

### PROBLEM: BLOCKCHAIN PROTOCOL SCALABLE FOR MANET & IOT DEVICES

#### WHAT IS BLOCKCHAIN? AN ANSWER TO THE QUESTION: "HOW DO I STORE DATA DIGITALLY AND ENSURE THE DATA REMAINS ACCURATE?"

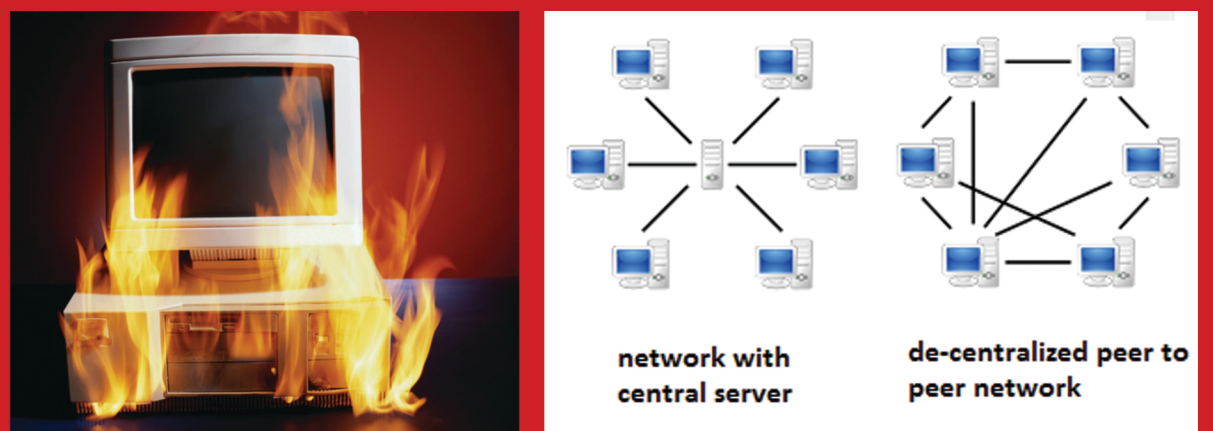


#### WHAT DOES "ACCURATE" MEAN AND WHY DOES IT MATTER?

Accuracy is important for several reasons, some of the more imaginable are to preserve attributions in the case of copyrights, to be able to make sometimes life and death decisions based off accurate information (e.g. an airplane's autopilot relies on information from altimeters that can have deadly consequences if the information is wrong), and to preserve a record of transactions (the fundamental underpinning behind crypto currency that enables them to have value).

#### ISN'T STORING IT ON MY COMPUTER SAFE ENOUGH?

This would be an example of central storage which is known to be fundamentally unsafe. Besides the required physical safety of the central unit (it would be a pain to lose the information in a fire) centralized information is more susceptible to malicious entities and natural data corruption.



#### SO WHAT IF NOT CENTRAL STORAGE?

Peer-to-peer is a decentralized internet protocol in which the work of maintaining the network is shared amongst the network's users. This helps preserve accuracy by storing multiple copies of the information across a network and moving them consistently. This alone is not enough to preserve accuracy which is why blockchains are a subset of peer-to-peer networks with more stringent communication and data verification protocols.

#### STANDARD BLOCKCHAIN LIMITATIONS

Regular blockchain grows linearly by use of a linked list, search/validation time is  $O(n)$  time complexity.

Linked list structure of blockchain is limiting -- there is no correlation between the structure and the data being stored, minimal advantages compared to other data structures. Designed for static nodes with continuous connection to the network, not designed for highly mobile or light-weight devices. Devices may drop out of the network at any time. Doesn't make use of the spatiotemporal nature of these devices.

Large computational, storage, and energy requirements

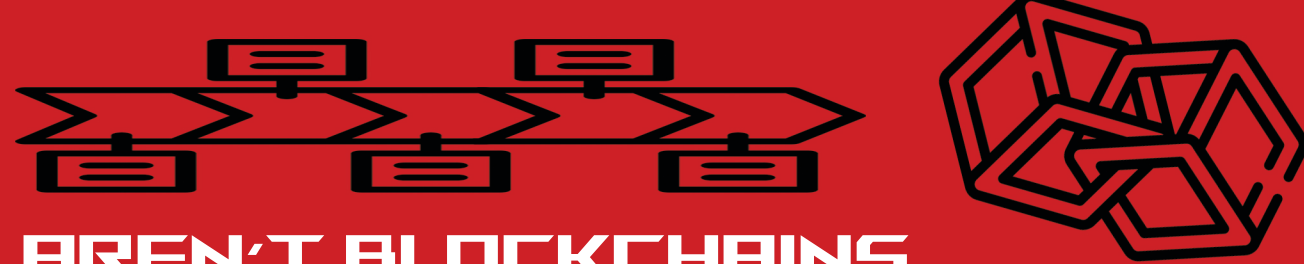
Validity algorithms uses large amounts of energy for computational processes

#### ETHICAL REASONS TO SOLVE THIS PROBLEM?

Many blockchain implementations, including most cryptocurrencies, are very energy intensive. In recent years it has come to light that the energy cost of maintaining and validating these currency blockchains is significant and continues to rise. For example, Bitcoin mining energy consumption surpassed the total energy consumption of the country of Argentina. (<https://www.bbc.com/news/technology-56012952>). Creating a more efficient blockchain protocol will limit future emissions and combat climate change by reducing power consumption per task.

