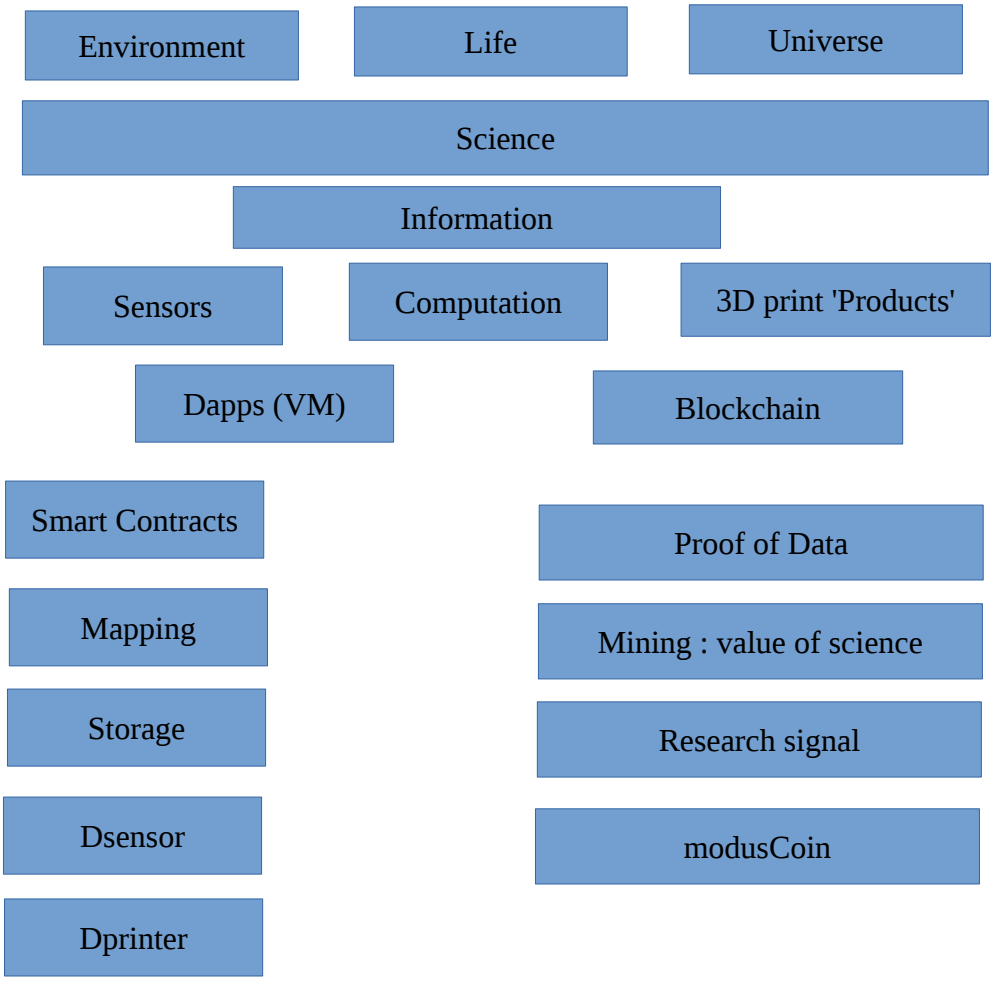
Modus :The Measure of Science – blockchain ideas, principals, objectives, big picture draft 1



Emotional pull
Science is the foundation of technology and at the heart of human civilization advancement. Combine scientific endeavor with blockchain methodology and this gives the potential to accelerate science research discovery and thus evolution of the human species.

The big problems of our time; environment of planet earth and our survival on it. The conscious human control over life, cure aging or DNA modification and finally understanding the cosmos at large.

Today, these complex problems are being addressed by very few humans. Humans centralized around government projects or scientific research labs of private corporations or non-profits. Computation power and software code being run on centralized computer infrastructure. The value of such research broadcast out. A science blockchain would be open to all, contributing sensor data, computation power and software code (research) and then the value is personalized first and then aggregated across the network to give the worldwide view.

Authority
Scientific method recognized across the planet. Putting it on a blockchain and liberating it to all is yet to be fully communicated or understood.

Technical
The technology now exists, networks, computation and mathematical trust mechanisms to propel the scientific endeavor forward, faster, better etc.

- Environment
    climate change: carbon dioxide, pollution(smog),

- Life
    cure aging, understand consciousness

- Universe (cosmos at large)
    laws governing creation and unfolding of a universe

Science
Science is the human construct to address the three above.

Information
Science is showing that information is weaved in to the fabric of everything.

Sensors
Range from electronics to human and those of other life.

Computation
Combing existing information to produce new.

3D Print (products)
The universal way of creating material objects.

Blockchain
The network connection between information.

Dapps (VM)
The information environment where network participants can contribute their own data and science Dapps(research) in the form of computer code to the network. Peer to Peer.

The key components of the Dapps are:

    Smart contracts

    Mapping
    Interaction of computation data with Dsensors or Dprinter

Storage/CPU power
The utility capability of having the data reliably available and privacy status to control of any peer wants.

