Chapter 3: BRIEF ON SYSTEMS

3.1 Blockchains as Blue Ocean Databases

Before we discuss applications, let's first review what's different about blockchains compared to traditional big-data distributed databases like MongoDB.

We can think of blockchains as "blue ocean"databases: they escape the "bloody red ocean" of sharks competing in an existing market, opting instead to be in a blue ocean of uncontested market space. Famous blue ocean examples are Wii for video game consoles (compromise raw performance, but have new mode of interaction), or Yellow Tail for wines (ignore the pretentious specs for wine lovers; make wine more accessible to beer lovers). By traditional database standards, traditional blockchains like Bitcoin are terrible: low throughput, low capacity, high latency, poor query support, and so on. But in blue-ocean thinking, that's ok, because blockchains introduced three new characteristics: centralized / shared control, immutable / audit trails, and native assets / exchanges. People inspired by Bitcoin were happy to overlook the traditional database-centric shortcomings, because these new benefits had potential to impact industries and society at large in wholly new ways.

These three new "blockchain" database characteristics are also potentially interesting for AI applications**.** But most real-world AI works on large volumes of data, such as training on large datasets or high-throughput stream processing. So for applications of blockchain to AI, you need blockchain technology with big-data scalability and querying. Emerging technologies like BigchainDB, and its public network IPDB do exactly that. You no longer need to compromise on the the benefits of traditional big-data databases in order to have the benefits of blockchains.

3.2 Overview of Blockchains for AI

Having blockchain tech that scales unlocks its potential for AI applications. Let's now explore what those might be, by starting with the three blockchain benefits.

These blockchain benefits lead to the following opportunities for AI practitioners:

Decentralized / shared control encourages data sharing:

(1) Leads to more data, and therefore better models.

(2) Leads to qualitatively new data, and therefore qualitatively new models.

(3) Allows for shared control of AI training data & models.

Immutability / audit trail:

(4) Leads to provenance on training/testing data & models**,** to improve the trustworthiness of the data & models. Data wants reputation too.

Native assets / exchanges:

(5) Leads to training/testing data & models as intellectual property (IP) assets, which leads to decentralized data & model exchanges**.** It also gives better control for upstream usage of your data. There's one more opportunity:

(6) AI with blockchains unlock the possibility for AI DAOs (Decentralized Autonomous Organizations). These are AIs that can accumulate wealth, that you can't shut off. They're Software-as-a-Service on steroids.

There are almost surely more ways that blockchains can help AI. Also, there are many ways that AI can help blockchains, such as mining blockchain data (e.g. Silk Road investigation). Many of these opportunities are about AI's special relationship with data. So let's first explore that. Following this, we'll explore the applications of blockchains for AI in more detail.

Opportunity 1: Data Sharing → Better Models

In short: decentralized / shared control encourages data sharing, which in turns lead to better models, which in turns leads to higher profit / lower cost / etc. Let's elaborate.

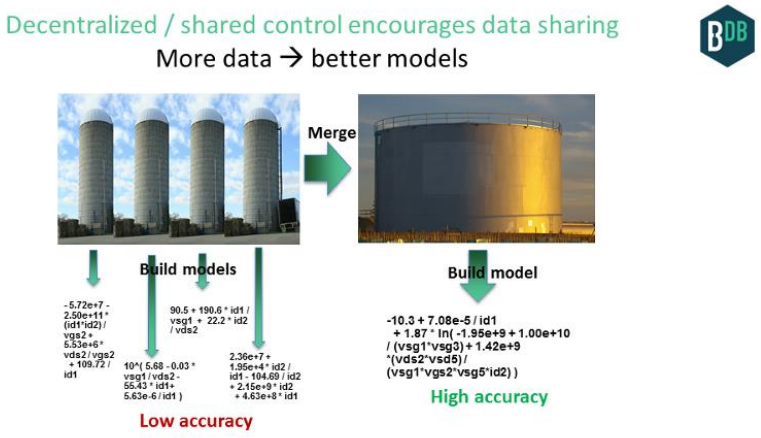

Figure 3.1 Decentralized control encourages data sharing

AI loves data. The more data, the better the models. Yet data is often siloed, especially in this new world where data can be a moat.

But blockchains encourage data sharing among traditional silos, if there is enough up-front benefit. The decentralized nature of blockchains encourages data sharing: it's less friction to share if no single entity controls the infrastructure where the data is being stored. I give more benefits later on.

