Blockchain Critical Feature for Enterprises: Privacy

Original: https://www.btcc.com/en-US/academy/research-analysis/blockchain-critical-feature-for-enterprises-privacy

Blockchain Privacy is Really Hard

Central to the magic of blockchain technology is the consensus algorithm, the tool that maintains the validity of the entire network. The simplest way to understand a consensus algorithm is that it involves everyone being able to check everyone else's work. Zero-knowledge proofs (ZKP) are an almost magical form of math that allow you to provide mathematical proof that a statement is true without providing the underlying supporting data. Using ZKPs, we can replace actual data with a proof, maintaining the integrity of the network but enabling user privacy.

ZKPs are themselves hard to implement and run efficiently. Zcash pioneered their use on a blockchain in 2016 and Ethereum incorporated some key changes making them possible in 2017. Given the immense time and cost involved in implementing blockchain privacy, it's reasonable to wonder if it's worth all the time and effort. When it comes to enterprise usage, there can be no doubt. For some applications, such as fungible financial assets, public blockchains without privacy are not so far away from stock exchanges and other public markets where it is possible to see price and volume but not have a good idea of who is buying or selling.

It's a different story if you are moving around tokens specific to your product. In those cases, you're now showing lots of business information – like your production rate, inventories and sales. Companies strongly prefer to keep that kind of data under wraps.

The Benefits of Blockchain

Blockchains represent a terrific opportunity to erase the data silos between companies with standardized and integrated information. Companies could represent their inventory movements as the transfers of digital tokens. Because a token can only be owned by one participant at a time, the system forces reconciliation between parties and will result in much higher accuracy.

Not only would blockchain-based supply chains be much more accurate, they would also be much more efficient. Companies today must painstakingly match up purchase orders, invoices and shipments and then verify that prices paid are in alignment with those agreed in the master contract between buyer and seller. On-chain, smart contracts would automatically keep track of prices, applying volume discounts and rebates, and automating payments when deliveries are made.

We can cut the cycle-time required to handle documents by more than 90% on a blockchain and the cost of administration by around 50%. Unfortunately, without strong privacy, none of this is going to get widespread adoption. If a company were to implement these processes today, their competition would instantly be able to see how much it was producing, how much it was buying in raw materials, its key sales markets, and even the prices paid all along the supply chain. Data points like these are often among a company’s most closely guarded secrets.

The good news is that, after a long wait and a lot of effort, robust privacy tools for enterprises are on the way. Using Ethereum layer 2 networks such as Polygon Nightfall, it will be possible to trade financial tokens as well as privately transfer supply chain tokens. For those holding the tokens, they will have access to history information and traceability. But to external observers, all they will see is a continuous flow of mathematical proofs.

Secure, private token transfers are a good start, but they don’t reflect the whole picture. The second part of the puzzle is how to enable secure business logic so smart contracts can execute business logic in addition to simply moving tokens privately. If you think about the typical business agreement between two parties, it involves the exchange of money for stuff under the terms of an agreement.

Digital tokens are great for representing both the “money” and the “stuff” whether they are real or virtual, crypto or fiat.

Privacy Technology

The agreement part is more complicated. Agreements typically include complex logic such as, “If I spend more than $1 million dollars, reduce all my list prices by 10% for the rest of the calendar year.” Turning this into private logic that is both secure and scalable is more challenging but also achievable. There are several approaches that can be used here, including asking both parties to do the same calculations off-chain and compare results as well as converting the entire logic into a mathematical circuit based on a zero-knowledge proof.

Privacy matters. The internet before widespread encryption was an interesting place, but it wasn’t commercially very useful. Every message, every transaction occurred in full public view. It was only the arrival of scalable public key encryption built into the web browser that suddenly turned the internet into the world’s commercial infrastructure. Before then, inputting your credit card number into a web form was only for the most foolishly daring among us. When we look back upon the history of blockchain technology, I think we will come to see the widespread deployment of privacy technology in the same light.