Dsensor
Utility library to allow all sensors to interact with Dapps

Dprinter
Utility library to allow any printing of material object in the universe.

Blockchain
The primary role of the blockchain is to facilitate trust and universal rules across the network.

Blockchain2.0 Sidechains / smart contracts
This propsed as the next evolution of the blockchain technology. This allows more advanced scripting in contracts i.e. computer code written rules to describe the 'law' of the terms of a contract.

The blockchain facilitates:

Proof of Data
Before we explain proof of data lets put down the foundations of existing proofs:

Proof of work

Bitcoin blockchain
Motivation: decentralized trust banking/money peer to peer.
Upfront mathematical model to issue 21million coins over a period of time. That is mining prime numbers, using HashCash.

Hashcash bring a simple and elegant mathematical property of easy to validate but hard (requires a lot more work) to compute.

These elements brought together in the act of mining to create a block.

The first block solves the first mathematical Hashcash i.e. that is how many zeros present at the start of a hash. This mathematical model infers computational power equals votes. Like in a democracy, each individual is given a voting card. The Upfront rules of bitcion then allocate a number of bitcoins to the entity finding the first block. This number is arbitrary and the chose of the founder of the bitcoin blockchain. The mathematics are those of cryptography and involve the notion of public and private key to crypt and de-cypt data to produce as a string of numbers known as a hash.

The second block is then mined. But what if two entities solved the new block and claim it? The rule governing the blockchain is that the longest accepted chain is the accepted chain. Bitcoin blockchain requires the hash of the previous block to be included in the subsequent block hence, the network can keep track and come to a consensus on the longest chain. The Upfront model design of bitcoin blockchain was to vary the difficulty of discovery to finding of a new block every 10 minutes.

This blockchain setup provides a trust and security model if the following is maintained. As long as no

one entity has over 51% of computation power in the nextwork, remember computation power is votes, thus if one entity has 51% of the votes then they could in theory rewrite the order of the blocks in the blockchain.

This is bad because a bad entity could double spend the bitcoins they have received during mining. That is, create two blockchains, the first spending the bitcoins on gold and then delete it and then create a second that buys silver. The entity that delivers the silver will get paid their bitcoins but the entity that sold the gold will not get paid, even worse, there will be no transaction or audit evidence to show they sold the gold.

Double spend is a symptom of trust or in this case lack of trust. Traditionally civilization have created social constructs like banks to act as trust brokers. However, a bitcoin blockchain uses mathematics.

The mathematical construct used is called Proof of Work. An owner of bitcoin buys gold, this transaction is recorded on the current block on the bitcoin blockchain. How does the entity selling the gold for 50 bitcoins know the buyer has in fact 50 bitcoins? The two entities exchanges bitcoin addresses along with the amount of bitcoin and a hash for that transaction. The entity selling the gold takes this hash number and performs a 'proof of work' hashing calculation to verify that indeed the buying entity has transaction listed in a valid block on the bitcoin blockchain. This shows they have more than the amount of bitcoins e.g. they mined 25 coins, exchanged fiat US for 100 bitcoins etc. As a result, given the hash is in agreement then given 51% integrity is in place, they seller can be sure the transaction can go ahead. As the chain of blocks become long and the number of transaction increases, the hashing required could become costly time and for CPU. To keep this to a minimum, transactions in a block are reduced via a merkle tree to a single hash number. It is this single has number per block that bring efficiency to receiving blockchain checking.

The ability to achieve such a model of commerce is a big breakthrough in computer science, solving a long lasting big problem, how to enable trust in a peer to peer distributed network.

In terms of society it provides a trust mechanism, that is without the reach of human interference.

Bitcoin has established an economic price or monetary value via creating a market price between bitcoin and other fiat currencies.

Bitcoin applications are called Wallets and can be on various computer run environments, Linux, windows, browsers, smarts phones and all need access to the Internet.

Proof of Stake

Only possible if existing proof of work blockchain has been established. The world now has established this, it is called the bitcoin blockchain.

People see room for improvement over Proof of Work systems:

- scaling the number of transactions per block
- reduce the wastefully computation power on meaningless calculation (ie hashcash)
- centralization motivation of mining in to pools (should be decentralized)
- Security can be compromise in proof of work with less bitcoin available as a reward
- others

How does proof of Stake differ?

Assuming a proof of work blockchain is operating or a pre-mined new blockchain is established via proof of work, then coins are allocated to peers. This grants the peer the right to mine a new block.

How is consensus reached on the longest chain on the blockchain under Proof of Stake? This has yet to be fully demonstrated. Various techniques are being put forward. More detail on these to follow.

Proof of Data

How does proof of data differ from proof of stake and proof of work?

Motivation: decentralized science peer to peer. Where each peer can apply the science of the network to their own individual data.

Upfront, there is the existing knowledge of the world represented in information. Looking forward there is no arbitrary limit to put on the volume of information that will represent knowledge. From an individual peer point of view, the volume of data associated with a peer while probably finite it does tend towards infinity. The conclusion put forward is that it makes no sense to have a science blockchain with a finite, i.e. fixed block number up front or on an annual allocation.

