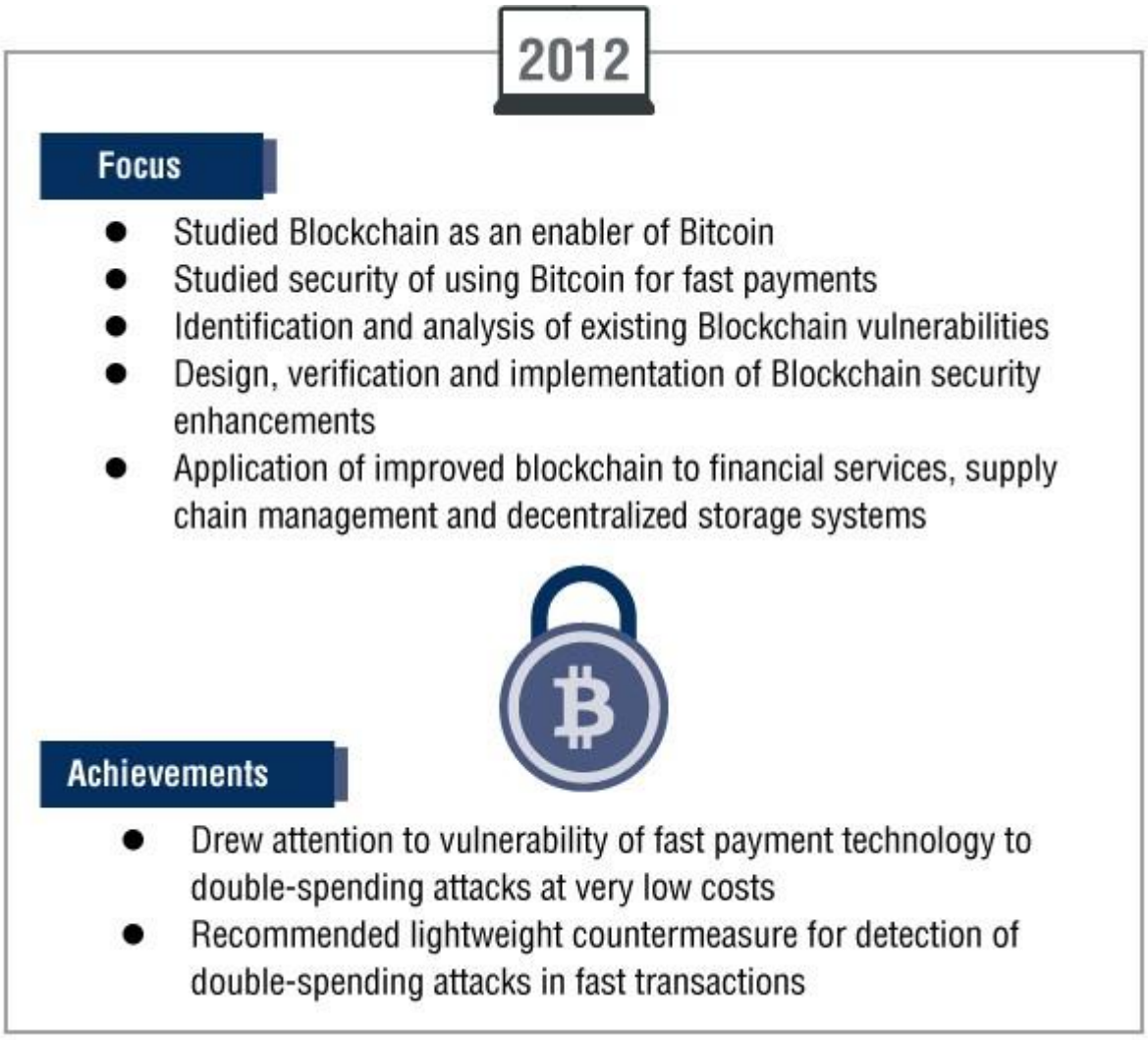
It Began with Bitcoin

NEC's research team recognized the potential of blockchain in 2012, when this technology was merely an enabler of Bitcoin.