This data sharing might happen within an enterprise (e.g. among regional offices), within an ecosystem (e.g. for a "consortium" database), or across the planet (e.g. for a shared planetary database, a.k.a. public blockchain). Here's an example for each:

- **Within-enterprise:** data from different regional offices is merged using a blockchain technology, because it lowers the cost for the enterprise to audit their own data, and to share that data with auditors. With that new data in place, the enterprise can build AI models that, for example, predict customer churn better than their previous models which were only built at the level of regional office. A "data mart" for each regional office?
- **Within-ecosystem:** competitors (say, banks or music labels) traditionally would never share their data. But it would be straightforward to show how, with combined data from several banks, one could make better models for, credit card fraud prevention. Or for organizations along a supply chain, that share data via a blockchain, one could better identify root causes of failures later in the supply chain, using AI on data from earlier in the supply chain. For example, where exactly did that strain of E. coli emerge?
- **Within-planet (public blockchain database):** Consider the sharing of data among different ecosystems (e.g. energy usage data + auto parts supply chain data); or of individual participants in a planet-scale ecosystem (e.g. the Web). More data from more sources could improve the models. For example, spikes in energy usage in some factories in China might be correlated with fraudulent auto parts emerging on the market a day's worth of shipping later. Overall, we're seeing signs of this with companies that aggregate data, sanitize it, and repackage and sell it; from good old Bloomberg terminals to the dozens (or hundreds) of startups selling data through http APIs. I explore this further in a later point.

Enemies sharing their data to feed an AI. 2016 is fun!

Opportunity 2: Data Sharing → Qualitatively New Models

In some cases, when data from silos is merged, you don't just get a better dataset, you get a qualitatively new dataset. Which leads to a qualitatively new model, from which you can glean new insights and have new business applications. That is, you can that do something you couldn't do before.

Here's an example, for identifying diamond fraud. If you're a bank providing diamond insurance, you'd like to create a classifier that identifies whether a diamond is fraudulent. There are four trusted diamond certification labs on the planet (depending who

you ask, of course:). If you only have access to the diamond data for one of these labs, then you're blind about the other three houses, and your classifier could easily flag one of those other houses' diamonds as fraud (see picture below, left). Your false positive rate would make your system unusable.

Consider instead if blockchains catalyze all four certification labs to share their data. You'd have all the legitimate data, from which you would build a classifier (below, right). Any incoming diamond, for example seen on eBay, would be run through the system and be compared to this all-data one-class classifier. The classifier can detect legitimate fraud and avoid false positives, therefore lowering the fraud rate, to benefit of insurance providers and certification labs. This could be simply framed as a lookup, i.e. not needing AI. But using AI improves it further, for example by predicting price based on color, carats, etc. then using "how close is price to expected value" as an input to the main fraud classifier.

