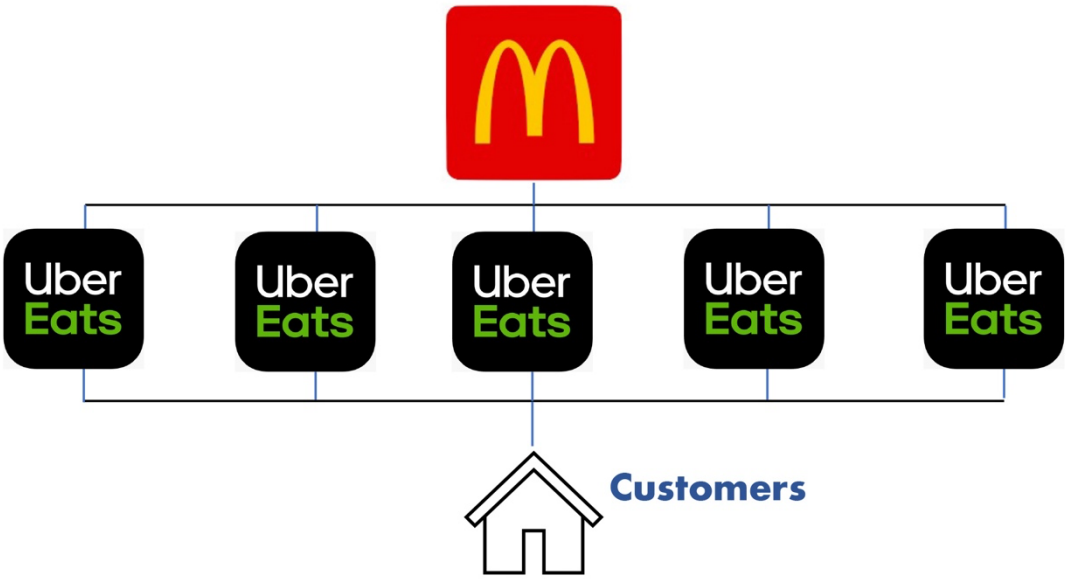
Blockchain's Next Act and Real-World Data



trademarks property of McDonald's Corporation and Uber Technologies respectively

…and the Illusion of UberEats DeFi Solutions

A blockchain's primary purpose is to enable efficient trustless transactions without an intermediary. With a simple collection of wallets, keys, and seeds, new users can trade and transfer digital currencies anytime anywhere. From there, new users can choose to transact on a selection of decentralized and centralized platforms to match their technical and security needs.

But now, everybody's waiting for blockchain's disruptive next act. Blockchain platforms are expected to transform securities markets, tokenizations, product provenance, and identification systems for healthcare, voting, and other "secure/private/transparent" environments. Blockchain looks like a good candidate where permanence, privacy, and selective transparency are desired.

Virtually every aspect of this next act has off-chain data integration at its core. For systems that get the integration right, entirely new markets will be possible. For projects that get the integration wrong, the setback to the blockchain ledger revolution could be widespread and permanent.

If It's Important, There's Only One Answer.

Trustless engagement and distributed validations are at the heart of most blockchain environments. Trustless protocols allow transactions without intermediaries, and distributed ledgers reduce single point of failure risk.

But is this same trustless/distributed model desirable or even useful with respect to off-chain data, blockchain oracles, and smart contract applications? Where outcomes are consequential and highly specified, does a plurality of delivery nodes and additional data values do anything practical?

When parties contract over an uncertain event (e.g. a stock price, a horse race), they should always want a singular and definitive outcome. For example, when trading options over Tesla, Microsoft, or Ether, the parties will not be interested in the consensus view of a closing price; they will be interested in a verifiable and auditable value which is derived with particular specificity and probably consistent with an official published result where possible.

Continuing with the Tesla example, there may be many "end of day" prices to find and report but using anything other than that single price determined by TSLA's primary exchange is wrong. Further, while it may seem comfortably busy for an army of affiliates or hobbyists to report lots of data points, the reality is likely to include duplicative or bad data passed through a common AWS gateway.

The "Uber Eats Solution" to Defi

Imagine a small town with one McDonald's location, where we're trying to validate both BigMac provenance and eliminate a single point of failure (e.g. an outage at the counter or drive-through).

A state-of-the-art oracles solution likely involves inserting an army of UberEats drivers in between the single McDonalds restaurant and its customers. The army of UberEats drivers would give the illusion of removing the single point of failure risk because there are many of them, and oracle operators might argue that outcome-provenance has improved because the driver's reputation would be damaged if s/he attempted to deliver counterfeit BigMacs.

Like in our Tesla example, actual consumers of the data (or BigMacs) have not benefited from the trustless and distributed arrangement; the local McDonalds is either open or closed, and a BigMac is a BigMac.

The "Uber Eats Solution" gets worse in the cases of private data relating to enterprise blockchains, healthcare systems, and voting networks. A consensus view from a bunch of hobbyists or affiliated agents relating to a vaccine outcome or public health event is probably counterproductive.

While there's an intellectual appeal to maintaining a "defi" character and pretending that single source delivery-and-accuracy can somehow be eliminated, new markets and enterprise blockchain are likely to suffer from this orthodoxy.

And Then There's Speed and Scale…

Pioneering blockchain users have been patient with transaction times and transaction costs.

Retail and institutional commerce and finance are unlikely to flourish in environments where it takes time for the data values to wind themselves through a "trustless" maze. Further, paying

excessive data fees (for unnecessary data delays) is likely to stall many otherwise viable applications.

Plus Data is Usually Owned…

For the foreseeable future, distributed and decentralized systems will necessarily consume data from many conventional sources. Participants is CeFi (Centralized Finance) are accustomed to intellectual property and copyrights, where live prices from the NYSE, Nasdaq, or the World Gold Council are subject to strictly enforced licensing agreements.

Data services and data licensing can be one of the most expensive line items for many financial services and trading organizations. Best case, these DeFi oracle solutions duplicate costs. Worst case, they induce theft of service.

And We'll need to Audit That…

Even with the best intentions to reduce centralized data storage and value reporting vulnerabilities, all of these smart oracle systems can wind up with tremendous overhead, including a multiplication of the off-chain data storage problem they were trying to solve in the first place.

So…

Early systems of trustless data oracles usually begin with the mythology that unidentified ligher-than-cloud-based agents will gently impart real truths onto the blockchain through a construction of consensus protocols. Except in measures of social sentiment, consensus guided validation is not a substitute for direct accuracy.

Imposing a trustless/distributed data-values regime over blockchains, based on game theory, is a solution in search of a different problem. The intellectual exercise of trustless-truths needs to become a proper exercise in data provenance, tracing, and storage…and it usually does.

Over the past few years, certain projects have pivoted from an exercise of temporal collective wisdom, to the proper tracking, tracing and storage of values. In the transition, the processes and challenges have changed to the integration of layered-and-linked storage where there's real auditability and repeatability of who's providing what values…remembering, if it's important, there's usually only one value.

# # #