In a bid to strengthen the global crypto ecosystem, the NEC team invested time in the:

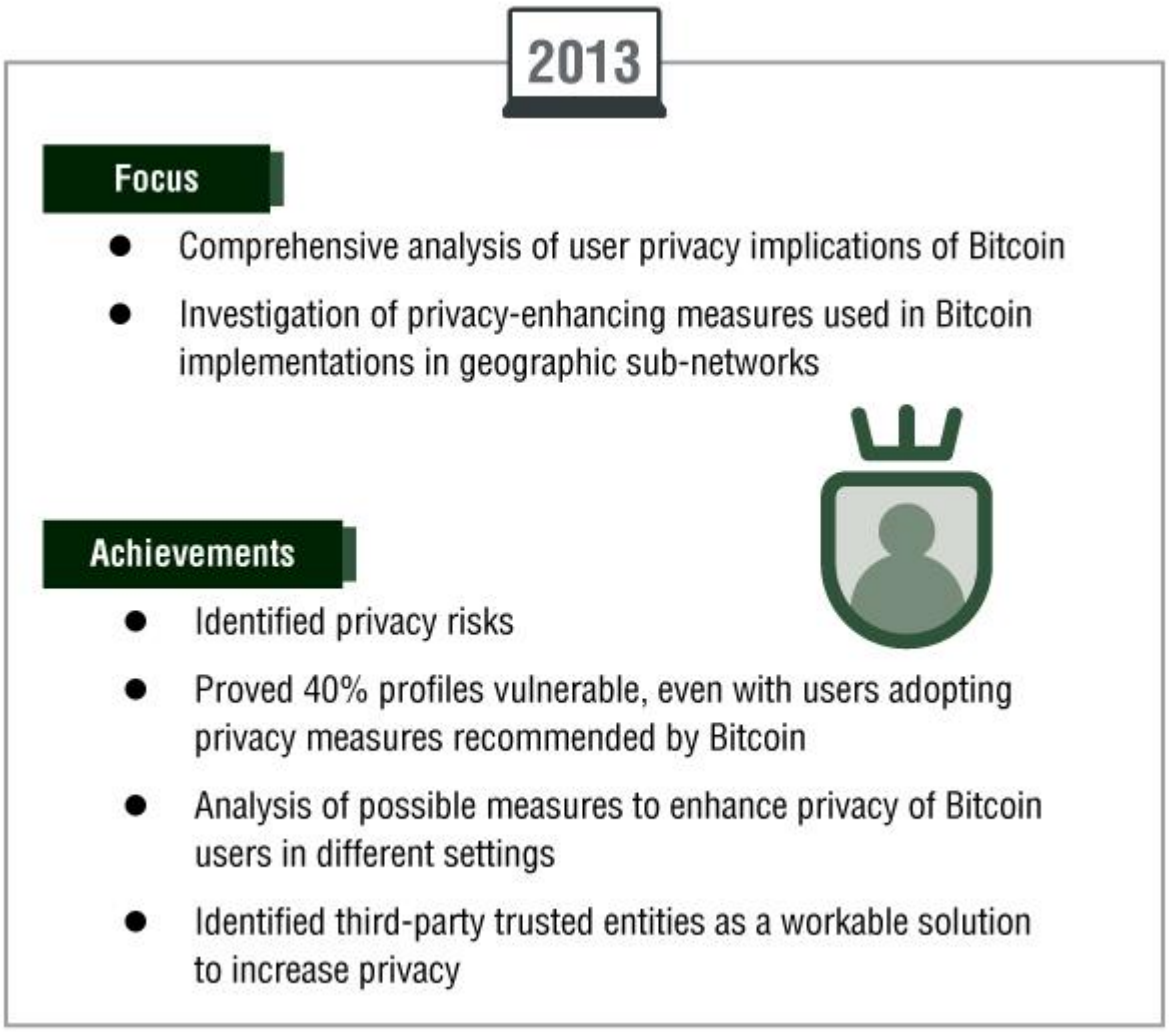
- Identification and analysis of vulnerabilities of Blockchain solutions
- Design, verification and implementation of Blockchain security enhancements
- Application of improved blockchain to financial services, supply chain
- management and decentralized storage systems



The team studied Bitcoin transactions and the security of using the digital currency for fast payments, when the time between exchange of currency and goods is only a few seconds.

The team found that double-spending attacks could be made on these fast payments at very low costs.

NEC recommended a lightweight countermeasure for the detection of double-spending attacks in fast transactions.



NEC proposed a solution to enhance Privacy and Security

By 2014, Lightweight Bitcoin clients were gaining increasing adoption among Bitcoin users.