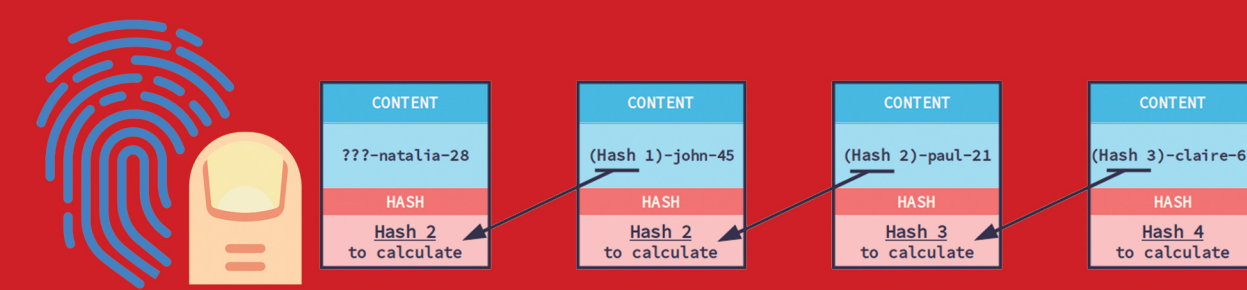
#### WHAT IS A BLOCK?

A data structure that holds the transactions (record of node activities) of all the nodes in the cluster within a window of time that is given a unique hash based on its own data as well as that of the blocks prior. This hash acts to not only verify the contents but the position of the block in the blockchain. The incorporation of the data previous in a hereditary fashion into the current block hash is what is meant by "chaining".



#### AREN'T BLOCKCHAINS OVER-HYPED LINKED LISTS?

What sets blockchain apart from a linked list is the hereditary chaining of hashes, the ability of the blockchain to act and self regulate (e.g. forging new blocks or constant self verification of its data), and the distributed storage and tasking of the blockchain across its member nodes.

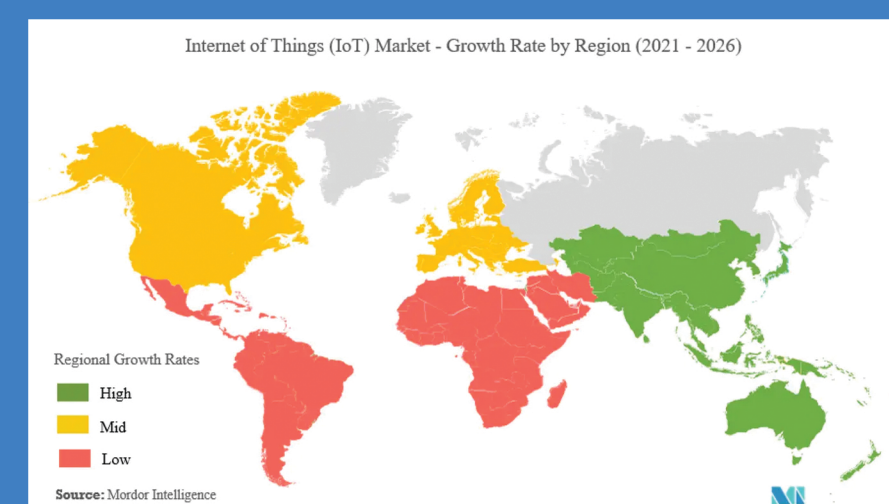
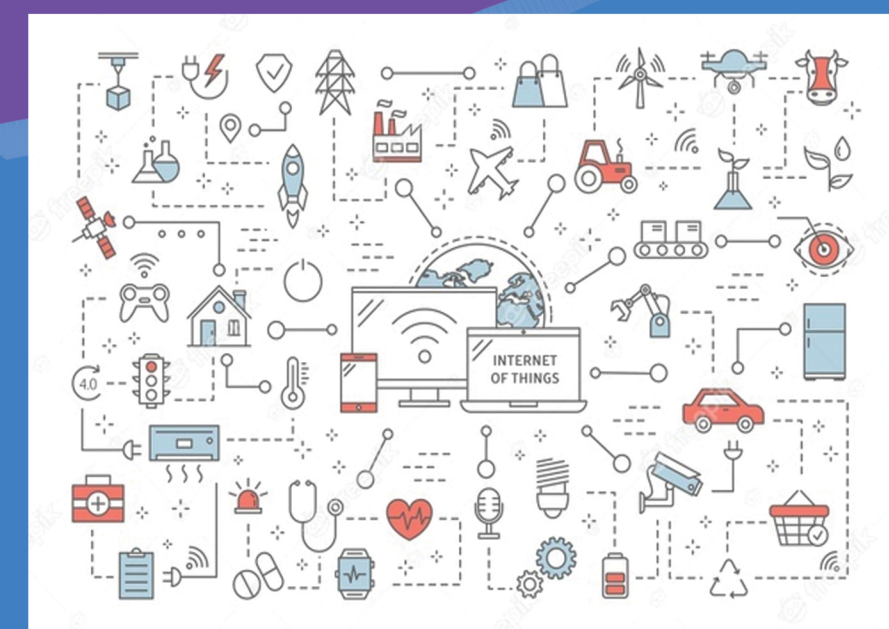
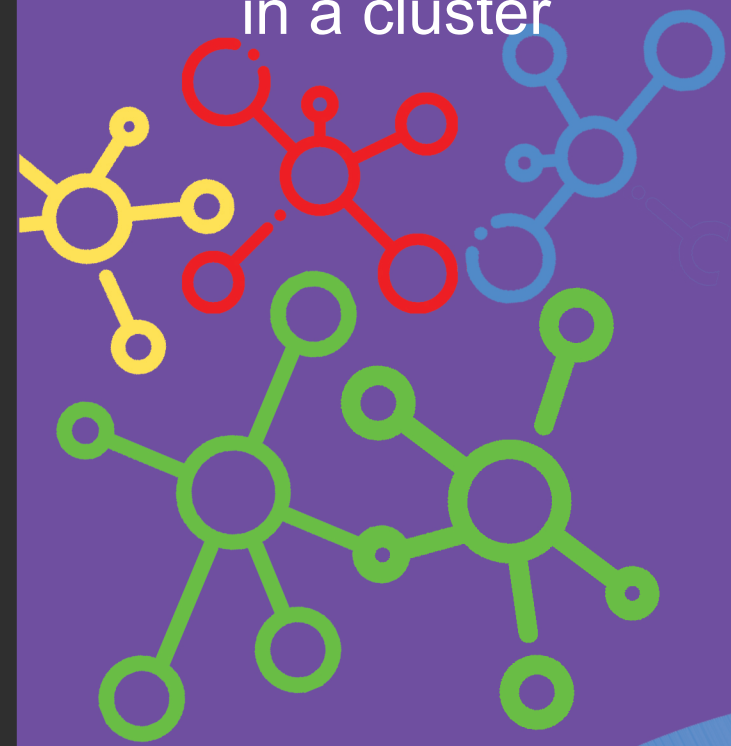