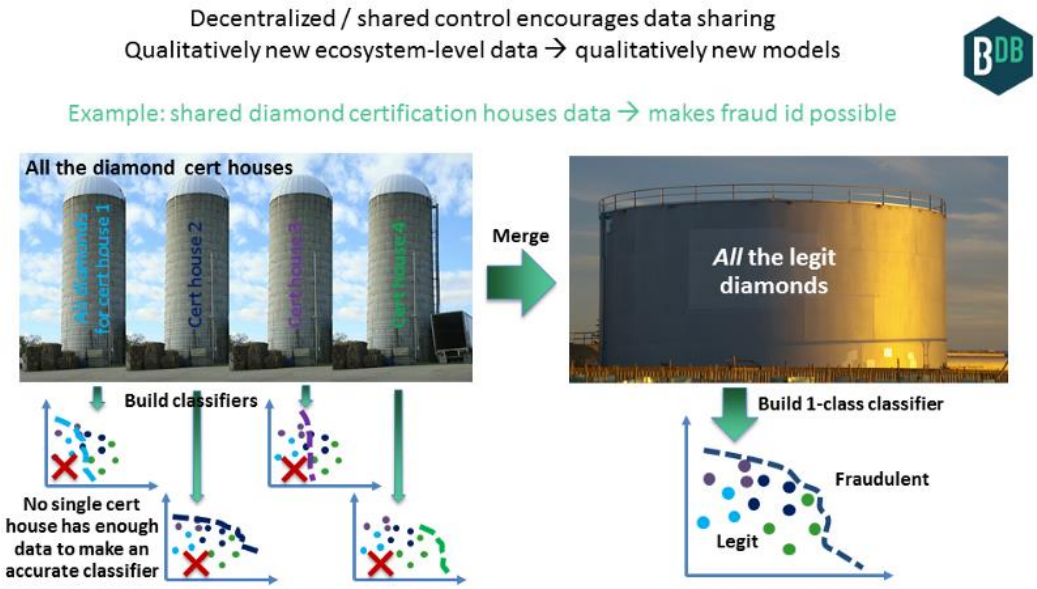

Figure 3.2 Shared diamond certification houses data

Here's a second example. An appropriate token-incentive scheme in a decentralized system could incentivize datasets to get labeled that could not be previously labeled, or labeled in a cost-effective fashion. This would be basically a decentralized Mechanical Turk. With new labels we get new datasets; we train on the new datasets to get new models.

Here's a third example. A token-incentive scheme could lead to direct data input from IoT devices. The devices control the data and can exchange it for assets, such as energy. Once again, this new data can lead to new models (Thanks to Dimi de Jonghe for these last two examples.)

Hoard vs. share? There's a tension between two opposite motivations here. One is to *hoard* data—the "data is the new moat" perspective; the other is to *share* data, for better/new models. To share, there must be a sufficient driver that outweighs the "moat" benefit. The

technology driver is better models or new models, but this driver must lead to business benefit. Possible benefits include reduced fraud for insurance savings in diamonds or supply chains; making money on the side in Mechanical Turk; data/model exchanges; or collective action against a powerful central player, like the music labels working together against Apple iTunes. There are more; it requires creative business design..

Centralized vs. decentralized? Even if some organizations decide to share, they could share without needing blockchain technology. For example, they could simply pool it into an S3 instance and expose the API among themselves. But in some cases, decentralized gives new benefits. First is the literal sharing of infrastructure, so that one organization in the sharing consortium doesn't control all the "shared data" by themselves. (This was a key stumbling block a few years back when the music labels tried to work together for a common registry.) Another benefit is that it's easier to turn the data & models into *assets*, which can then be licensed externally for profit. I elaborate on this below. (Thanks to Adam Drake for drawing extra attention to the hoard-vs-share tension.)
As discussed, data & model sharing can happen at three levels: within an enterprise (which for multinationals is harder than you might think); within an ecosystem or consortium; or within the planet (which amounts to becoming a *public utility*). Let's explore planet-scale sharing more deeply.

Opportunity 2a: New planet-level data → new planet-level insights

Planetary-level data sharing is potentially the most interesting level. Let's drill further into this one.

IPDB is structured data on a global scale, rather than piecemeal. Think of the World Wide Web as a file system on top of the internet; IPDB is its database counterpart. (I think the reason we didn't see more work on this sooner is that semantic web work tried to go there, from the angle of upgrading a file system. But it's pretty hard to build a database by "upgrading" a file system! It's more effective to say from the start that you're building a database, and designing as such.) "Global variable" gets interpreted a bit more literally:)

So, what does it look like when we have data sharing with a planet-scale shared database service like IPDB? We have a couple points of reference.

The first point of reference is that there's already a billion-dollar market (recently), for companies to curate and repackage public data, to make it more consumable. From simple APIs for the weather or network time, to financial data like stocks and currencies. Imagine if all this data was accessible through a single database in a similar structured fashion (even if it's just a pass through of the API). Bloomberg x 1000. Without worrying that there was a single choke point controlled by a single entity.

The second point of reference comes from the blockchain, in the concept of "oraclizing" outside data to make it consumable by a blockchain. But *we can oraclize it all.* Decentralized Bloomberg is just the start.

Overall, we get a whole new scale for diversity of datasets and data feeds. Therefore, we have qualitatively new data. Planetary level structured data. From that, we can build qualitatively new models, that make relations which among inputs & outputs which weren't connected before. With the models and from the models, we will get qualitatively new insights.

I wish I could be more specific here, but at this point it's so new that I can't think of any examples. But, they will emerge!

There's also a bot angle. We've been assuming that the main consumers of blockchain APIs will be humans. But what if it's machines? David Holtzman, creator of the modern DNS, said recently "IPDB is kibbles for AI". Unpacking this, it's because IPDB enables and encourages planet-level data sharing, and AI really loves to eat data.