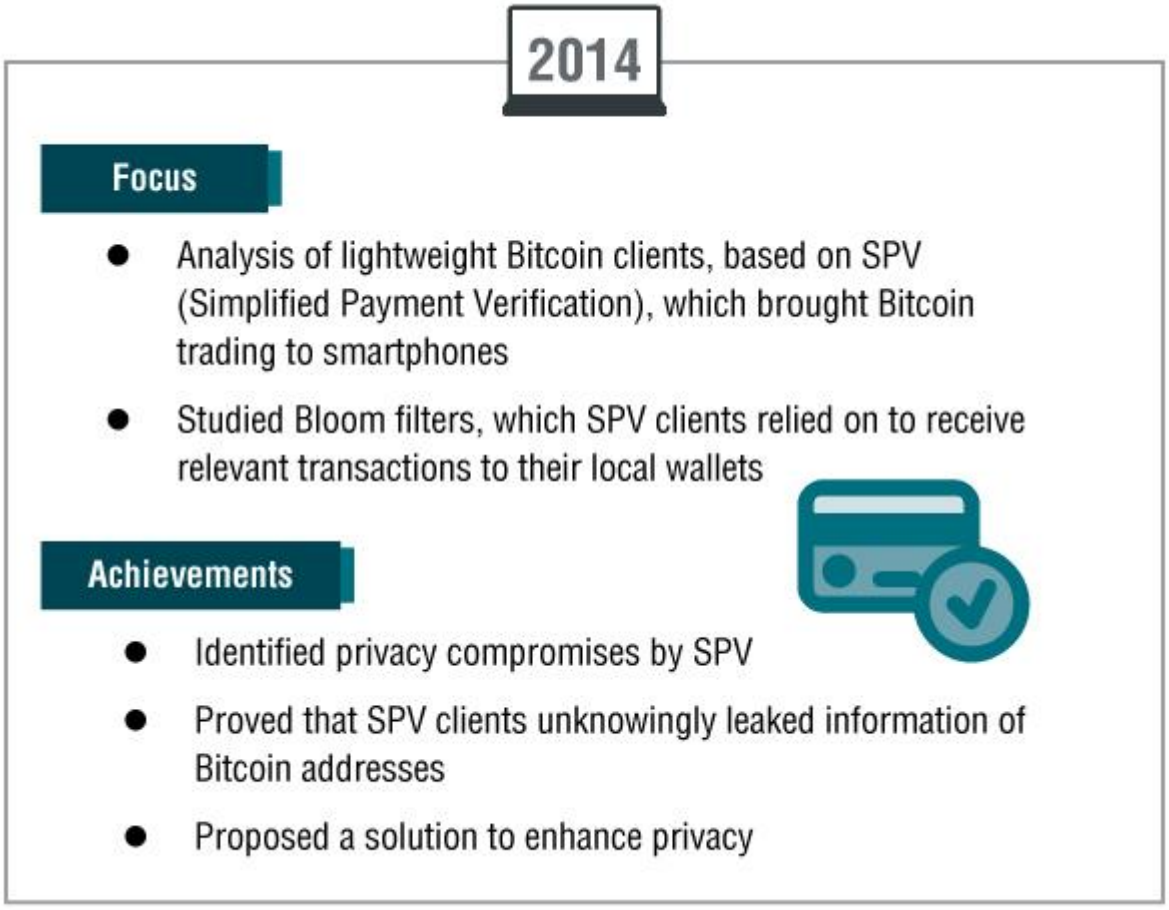
These were based on SPV (Simplified Payment Verification), which required users to download and verify only a part of a block in the chain.

SPV brought Bitcoin trading to smartphones.

SPV clients relied on Bloom filters to receive relevant transactions to their local wallets.

The NEC team and our partners determined that SPV compromised privacy.

Providing analytical and empirical proof, the team highlighted how SPV clients leaked considerable information of Bitcoin addresses, while also proposing a solution to enhance privacy.

