Bitcoin Suisse | Decrypt

September 10, 2019 | Season 1 Episode 8

Connecting Blockchains to Real Life

Unleashing the full potential of blockchain technology will require a constant feed of data from the off-chain world. How can this link be established?

Written by Dr. Raffael Huber from Bitcoin Suisse Research
and Demelza Kelso Hays and Mark J. Valek from incrementum

A major selling point of blockchains is the ability to cut out middlemen and save costs by enabling previously impossible levels of automation. For example, a codified flight cancellation insurance contract on a blockchain could instantly reimburse an unlucky passenger whose scheduled airplane never took off. This would remove a lot of bureaucratic steps and improve the customer experience while saving friction costs for the insurance company. But there is one issue – how does the smart contract know that the airplane remained on the ground?

Providers of real-life data are called *oracles*. For a blockchain, such **oracles are sources of truth about the outside world**. In the example above, an oracle would confirm the validity of the insurance claim, possibly leading to a payout to the beneficiary.

> *"Oracles exponentially increase the scope of what crypto can do."*
> *– Ari Paul*

The use cases for oracles are broad. In the world of the future, where blockchain supports the financial infrastructure or entire smart cities, a continuous stream of off-chain data will be required to unlock the full potential of blockchains. Already today, oracles are essential for decentralized finance (DeFi) platforms. MakerDAO, for example, the issuer of the DAI stablecoin with more than 1.4 million ETH locked as collateral for loans,[1] relies on accurate price feeds to determine whether a loan still has enough collateral locked up or needs to be liquidated. As such, both MakerDAO and its DeFi peer Compound have recently launched initiatives towards improving their oracle systems.[2,3]

The value proposition of blockchains strongly depends on their level of decentralization. A system is only as decentralized as its least decentralized part. As such, **it is crucial that oracles are just as devoid of single, centralized points of failure as the underlying blockchain**.

The damage that misreporting by oracles can cause was illustrated by the Libor scandal. Banks deliberately manipulated the Libor to benefit their trading positions, resulting in almost $10 billion in fines.[4] As such, the network of oracles that set the Libor was not sufficiently

1. https://defipulse.com/maker
2. https://blog.makerdao.com/introducing-oracles-v2-and-defi-feeds/
3. https://medium.com/compound-finance/announcing-compound-open-oracle-development-cff36f06aad3
4. https://www.cfr.org/backgrounder/understanding-libor-scandal

decentralized and not collusion resistant. The economic gains of misreporting seemed to outweigh the financial risks. This shows that a system of oracles needs to be carefully designed such that the game-theoretical equilibrium incentivizes honest reporting.

> *"Centralized oracles fundamentally go against the security model of our space, because you once again have a single point of failure."*
> *– Sergey Nazarov*

To increase the probability that data provided by oracles is correct, two layers of redundancy should be considered. First, multiple sources for the requested real-life data ensure that, for example, a single malfunctioning sensor cannot corrupt the whole network that pulls data from it. Secondly, the more independent oracles attest to the validity of an off-chain input, the more likely it becomes that the input is indeed true.

Is the Wisdom of the Crowd an Alternative Source of Truth?

A second strategy for harnessing the truth about the outside world is to use information from prices in financial markets. All markets capture our predictions of the future. Futures markets for oranges contain the market's predictions for Florida weather. Catastrophe bonds price in the market's predictions of catastrophic weather events like hurricanes and floods.

Prediction markets are markets that are designed specifically to predict the outcome of a future event. For example, who will win the 2020 election in the US? Individuals can bet on the outcome of events by buying and selling shares on online marketplaces. Trading the shares on an exchange enables price formation, and this price can be used as a proxy for the probability of an outcome happening in the real world. The price is a single point of data that can be fed into oracles and smart contracts.

Prediction markets capture collective wisdom and have been shown to be more accurate on average than expert opinions and survey polls. In the famous trivia show, *Who Wants to be a Millionaire*, polling the audience gives a correct answer 91 % of the time compared to 66 % when phoning an expert.