#### WHAT DOES IT MEAN TO HASH?

Hashing is creating a value of a predetermined size that is a unique representation of the data being hashed. Different data begets different hashes and in such a way a hash may be thought of as a fingerprint. Re-hashing your data will prove it either has not changed because the new hash is the same as the one prior or that it has changed because the new hash is different than the previous.

#### WHAT IS A NODE?

Node is used to describe a member of a network or an individual computer/sensor in a cluster



#### MOBILE AD HOC NETWORK (MANET)

Network that can be set up without an infrastructure (ad hoc) made up of nodes that are highly mobile. The nodes contain programming and hardware that allow them to communicate with each other as without a central unit.

The individual devices that make up the network need not be of the same type, they only need to have the functionality to create a MANET by connecting to other devices using compatible frequencies and protocols.

Mobile Wireless Sensor Networks are a type of MANET (e.g. environmental sensors like humidity sensors, thermal sensors, cameras, etc.) and best represents the node behavior in our project.

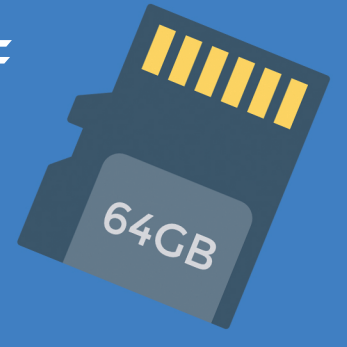
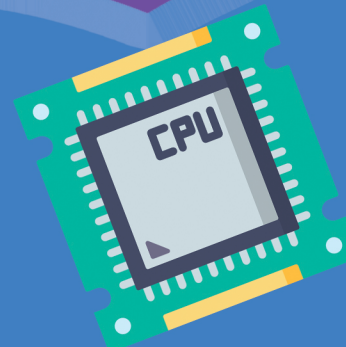
#### HOW DO NODES COMMUNICATE?

Several messaging architectures can be incorporated into a blockchain. While each has its respective security measures, there are other advantages that a blockchain can leverage in accordance with its goal, such as time taken or message distribution speed. Examples include the publish-subscribe model (PubSub) and the point-to-point model.



#### ASSOCIATED RESTRAINTS OF IoT AND MANET TECHNOLOGY

Processing speed and memory of smaller devices



#### INTERNET OF THINGS (IoT)

Devices (sensors, appliances, integrated systems, etc.), that connect to the internet in order to provide additional and often remote functionality. They are designed to take some input, be it from a user, sensor or another device, and either transmit it over the internet or translate it into some useful information for the user.

"66% of homes in the region have at least one IoT device. Additionally, 25% of North American homes boast more than two devices. The average household in the region would have an average of 9 devices by 2022, and nearly half (48%) of total devices and connections will be video capable." - A mordor Intelligence survey (circa. 2016)\*