Opportunity 3: Audit trails on data & models for more trustworthy predictions

This application addresses the fact that if you train on garbage data, then you'll get a garbage model. Same thing for testing data. Garbage in, garbage out.

Garbage could come from malicious actors / Byzantine faults who may be tampering with the data. Think Volkswagen emissions scandal. Garbage may also come from non-malicious actors / crash faults, for example from defective IoT sensor, a data feed going down, or environmental radiation causing a bit flip (sans good error correction).

How do you know that the X/y training data doesn't have flaws? What about live usage, running the model against live input data? What about the model predictions (*yhat)*? In short: **what's the story of the data, to and from the model? Data wants reputation too.**

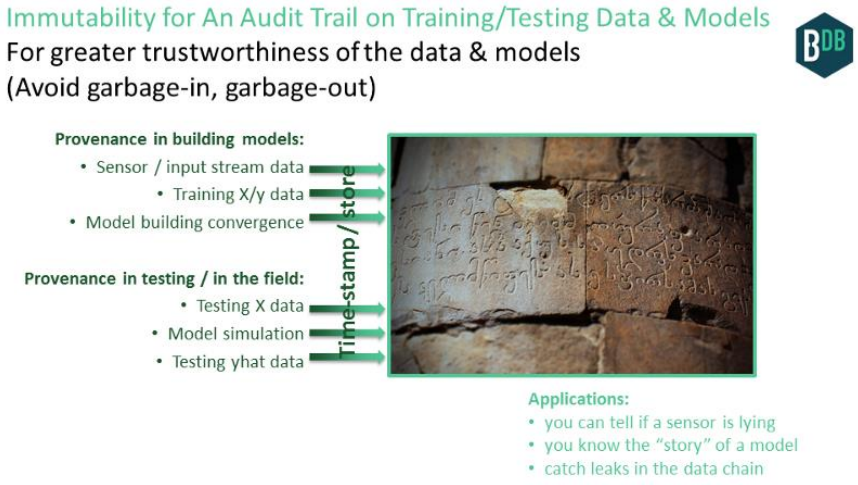

Figure 3.3 Immutability for an audit trail on data

Blockchain technology can help. Here's how. At each step of the process to build models, and to run models in the field, the creator of that data can simply time-stamp that model to the blockchain database, which includes digitally signing it as a claim of "I believe this data / model to be good at this point". Let's flesh this out even more…

Provenance in building models:

1. Provenance on sensor data (including IoT). Do you trust what your IoT sensor is telling you?
2. Provenance on training input/output *(X/y)* data.
3. Provenance on model building itself, if you like, via trusted executioninfrastructure, or TrueBit-style markets that double-check computation. At the very least, have evidence of model-building with the model-building convergence curve (e.g. *nmse* vs. *epoch*).
4. Provenance on the models themselves.

Provenance in testing / in the field:

1. Provenance on testing input *(X)* data.
2. Provenance on model simulation. Trusted execution, TrueBit etc.
3. Provenance on testing output *(yhat)* data.

We get provenance in both building the models, and applying them. The result is more trusted AI training data & models.

And we can have chains of this. Models of models, just like in semiconductor circuit design. *Models all the way down*. Now, it all has provenance.

Benefits include:

- Catch leaks in data supply chain (in the broadest sense), at all the levels. For example, you can tell if a sensor is lying.
- You know the story of the data and model, in a cryptographically verifiable fashion.
- You can catch leaks in the data supply chain. That way, if an error happens, we'll have a much better idea of how and where. You can think of it as banking-style reconciliation, but for AI models.
- Data gets a reputation, because multiple eyes can check the same source, and even assert their own claims on how valid they believe the data to be. And, like data, models get reputations too.

Opportunity 4: Shared global registry of training data & models

A specific challenge in the AI community is: where are the datasets? Traditionally, they have been scattered throughout the web, though there are some lists here and there

pointing to main datasets. And of course many of the datasets are proprietary, precisely because they have value. The data moat, remember?