Can we use the mathematics of little effort to verify and a high amount of effort to compute ie hashcash thinking to give trust over science data? I can think of no logic that would make this apply to a science blockchain. That is why a science blockchain has to operate differently from a blockchains conceived to act as a monetary currency.

How is the first science block created on a science blockchain? Science is practiced in the realm of humans thus we need to use the mathematics of trust of a proof of work blockchain to seed the science blockchain i.e. the need to use an existing block on the bitcoin blockchain (i.e. a sidechain). This new science side chain will then perform an arbitrary proof of work (hashcash or protein folding etc.) calculation to seed or pre-mine blocks.

When a peer joins the science (sidechain) blockchain i.e. downloads a Dapp(wallet), they will be allocated one of the pre-mined blocks.

What will the reward per block be? An arbitrary amount? Why not? Good as anything that could be more sophisticated.

Lets say this peer brings in information representing knowledge that is valuable, lets assume this peer brings in data from a sensor plus a computational model i.e. a software programme. Should this block be rewarded more than any other block? Establishing the value of existing information representing knowledge is difficult but the table below sets out criteria that can be explored.

The reward for 'mining' . In a currency context this simply a reward arbitrarily granted when a new block is established based on the upfront rules. However, in the context of science the following criteria could be encapsulated:

Action on data				
Use	Information	Dprinter	Attention	Dsensor
Compute	Energy	Time		
Complexity	Intelligence score	Code structure		
Outcome	Simulation	Reality	Apply other places	General law

Proof of data is a special type of proof of stake.

The peer has downloaded a science Dapp. From this Dapp they can now build their own Personal Blockchain. For example, data collected from the garden recording climate data or from a wearable sensor on their being. This data is recorded on their own Personal Blockchain after it has gone through proof of data. Like in proof of stake the Dapp will contain a pre-mined block. The new sensor data will be hashed to this block.

How much data can be assigned to a Personal Block on a personal Blochchain before reference to a main science sidechain blockchain? How frequently? Good questions.

The answer and goal of the concept is that the sensor data entering the personal blockchain can not be made up data. But this an extremely hard and difficult problem to overcome i.e. the sensor could use Dsensor library on the micro controller and record data directly to the personal blockchain however the sensor data could be for the last 4 years i.e. data captured honestly before the concept of a science blockchain even was thought up. Some peer data will be factually valid for others it could be simply made up (Spam).

Those making up the data will have to incur the energy/computation and when they apply to get their block confirmed on the main science blockchain(sidechain) it will be done so in that context, the hash will inform the network the data was historical or that it was via secure micro-controller library. The mathematics and proof of data hashing gives this trust to the data.

If the the made up data enters the blockchain, it is still not safe. If in subsequent exchanges or results from use of the data in Dapps suggest the data does not stack up then the block can be identified and remove/blacklisted and the network informed. Thus this provides a strong disincentive to make up data and Dapps and peers will not want to exchange or use the data.

Does proof of data prevent a 51% attack? As a personal blockchain have unlimited length therefore a network attack is no applicable. The sidechain creation via proof of work mining could be subject to manipulation but this again would be record on the bitcoin blockchain thus an audit-able record of their action would be available to the network i.e. the existing proof of work provides an umbrella for network attacks to sidechains and thus on to personal blockchains.

What about double spending? In a science blockchain world this does not exist. What does exist is the trust in the data recorded as explained above. Data will be double spent. In fact it will be used many many times, there will be no known limit on the use of the data (constrained by the energy and technology available in the world).

Incentives in proof of data:

Want peers to contribute data from sensor and scientific knowledge represented in information.

What about a new research idea. How does the Dapp value that block?

Merkle trees bring information retrieval efficiency/checking to a proof of work blockchain transaction. How does a Science sidechain bring information retrieval efficiency and checking to a personal blockchain? The science blockchain goal is to connect the right data (hence peer) to the right computation 'research' and have the value first displayed back at the peer. The peer should also be notified of new 'research' computation that is most applicable to their personal blockchain. Bringing this capability, let alone efficiency to the process is a very difficult problem and far exceeds using a merkle tree to validate a simple list of transactions. The blockchain needs to evolve from mere transaction certainty validation to some sort of 'value' judgment on the both the data held, the computation and hence value to any individual peer. This difficult problem will need to be addressed stage by stage, first bringing confidence the data is trustworthy on a personal blockchain, usage of data in peer network, usage of computation(research) across the existing network i.e. an audit trail of use. From this start, more complex 'value' systems can be explored as per the table above.

Mining
Creation of sidechain. Pre-mining proof of work algorithm.
Creation of a Personal blockchain block via proof of stake.

Research signal
This will replace price (as in monetary) signal as the governing number for the network to collaborate on.

modusCoin
The pre ming proof of work on seeding the sidechain, will equal the value of all existing science value in the world on creation. Right now an arbitrary number. In time a value could be crowd sources on the value potential or new information added to the network e.g. using prediction markets with 'votes' from the existing network.