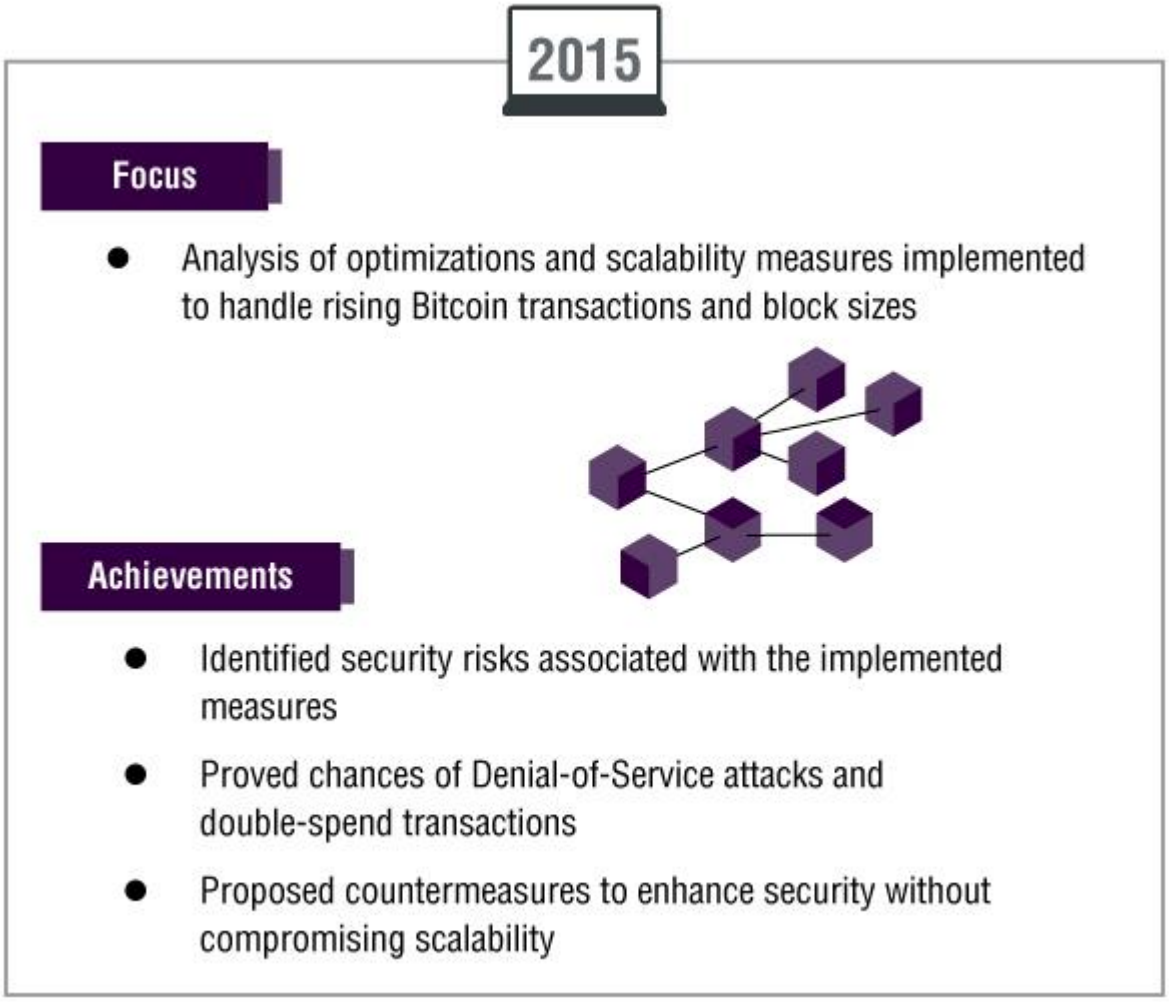


In 2015, there was a significant rise in the number of Bitcoin transactions and block sizes, which was only expected to increase.

To tackle this situation, Bitcoin implemented a number of optimizations and scalability measures.

NEC and our partners discovered that these measures came at the cost of security; and proved that an adversary could exploit them to mount Denial-of-Service attacks and cause double-spend transactions.

NEC and our partners proposed several countermeasures to enhance security without compromising scalability.



NEC developed a Blockchain for Enterprise Use

By 2016, Proof of Work (PoW) powered blockchains accounted for over 90% of the total crypto market capitalization.

The security provisions of variant (forked) PoW blockchains had not received much attention till then.

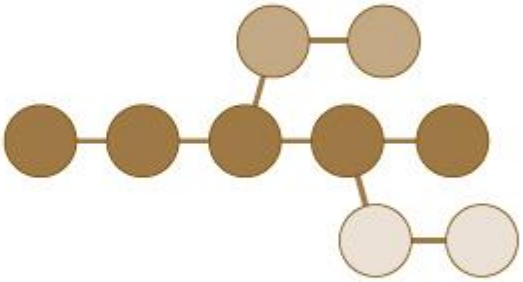
NEC and our partners proposed a novel quantitative framework to analyze the security and performance implications of PoW blockchains.

The framework took into account adversary attacks as well as real world constraints to facilitate comparisons of the tradeoffs between performance and security provisions.

2016

Focus

- Analysis of security provisions of variant (forked) Proof of Work (PoW) powered blockchains



Achievements

- Proposed a novel quantitative framework to analyze the security and performance implications of PoW blockchains
- Framework took into account adversary attacks and real-world constraints to facilitate comparisons of trade-offs between performance and security provisions

The team continues to study the impact of blockchain technology and to explore new horizons with this innovative technology, with the objective of empowering people, businesses and society.

2017

Focus

- Researching a blockchain that addresses security and privacy vulnerabilities
- Investigation of novel architecture to meet industry standards and practices
- Developing a blockchain for enterprise use

Achievements

- Developed a blockchain for enterprise use
- With strong security and privacy measures
- Allowing interoperable scalability
- Incorporation of policy management