# Privacy on Public Blockchains:

# EY Clients and the Blockchain Curious Must Leverage this "Best of Both Worlds" Breakthrough

Excerpt for EY

December 2019

Sam Duncan, Research Analyst

Defining Future Business Operations

# Privacy on public blockchains: EY clients and the blockchain curious must leverage this “best of both worlds” breakthrough

For years, blockchain has been labelled “a solution looking for a problem.” Combined with intense hype, it has been considered for every problem ranging from the world hunger crisis to the mystery of who left the office door unlocked last week. We’re finally seeing genuine applications for blockchain emerge to deliver tangible business value, be it offering a decentralized energy marketplace or enhanced drug provenance. However, one of the biggest debates rages on—between public and private blockchains. For anybody investing in or considering blockchain technology, specifically EY clients, the firm’s recent efforts could eliminate one of the key conundrums and turn speculative blockchain exploration efforts into genuine applications and value.

At the recent EY EMEIA Blockchain Summit in Paris, Paul Brody, the firm’s global blockchain leader, explained how EY is moving the enterprise gaze toward public blockchains that leverage zero-knowledge proofs (ZKPs). EY is solving the historic issue of privacy on public blockchains as ZKPs afford EY’s enterprise clients all the benefits of a public blockchain while maintaining privacy.

## Many enterprises overlook public blockchains as they simply cannot leave their data for the world to see

Using private blockchains or joining a blockchain consortium are implementations frequently favored by businesses over public blockchains, and it’s easy to see why. Public blockchains, by their very nature, allow anybody to participate in the network, whether reading the ledger or writing on it, meaning all transactions or smart contracts are completely visible. Private blockchains, on the other hand, and even consortiums, allow for a level of privacy as they aren’t truly decentralized; a single firm or a group of firms governs the network. This means private blockchains allow for all the benefits of a public blockchain—decentralization, smart contracts, and immutability, to name a few—while maintaining privacy for the enterprise—ensuring customers or competitors don’t have access to private data.

However, private blockchains aren’t the holy grail of decentralization; they require an intermediary firm to set up and maintain the entire network, whereas a public blockchain shares this cost across participants. Furthermore, the true benefit of blockchain is realized when many enterprises are

 

operating on the network, and this is more difficult to achieve when leveraging private blockchains. Ultimately, if there are a dozen private blockchains, firms will be fragmented between them rather than together on a single decentralized network. In the words of Paul Brody, EY's global blockchain leader, at its recent EMEIA Blockchain Summit in Paris:

*"If everybody throws a party on the same night, you're not going to have many attendees."*

## Zero-knowledge proofs are the first step toward genuinely private transactions on a public blockchain

The first step toward discovering public blockchains' missing ingredient, privacy, was the introduction of zero-knowledge proofs, allowing participants to encrypt their transactions while operating on a public blockchain. This method of cryptography offers the privacy many firms need, particularly those in the financial services sector, while allowing them all the benefits of a public blockchain. EY extensively researched the idea, and in October 2018, the firm launched the EY Ops Chain Public Edition prototype, which it claims was the first implementation of ZKP technology on the public Ethereum blockchain. Following this, in April 2019, the ZKP blockchain transaction technology was released in an experimental form to the public in the form of Nightfall.

In his keynote, Brody explained that while the cost per transaction began around the $100 mark, he believes it has now been significantly reduced to about $8 or $9. When dealing with high-value transactions, this is perfectly acceptable, but problems arise when dealing with high-volume, low-value transactions. Ultimately, if a firm is dealing with a thousand low-value transactions, the cost of using this form of cryptography may exceed the revenue generated from the transaction, essentially making it a non-starter.

But, as was the case with other popular methods of cryptography, it is likely that over time, the cost per transaction will continue to decrease. EY is aiming for a cost per transaction below a dollar, making private transactions on a public blockchain a genuine possibility. And this is something the firm achieved in December 2019 – by batching multiple proofs together EY was able to reduce the cost per transaction to approximately $0.05.

ZKP can already be seen in action with Zcash, a digital currency, proving this method of cryptography can be applied to blockchains.

The founders of Zcash recognized that while the transparency of other cryptocurrencies deterred cybercriminals—a definite benefit—it also dissuaded genuine individuals and enterprises alike from adopting the technology. By leveraging ZKP, the firm has created an encrypted open ledger. This means that while every transaction is recorded on the blockchain, they are also encrypted, and therefore only accessible to those who have the necessary permissions. Zcash stands as working proof that ZKP can be used in blockchains, and it was referenced in a blog post about the release of Nightfall.

## The Bottom Line: Blockhain bullsh*t is still out there, but thanks to firms like EY investing in research and development, we're starting to see real gold emerge as they tick off major challenges to enterprise adoption.

By now, we all understand the range of benefits blockchain can offer: optimizing processes, reducing costs, and providing transparency, to name a few. EY's continued efforts in blockchain research mean all of these benefits could be available on public blockchains with the crucial privacy that enterprises need. Ultimately, enterprises experimenting with blockchain must take note of EY's continued investments in blockchain, as should their current clients—specifically, delving into the introduction of ZKPs and Nightfall—if they hope to transform their experimentation with blockchain into genuine use-cases, benefits, and business value.

## HFS Research author

### SAM DUNCAN | Research Analyst

Sam is a Research Analyst at HFS. Sam is a recent graduate from Bournemouth University where he studied economics. During his studies, he took a particular interest in macroeconomics and global markets. Sam has also spent some time studying law, accounting, and investment management.

## About HFS Research: Defining future business operations

The HFS mission is to provide visionary insight into major innovations impacting business operations, including: automation, artificial intelligence, blockchain, Internet of things, digital business models, and smart analytics.

HFS defines and visualizes the future of business operations across key industries with our Digital OneOffice™ Framework.

HFS influences the strategies of enterprise customers to help them develop OneOffice backbones to be competitive and to partner with capable services providers, technology suppliers, and third-party advisors.

Read more about HFS and our initiatives on www.HFSresearch.com or follow @HFSResearch.