Community Meeting Notes (Jan 10, 2018) - Blockchain to Design

Description

Presenters: Edward Buchi

Participants will learn to create their own addresses.This workshop will introduce the concept of Blockchains to answer two simple questions: what is it, how is it relevant to Design?

Resources

- Slides (keynote, pdf)
- Video Recording

Notes

A broad subject, but Edward has narrowed it down to a few core subjects for our benefit.

Blockchain:

- **Bitcoin the first Blockchain**
  - 03/Jan/2009 - First time Bitcoin started.
  - Response to how people in the financial industry mismanaged wealth.
  - Typical attributes of currency:
    - scarce
    - durable
    - divisible
    - portable
    - verifiable
    - fungible
  - Added attributes of cryptocurrency:
    - inimitable - cannot be duplicated
    - decentralised - there is no single institution or country controlling the currency
    - digital
  - Cryptocurrency Value = Belief in the utility of the Blockchain network; will automate a lot of what banks do

- **What are blockchains?**
  - Are the memory of the Internet.
  - Made of computers, instead of neurons, spread out all over the world.
  - Gives Internet access to data to access critical functions.
  - Does not need to go to the bank; can safely send records to specialists without that data being falsified.
  - Gives the Internet access to data in order to execute critical functions and not rely on external sources of information.
  - Bitcoin - databases owned by banks.
  - A blockchain network is a type of distributed network. It also refers to the structure data is stored in.

- **How Blockchains work (simplified technical explanation)**
  - A user needs two basic things:
    - A private key and a public key
      - A private key is like a password
      - A public key (aka address) is like a phone number
      - if you lose the private and public key, you'll lose access to your blockchain.
        - It is difficult to hack, so unlikely able to retrieve the data (e.g. this is how people have lost their bitcoin)
  - Basics components of a block
    - Example: bitcoin blockchain
    - A Hash is a condensed form of a digital file of anything
    - A function that, when data is run through it, will produce an identical (and often unique) result for the same given input
    - Merkle Tree, Merkle Root Hash
    - Component 1: Transaction Hash + Component 2: Previous Block Hash + Compotnent 3: Random number = Block Hash #
    - Change one block it would change the history of the rest of the Blockchain, because it would affect all hashes down the line.
    - Data security is maintained by having a copy of the blockchain
    - If a node would have a faulty copy of the blockchain, the other nodes (the network) would just ignore it
  - Who gets to be a node and what is the incentive?
    - anyone can be a node
    - the more computers there are the harder it is to come up with the NONCE
      - the NONCE is a method to build new blocks
      - only one node has the right to write the next block
        - the first node to "guess" the NONCE, gets to write the next block
        - Mining is volunteering for the network for the intention of winning the reward (NONCE – a hash result).
    - in terms of bitcoin, the node that writes the next block receives 12 bitcoins.

- **Implications in the world at large**

- Decentralised applications
    - The whole program exists on the blockchain network, injected into the blocks themselves. Don't need to get Amazon to host that app; inject it into the network and as long as it is alive, it will run forever.
    - Examples:
        - WeiFund - open-sourced crowd-funding
        - https://www.cryptokitties.co
        - Questions relating to the "enforcability" of artificial scarcity within a given blockchain
- Decentralised companies
    - "Smart contract" is a term from Etherium referring to a program that is injected into the chain. A program may spam multiple blocks (e.g. crypto kitties is 6–this helps with edits). Etherium provides a virtual machine (EVM) and has their own programming language that it runs.
    - Example: Slocket - build devices that have smart contracts in them (like bicycle locks)
        - A smart contract pays dividends to the shareholders; if the company were to go bankrupt, the locks would still work if the shares pay shareholders because it still exists on the blockchain.
        - A smart contract will only work well with a large network of users.
    - For Etherium to prevent large programs, which would eat up the resources, they built in a concept of gas. A smart contract needs to pay an amount of gas proportional to their size.
        - crypto kitties actually clogged the blockchain at one point when it became so popular and all the nodes had to process crypto kitties.
- Decentralised storage
    - Imagine Google Drive but files stored are not owned by Google
    - Example: Filecoin - Treat your hard drives like airbnbs – renting out your hard drive space
    - Example: Sio
- Machine addresses
    - Getting machines/addresses and facilitating payments between them
    - Example: Iota
- User owned accounts
    - Identity – anything that proves who you are can be stored online and can be used as proof to show you who you are.
    - Example: Civic Secure Identity Platform
- User owned data
    - Only users own their data; they have control of it as long as they have the private key. Not Google or Dropbox.