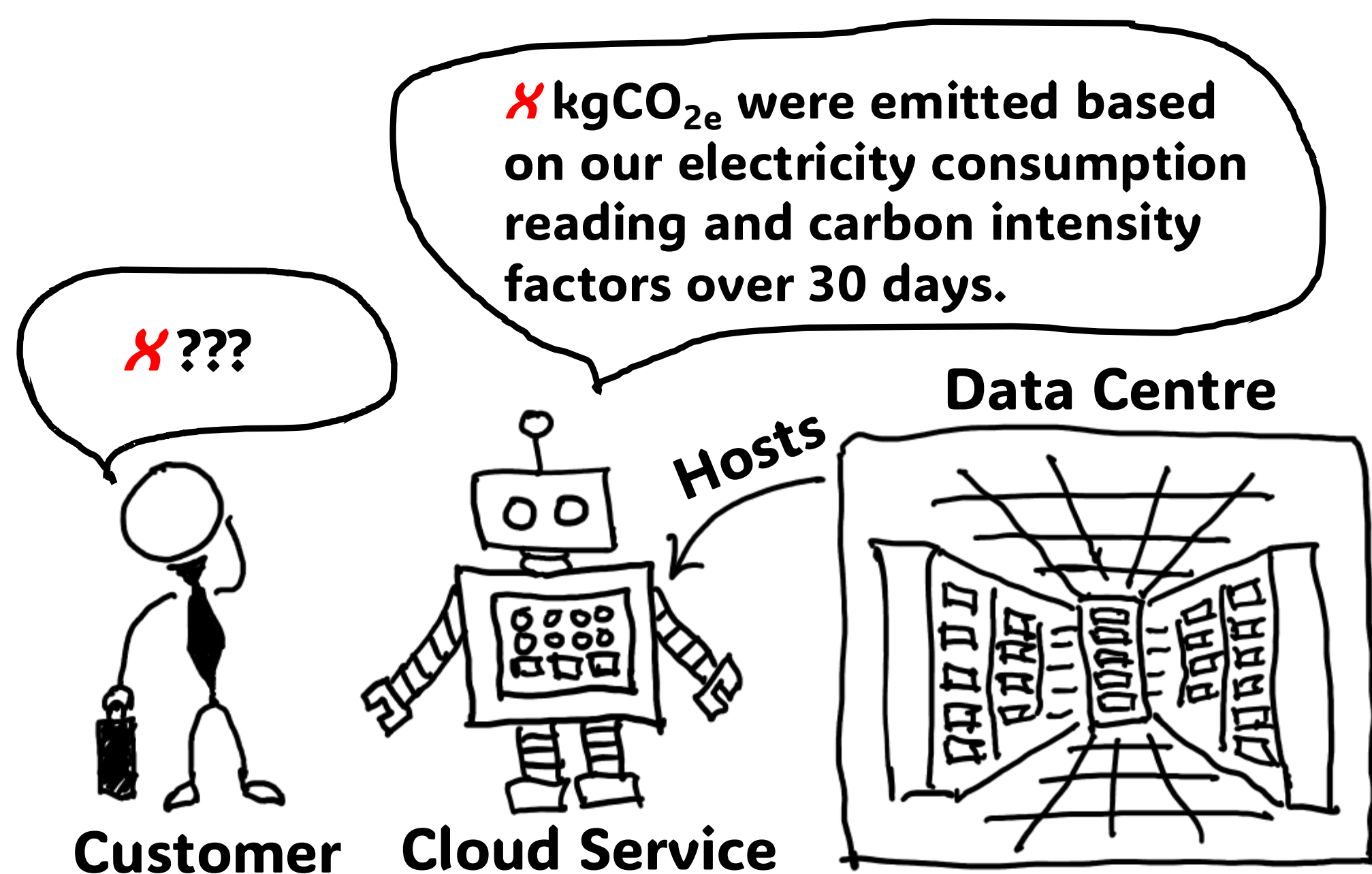


Emission Impossible

Verifiable and Scalable Carbon Emissions Reporting for Cloud Computing, without Revealing Private Data



There is little trust in the accuracy of sustainability data. Business initiatives and regulatory requirements mean that data-centre operators and their customers need to report the carbon emissions arisen from the use of computing resources. At present, these reports are neither verifiable nor required to be independently audited. Data-centre operators are not incentivised to accurately report all emissions, for business and competitive reasons.

Challenges

1. **Real-world vs System:** How to represent a real-world scenario as a proof system?
2. **Threats:** Adversaries want to learn business sensitive information, and data-centre operators want their report to look good.

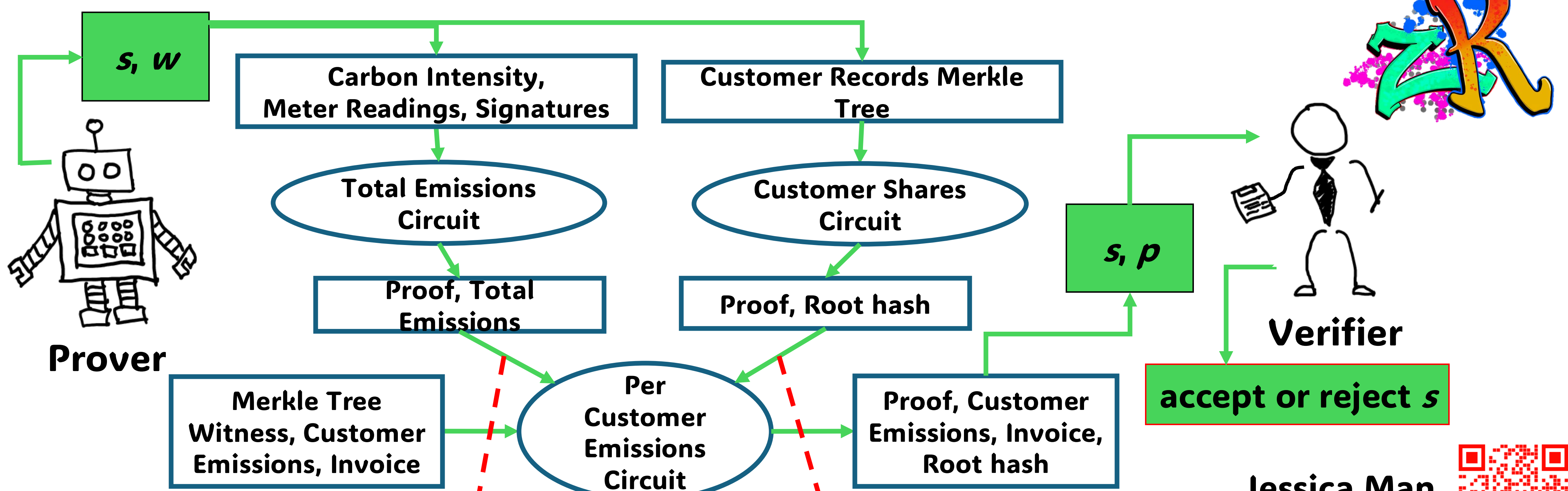
Our Contributions

1. Implemented a proof system with **zk-SNARK** that allows a data-centre operator to report verifiable emissions data to their customers.
2. Customers only learn the information they are explicitly given.
3. No emissions are omitted and allocations to customers are fair.
4. The system can scale to support more than one million customers with **RECURSIVE** zk-SNARK.

zk-SNARK: zero-knowledge Succinct Non-interactive ARgument of Knowledge



Public arithmetic circuit: $C(\text{public statement } s, \text{private witness } w) \rightarrow \text{Proof } p$



Proof output become input in the recursive step

Jessica Man
(psjm3)

