Community Meeting Notes (Mar 14, 2018) - Critical Perspectives on the Blockchain

Description

Presenters: Edward Buchi, Nelia Teixeira, Michealagelo Yambao

Blockchain Networks have such high potential to change how society works, 10 years of growth has proved this. But where's the revolution? Join us at the OCADs Inclusive Design Research Centre for a workshop on Blockchain to discuss the dark side of Blockchain tech, what can hold it back, how it can be subverted and is there a way out?

Resources

Video Recording

Slides

Notes

- Consensus Algorithms
  - Needs to be Byzantine fault tolerant
    - The systems is designed to reach consensus without necessarily having to talk to each other
  - Proof of Work
    - used by BitCoin and currently Etherium (etherium wants to change)
    - A node has to guess the Nonce to write the block
      - The reward is currently about 12 bit coins
      - This is referred to as mining
    - The more hardware on the network the more difficult it is to guess the number
      - This is wasteful of energy and resources as farms of hardware are used to guess the random numbers
      - costs roughly $400million world wide
  - Proof of Stake
    - Etherium will move towards using this
    - Rathering finding a nonce, it uses a system of betting
    - costs about $1million to setup a node plus
    - The block that gets voted on the most is injected into the chain
      - any fees associated with this block are split amongst the validators that bet on it
    - Creates a situation where there are only a few validator nodes, because of the costs
      - Because of the smaller number of nodes, it makes it more susceptible to discovery and attack
- Value and Volatility
  - What determines value?
  - In traditional systems currency created by a centralized authority
  - With the blockchain individuals can create currency
    - value determined by market
  - Last year's market cap for all blockchains is $146.2B
  - Banks in Canada are increasingly de-risking blockchain currencies, making it harder to transfer to your bank account.
  - Token value determinants by William Mougayar:
    - Role
    - Features
    - Purpose
  - These currencies are digital fiat currencies with nothing tangible backing them
    - Because of this they are only fuelled by speculation
    - this volatility is a barrier to real world use
- Disintermediation
  - The blockchain can automate all of the administration work
    - e.g. in the traditional system bank holds funds, lawyers officiate contracts, services like PayPal facilitate payments.
    - however currently no consumer protections on Blockchain services
    - the individual has more autonomy but also much more responsibility
- Smart Contracts
  - not a legal contract, it is a computer program that has some legal attributes
  - live on the blockchain
  - immutable
  - always on as long as there are nodes on the network
  - they run on gas (gas is an amount of ether necessary to run the smart contract)
  - An Oracle is an agent that verifies real-world occurrences and feeds this information into the smart contract
    - an oracle can be any input source: machine person, etc.
  - Case Study: DAO Failure
    - cryptocurrency is not yet legally considered money

        - this could change
    - remedied by forking the block chain (Etherium classic and Etherium)
- Immutability
    - not easily rolled back
    - can't easily iterate on smart contracts
- Identity
    - can have oracles validate things like citizenship and etc.
    - a single blockchain identity can at as multiple IDs simultaneously
    - However, you need to take care of your private key, to prevent identity theft for example.
    - If the identity record is on a private network it can be manipulated and controlled by those running the network
    - Blockchain identities assumes a privileged user, e.g. has a computer, access to internet, can manage their private key