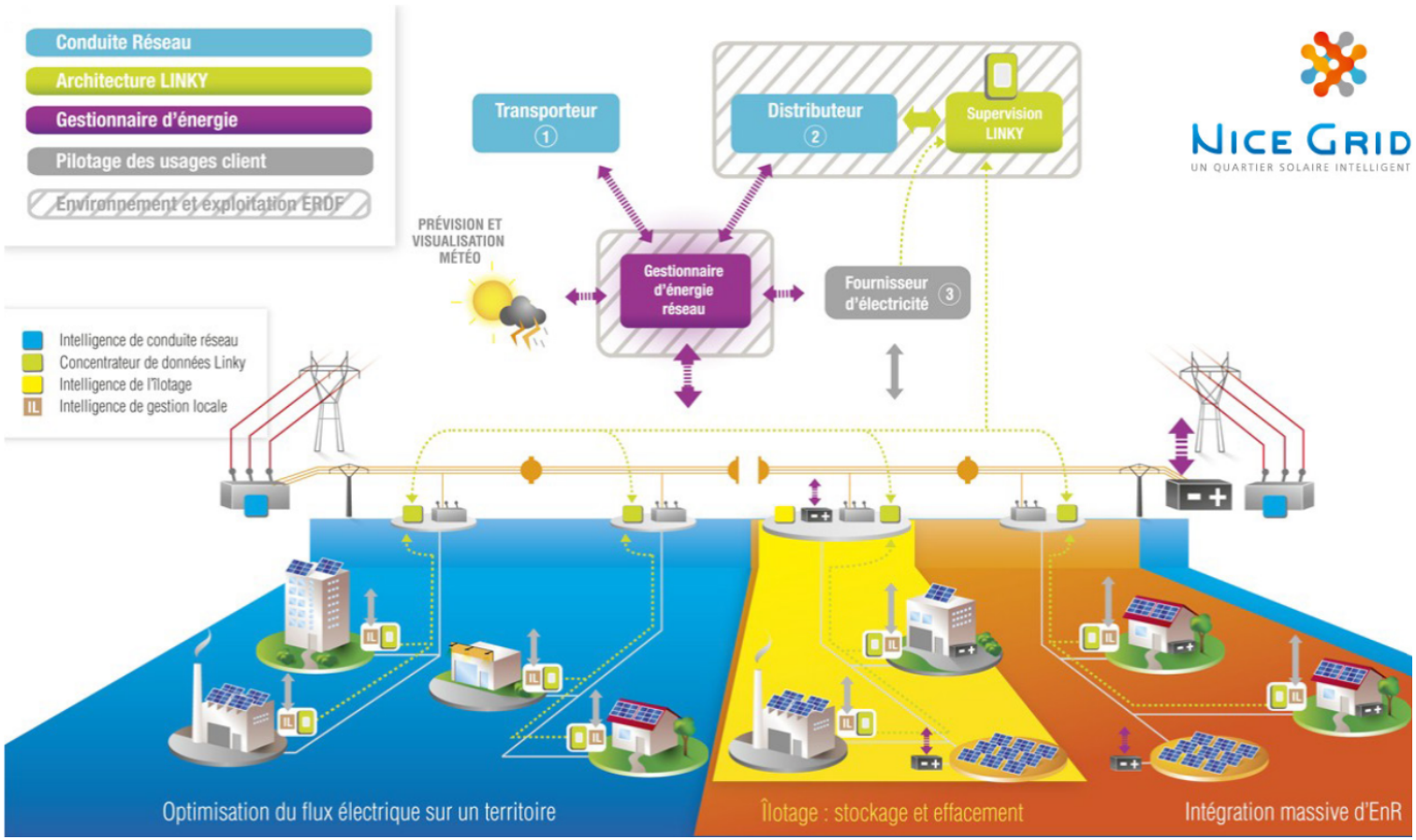
Technique de protection des données privées dans le contexte des marchés locaux d'énergie

Victor Languille (SEIDO: EDF/Télécom Paris)

