THEME 01

Where the blockchain meets the real world

technological innovation | blockchain | oracles

Blockchain technology promises to automatically process all sorts of digital transactions without mistakes and or possibilities for fraud. Not only does this make for reliable processing of payments or contractual agreements, it also ensures highly scalable and potentially cost-efficient processes that require no trusted intermediaries. Yet, these so-called trustless systems still need to be provided with reliable input and they need a means of executing their outcomes. In other words, the interface between the blockchain and the real world is of crucial importance and it is no wonder that many initiatives seek to develop reliable and scalable solutions to this.

Our observations

- Developers sometimes refer to data and processes that take place inside the blockchain as on-chain, and to everything outside that realm as off-chain. We've previously noted that this interface is one of the challenges blockchain technology still faces.
- In the public debate, blockchain technology is still mostly understood as an alternative means of settling financial transactions, such as with Bitcoin. In these cases, end users order a specific transfer of assets and the blockchain processes and stores the transaction in such a way that no one can alter or reverse it.
- More elaborate applications include so-called smart contracts that execute predefined agreements between stakeholders. Typically, these smart contracts describe specific conditions that, when they are met, set in motion the execution of an agreed transaction (e.g. the unlocking of a bicycle in a bike-sharing scheme or the paying out of an insurance fee in case of extreme weather).
- In the betting sector, several blockchain-based platforms offer a wide range of betting options that are processed automatically, from determining odds to accepting bets and paying winning bettors. These platforms obviously need reliable input, e.g. about sports results.
- So-called oracles feed the blockchain with real-life data. This might concern (semi-)public data that can be extracted from some database through standardized APIs or more elaborate AI systems that search and verify data on their own (i.e. software oracles), but can also be obtained by sensors that collect data from the real world, such as a car entering a parking garage or a product moving through a logistical process (i.e. hardware oracles). Finally, there are also human oracles who can provide the system with data. Initiatives such as Chainlink and Provable offer an oracle-as-a-service by retrieving and evaluating data from different sources.
- In theory, each of these types of oracles can be tampered with. Databases can be hacked and altered, sensors may be fooled and their signals forged and human oracles can have bad intentions themselves or be forced to provide false information. Because of this, developers of oracle systems will typically collect data from multiple sources and might rely on multiple sensors (even from different manufacturers).
- Initiatives using the crowd to source input for smart contracts, such as Realitio, need to verify the quality of that data and these platforms either use a majority vote (i.e. the most frequently provided answer is accepted as true) or a system in which data providers risk a penalty (i.e. have "skin in the game") when they provide false answers.

>> see next page

Connecting the dots

We have become used to using intermediaries to handle data, to process financial transactions (i.e. banks) and to verify and enforce contracts (i.e. lawyers and notaries). We have also grown used to trusting these and, to be sure, to devising ways of verifying their trustworthiness. For the most part, these trusted parties have served us well, but they are also costly, limited in their abilities (e.g. in terms of processing speed) and they may, despite all checks and balances, commit fraud.

Blockchain technology, and smart contracts in particular, offer an alternative in the form of trustless systems that can execute agreed-upon terms automatically and irreversibly without the interference of (human) intermediaries. Basically, a smart contract is a piece of code that contains the terms of a contract (typically in some kind of if-then expression) that will be executed once the predefined conditions are met. Given that this is code, and computers practically don't make mistakes, the contract will always be executed.

Yet, it is exactly this promise of infallible and impossible-to-tamper-with handling of data and transactions, on-chain, that shifts attention to the imperfections of real-world information and transactions. For instance, in food value chains, blockchain could help to empower small farmers and ensure they get a better price for their produce (i.e. by recording how much a farmer was paid for his produce). While such data cannot be altered once it's on-chain, it is very difficult to establish whether the farmer actually received the recorded amount of (cash) money (off-chain). Moreover, because there are no trusted intermediaries and everything takes place automatically, false input into a blockchain or failure to execute its output in the real world can spell disaster (e.g. automated payments on the basis of fake sports results).

There are basically two approaches to this problem. One might try to extend the reach of the blockchain by further digitizing the processes and bringing them on-chain. On the input end, software- and hardware oracles can, for instance, extract data from existing databases or generate data through sensors (e.g. smart cameras). On the output, or execution, end, all sorts of electronic hardware may be used to effectuate decisions reached on-chain. This may include smart locks, vending machines or even more elaborate robots. Still, bringing more real-life events on-chain through digitization merely shifts the problem. In the example of the farmer, for instance, he could be paid directly through the blockchain in a cryptocurrency, but this does not rule out the possibility of the farmer being forced to supply a disproportionate amount of produce or extorted to pay back (in cash) some of this money. Even further digitization could partially solve this problem, e.g. by digitally earmarking the farmer's pay so that it can only be used to pay for food or rent, but, again, this would merely lead to an arms race and shift the problem further.

The other approach is to develop scalable ways of acquiring reliable data from human sources and to use humans on the output end as well (i.e. to follow through on decisions made on the blockchain). These may use as many human oracles as feasible and take the majority or average of their "votes" as input for the blockchain. They may also introduce elements of gamification and issue rewards and penalties to those providing good and bad data. Obviously, these approaches work best with rather generic data such as sports results or other data that many (human) oracles can acquire simultaneously. In the case of small farms and the prices of their crops, these approaches would not work, as only the farmer and the middleman know what price was paid. In edge cases like these, when digitization and crowd-sourced data don't necessarily produce reliable results, and the fulfillment of conditions is difficult to verify, we may still have to rely on old-fashioned trusted intermediaries such as fair-trade organizations, lawyers and notaries. On the one hand this limits the scalability and added-value of blockchain solutions in these cases, yet, on the other hand, the use of blockchain technology may still add value in these cases as it introduces more transparency and, at least, makes for more efficient and reliable processing of data, even when that data itself is not flawless.The bottom-line here is that blockchain-based solutions still hold great promise, but also that its most valuable applications are cases in which digitization is almost complete (e.g. in media, gaming or some parts of finance and public administration) or data is generally available.

Implications

- **While a blockchain network on its own has no single point of failure (because the data is stored on so many computers), any oracle presents a vulnerability. A provider of external data might choose to falsify it, or a third party may interfere to tamper with data or sensors.**
- **In the end, for smart contracts to be meaningful in the real world, they should have legal status, similar to regular contracts, in order for the judicial system to be able to uphold one's rights (e.g. the police could be asked to step in to effectuate some decision produced by a smart contract). At the same time, the decentralized nature and broader ambitions of the "blockchain movement" somehow undermine the status quo.**
- **As we noted before, given the deliberate ambiguities we find in current law and regulation, it is questionable whether this can and should be captured in code or smart contracts. This presents a limitation for the application of smart contracts, which are most suited for business agreements and relatively simple contracts (of which there are plenty).**

>> see next page