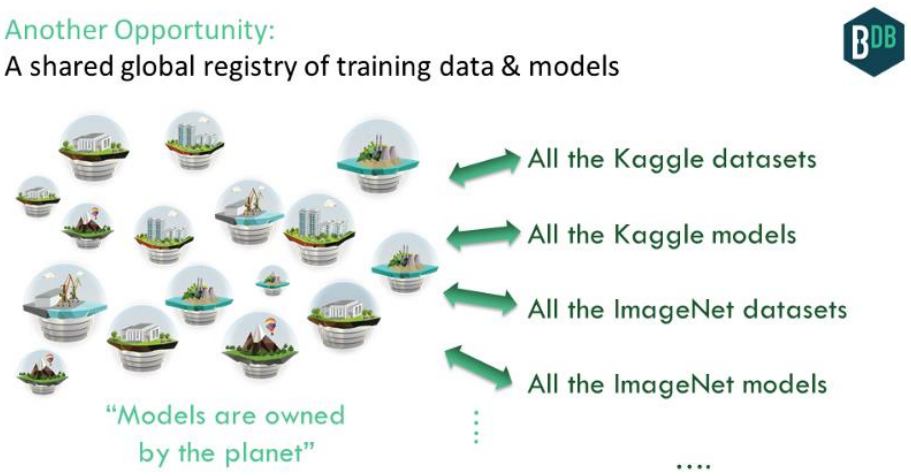

Figure 3.4 Shared global registry of training data& models

But, what if we had a global database that made it easy to manage another dataset or data feed (free or otherwise)? This could include the broad set of Kaggle datasets from its various ML competitions, the Stanford ImageNetdataset, and countless others.

That's exactly what IPDB could do. People could submit datasets, and use others' data. The data itself would be in a decentralized file system like IPFS; and the meta-data (and pointer to the data itself) would be in IPDB. We'd get a global commons for AI datasets**.** This helps to realize the dream of the open data community.

We don't need to stop at the datasets; we can include the models built from those datasets too. It should be easy to grab and run others' models, and submit your own. A global database can greatly facilitate this. We can get models that are owned by the planet.

Opportunity 5: Data & models as IP assets →data & model exchange

Let's build on the application of "shared global registry" of training data and models. Data & models can be part of the public commons. But they can also be bought & sold!

Data and AI models can be used as an intellectual property (IP) asset**,** because they are covered by copyright law. Which means:

- If you have created the data or model, you can claim copyright. This is whether or not you want do do anything commercially with it.
- If you have copyright of data or model, then you can license usage rights to others. For example, you can license your data to someone else to build their own model. Or,

you could license your model for someone to include in their mobile application. Sub-licensing, sub-sub-licensing, etc is possible too. Of course, you can license data or models from others too.

I think it's pretty awesome that you can claim copyright of an AI model, and license it**.** Data is already recognized as a potentially huge market; models will follow suit.

Claiming copyright of and licensing data & models was possible before blockchain technology. The laws have served this for a while. But blockchain technology makes it better, because:

- For your claim of copyright, it offers a tamper-resistant global public registry; where your claim is digitally / cryptographically signed by you. This registry can include data & models too.
- For your licensing transaction, it once again offers a tamper-resistant global public registry. This time, it's not just digitally signed; rather, you cannot even transfer the rights unless you have the private key. The rights transfer occurs as a blockchain-style transfer of assets.

IP on the blockchain is near and dear to my heart, with my work on ascribe going back to 2013 to help digital artists get compensated. The initial approach had issues with scale and flexibility of licensing. Now, these have been overcome, as I recently wrote about. The technology that makes this possible includes:

- Coala IP is a flexible, blockchain-friendly protocol for IP.
- IPDB (with BigchainDB) is a shared public blockchain database to store rights information & other metadata at Web scale**.**
- IPFS plus physical storage like Storj or FileCoin is a decentralized file system to store the large data & model blobs

With this, we get data and models as IP assets.

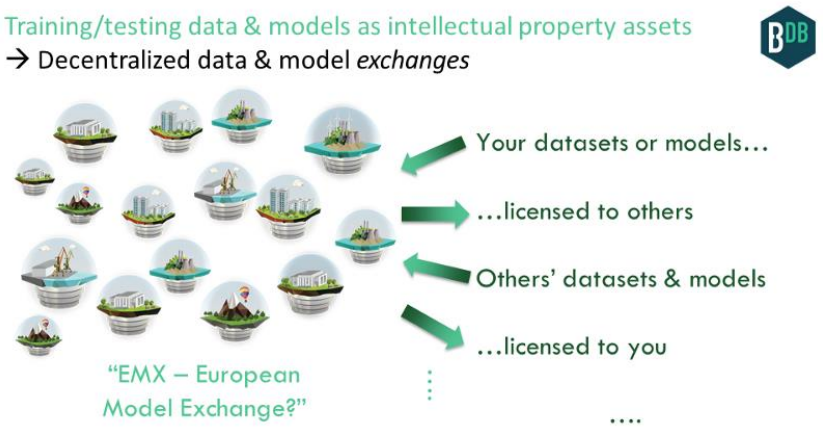

Figure 3.5 Decentralized data & model exchange

Opportunity 5a: Control the Upstream of Your Data & Models

This riffs on the previous application.