The roots of internet prediction markets began in the 1980s at Libertarian tech meetups in Palo Alto. Robin Hanson and others tried to find technological ways to improve the fact-seeking process on the internet. The first attempt was to make *threads* of conversations online so that internet users could see the main arguments and rebuttals in a debate. Gradually, this concept evolved into a prediction market because people needed to have a financial incentive in order to divulge their information and "participate honestly" in the debate.

Intrade.com was one of the largest prediction markets. Most topics were related to sports, but certain geopolitical questions garnered the website a politically incorrect reputation. For most of 2003, contracts for the capture of Saddam Hussein traded at 40 cents. This meant that there was a four percent chance that Saddam Hussein would be captured within the year. In the second week of December, the contract's trading volume skyrocketed. When the capture of Hussein was publicly announced on December 13, Hussein contracts had a return of 2'500 percent.

The ability for prediction markets to accurately predict precise outcomes means that certain traders do have insider information. Allowing insiders to profit from their knowledge can be seen as bad by regulators, but on the other hand, the trading results can effectively reduce asymmetric information. However, the larger looming question is how to regulate prediction markets. After all, the Hussein contract was effectively an assassination market.

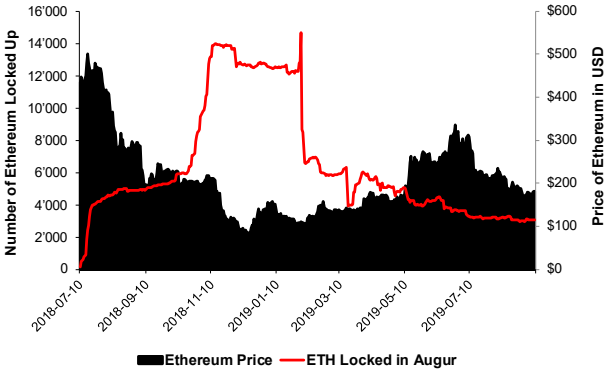
Operating prediction markets on the blockchain technology is important because prediction markets get shut down by corporations or the government. Intrade.com and the Policy Analysis Market were both shut down by the US government. Strangely enough, the Hollywood Stock Exchange has successfully dodged US regulators.

> *"The most heeded futurists these days are not individuals, but prediction markets, where the informed guesswork of many is consolidated into hard probabilities..."*
> *– The Economist: The Future of Futurology*

The two largest blockchain-based prediction markets are Augur (REP) and Gnosis (GNO). They are both a collection of smart contracts that are built on Ethereum. The idea is that anyone can create a prediction market about anything.

Augur investors that invested in the initial coin offering in 2015 paid approximately 60 cents per token, and the current price is $10.52. Augur has approximately a $124 million market capitalization and $7.1 million in average daily trading volume over the past year. The total value of approximately $545,000 worth of Ethereum is locked up by Augur smart contracts.[5]

Illustration 1: The number of total ETH locked up in Augur prediction markets peaked in February of this year.



Source: aleth.io, Incrementum AG.

However, we have a long way to go with prediction markets. The largest problem is low liquidity. Market-making on decentralized blockchains has high costs because order books are on-chain. If you have to update or cancel the order, you have to pay a transaction fee. Augur has seen bidding costs as high as one dollar already. Another problem is that decentralized blockchains can only process a limited number of transactions per section as we mentioned in Bitcoin Suisse Decrypt Season 1 Episode 5. Augur, for example, can do approximately four transactions per second.

Oracles are key to moving blockchains from their mostly siloed existence to a more impactful one for our everyday lives. **Only once a trustless, reliable connection to the outside world is established, will we witness the true power of smart contract platforms**.

5. https://defipulse.com/augur

Bitcoin Suisse AG
CH-6300 Zug
bitcoinsuisse.com

in collaboration with

incrementum