shared Ledger

B. *The contents of a "block"*

For the development of this element of the project, D3 was extensively used. A cube was created as an SVG image using mathematical equations. Trigonometry and coordinate geometry was extensively used. By adopting this approach, we are able to change the dimensions of the cube (in the back-end code) just by altering the starting point of the upper left edge and the length of the cube. All other dimensions are adjusted proportionately.

The idea behind developing this cube as an SVG image, as opposed to using a stock image, was triggered by the fact that a number of interactions needed to be added on each side of the cube. As the user clicks on any of the three visible sides, the information within each of these sides is displayed.

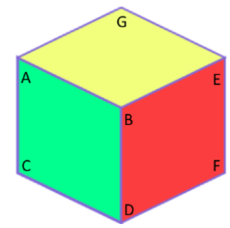

Figure 3 Dimensions of the Block

Given the coordinates of point A as (x1,y1), the length of the cube as l and the angle theta between the edges at point A, the coordinates of the remaining points of the cube are as follows:

Points	X Coordinate	Y Coordinate
B	x1+length* Math.sin(theta)	y1+length*Math.cos(theta)
C	x1+length* Math.sin(theta)	y1+length*Math.cos(theta)+length
D	x1	y1+length
E	x1+2*length*Math.sin(theta)	y1
F	x1+2*length*Math.sin(theta)	y1+length
G	x1+length * Math.sin(theta)	(y1+length*Math.cos(theta))-diag
Where diag = (length + length*Math.cos(2*theta))/ Math.cos(theta)		

C. *The formation of a "chain"*

The cube developed using the mathematical equations in the previous section is replicated thrice to form a chain of blocks. The information of the hash and the previous block is generated using the formation of a random string. The hash of each block is highlighted as the user hovers on the underlined text.

The concept of tampering of the block is further triggered by a click on any of the blocks in the blockchain. As the user clicks on a block the hash value of that block changes and the previous value is struck-through which also results in a change of the 'previous hash' value of the following blocks.

Figure 4. Formation of Chain

D. *Proof-of-Work*

This concept is developed using jQuery: another JavaScript library to enable ease in client-side scripting. A timer is used to calculate the proof-of-work required for each block. With each unit of time a random string of binary digits is generated. The total duration of the timer depends on which block in the chain is clicked upon by the user. Each block following the block that is clicked, adds 10 units of time to the timer. I unit of time represents 10 minutes.

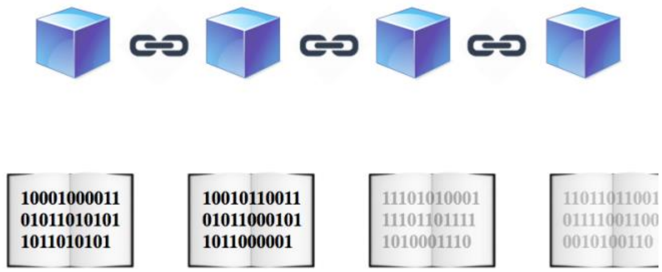

Figure 5. Proof-of-work

E. *The concept of distributed blockchain*

For the visualization of this concept a new block is created at the click of a button. But this new block is appended to each copy of the blockchain with each node, only when it is verified by all the nodes. This is visualized through click of another button: “Verify It”. This button is disabled unless a new block is created using the first button: “Create New Block”.

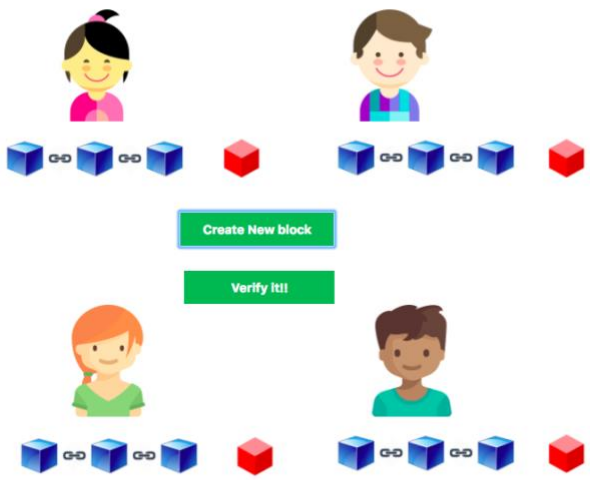

Figure 6. Formation of a new block

IV. Results and Discussion

From a visualization perspective, we have achieved the results as anticipated during the formation of our story-board. Our aim, through this project, was to identify the major key concepts in the working of the blockchain and represent it through various interactive visualizations. Barring a few exceptions, we have been able to develop the functionality of each of the various interactive elements. Some of the elements that remain underdeveloped are:

- In explaining the concepts of “The Block” we had intended the arrows that, on click on a side of the block by the user, points to various types of information through the use of curved lines. We were, however, unable to achieve this in D3 using the ‘Path’ and various other functions intended for curve drawing.
- In the “formation of the chain’ concept we had intended to display ovals around the ‘Previous Hash’ value of a block pointing to the ‘Hash’ value of the previous block through an arrow as soon as the user hovers on the underlined text. We were unable to achieve this due to the paucity of time and the complexity of the code involved in creating the oval shape, positioning it in alignment of the text and appending it to the SVG. We have achieved the highlight of the *Hash* and the *Previous Hash* value of each block by changing the colors as soon as the user hovers over the underlined text.

We encountered a number of challenges in developing this code. The most prominent challenges were:

V. Future Work

A. *Limitations*

Although we have taken care of a number of parameters that could go wrong, yet our code is not 100% bug-free. This code has the following limitations:

- The web-application runs properly on the Google Chrome only. This is attributed to the fact that not all browsers support all the versions of the D3.
- On re-sizing the window, the elements in the web-application do not resize and re-position themselves automatically. This anomaly can be attributed to not using ‘flex-boxes’ in the CSS rules.

B. *Improvements*

This web application can be improved in a number of ways:

- Resolving the issue of the disproportionate change of the web-page elements on resizing of the window using flexboxes in CSS rules.
- Instead of having the navigator buttons at the bottom of each page, the entire web-application can be combined within one page and each concept can be loaded on the web-page using one scroll-cycle.

VI. References

Victor, B. (2011, March 10). Explorable Explanations. Retrieved from Worry Dreams Website: http://worrydream.com/ExplorableExplanations/