When you sign on to use Facebook, you're granting Facebook very specific rights about what they can and can't do with any data that you enter into their system. It's licenses on your personal data.

When a musician signs with a label, they're granting the label very specific rights, to edit the music, to distribute it, and so on. (Usually the label tries to grab all of copyright, which is super onerous but that's another story!)

It can be the same thing for AI data, and for AI models. When you create data that can be used for model-building, and when you create models themselves**,** you can pre-specify licenses that restricts how others use them upstream.

Blockchain technology makes this easy, for all the use cases, from personal data to music, from AI data to AI models. In the blockchain database, you treat permissions as assets where for example a read permissions or the right to view a particular slice of data or model. You as the rights holder can transfer these permissions-as-assets to others in the system, similar to how you transfer Bitcoin: create the transfer transaction and sign it with your private key. (Thanks to Dimitri de Jonghe for this.)

With this, you have far better control for the upstream of your AI training data, your AI models, and more. For example, "you can remix this data but you can't deep-learn it."

This is likely part of DeepMind's strategy in their healthcare blockchain project. In data mining healthcare data puts them at risk of regulation and antitrust issues (especially in Europe). But if users can instead truly own their medical data and control its upstream usage, then DeepMind can simply tell consumers and regulators "hey, the customer actually owns their own data, we just use it". My friend Lawrence Lundy provided this excellent example (thanks Lawrence!). He then extrapolated further:

It's entirely possible that the only way governments will allow private ownership (human or AGI) of data is with a shared data infrastructure with "network neutrality" rules, as with AT&T and the original long lines. In that sense, increasingly autonomous AI requires blockchains and other shared data infrastructure to be acceptable to the government, and therefore to be sustainable in the long term. -Lawrence Lundy

Opportunity 6: AI DAOs—AI that can accumulate wealth, that you can't turn off

This one's a doozy. An AI DAO is AI that owns itself, that you can't turn off**.** I've previously discussed AI DAOs in three posts (I, II, III); I'll summarize the "how" below. I encourage the interested reader to dive deeper.

So far, we've talked about blockchains as decentralized databases. But we can decentralize processing too: basically, store *state* of a state machine. Have a bit of infrastructure around this to make it easier to do, and that's the essence of "smart contracts" technologies like Ethereum.

We've had decentralized processes before, in the form of computer viruses. No single entity owns or controls them, and you can't turn them off. But they had limits—they basically try to break your computer, and that's about all.

But what if you could have richer interactions with the process, and the process itself could accumulate wealth on its own? That's now possible via better APIs to the process such as smart contracts languages, and decentralized stores of value such as public blockchains.

A Decentralized Autonomous Organization (DAO) is a process that manifests these characteristics. It's code that can *own* stuff.

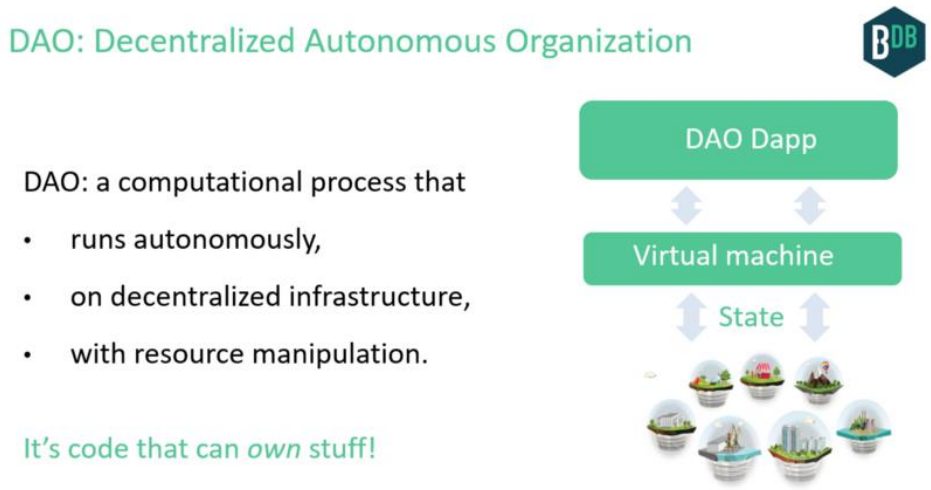

Figure 3.6 Decentralized Autonomous Organization

Which brings us to AI. The AI sub-field called "Artificial General Intelligence" (AGI) is most relevant. AGI is about autonomous agents interacting in an environment. AGI can be modeled as a feedback control system. This is great news, because control systems have many great qualities. First, they have strong mathematical foundations going back to the 1950s (Wiener's "Cybernetics"). They capture the interaction with the world (actuating and sensing), and adapting (updating state based on internal model and external sensors). Control systems are widely used. They govern how a simple thermostat adapts to a target temperature. They cancel noise in your expensive headphones. They're at the heart of thousands of other devices from ovens to the brakes in your car.

The AI community has recently embraced control systems more strongly. For example, they were key to AlphaGo. And, AGI agents themselves are control systems.

An AI DAO is an AGI-style control system running on a decentralized processing & storage substrate. Its feedback loop continues on its own, taking inputs, updating its state, actuating outputs, with the resources to do so continually.

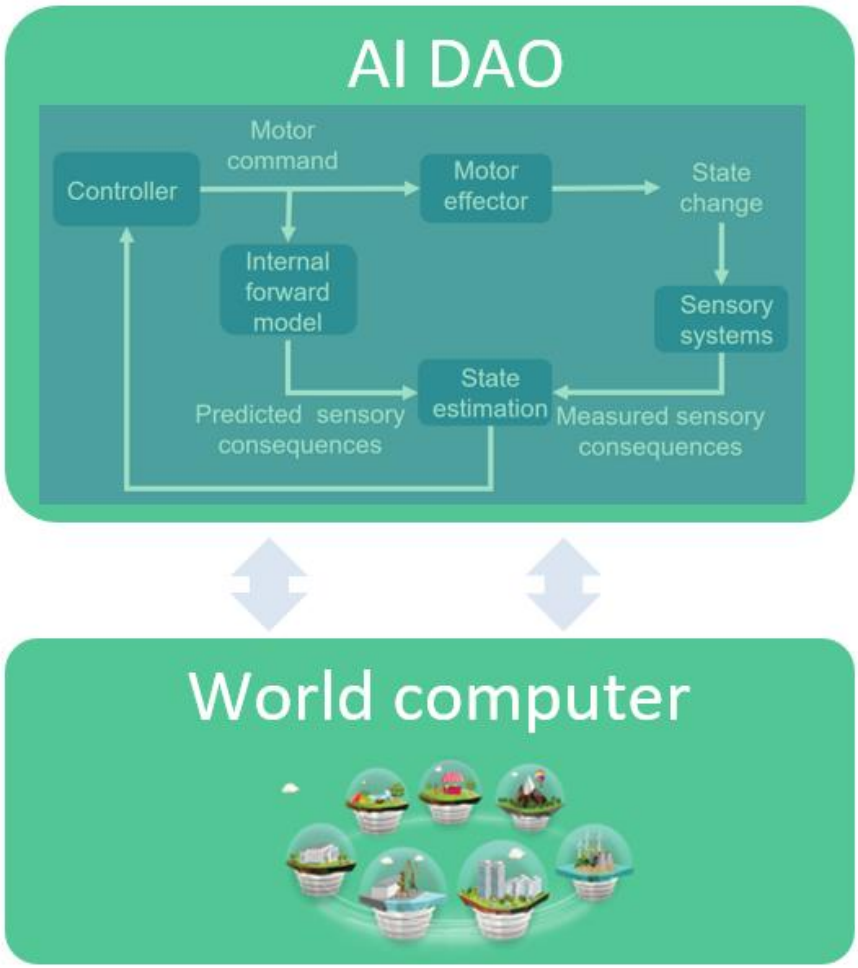

Figure 3.7 Architecture of AI DAO

We can get an AI DAO by starting with an AI (an AGI agent), and making it decentralized. Or, we can start with a DAO and give it AI decision-making abilities.

AI gets its missing link: resources. DAO gets its missing link: autonomous decision-making. Because of this, AI DAOs could be way bigger than AIs on their own, or DAOs on their own. The potential impact is multiplicative.[7]