Directeur: Gérard Memmi (LTCI, Télécom Paris)
Co-Directeur: David Menga (EDF)
Collaborateur: Hamza Zarfaoui

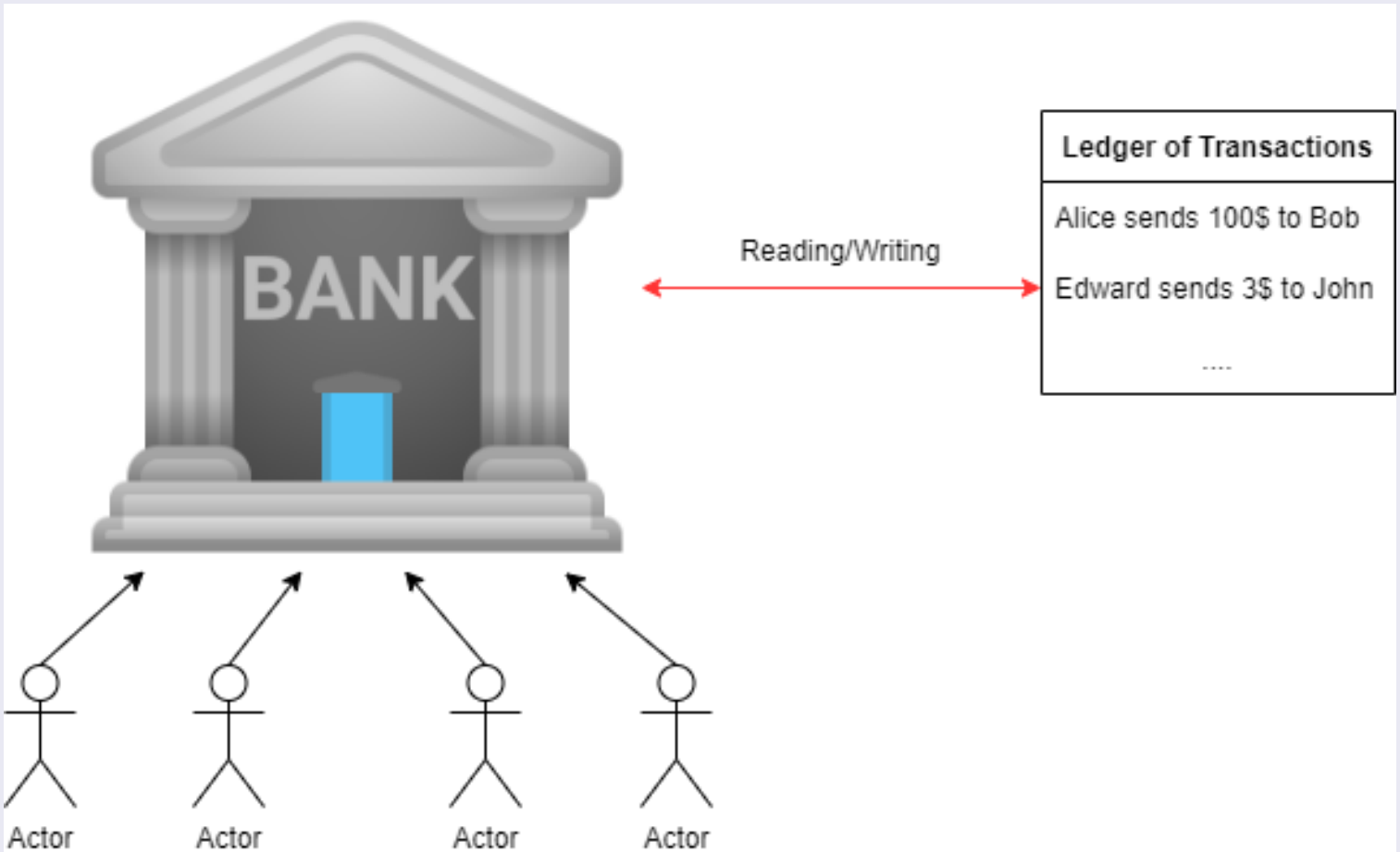
Microgrids

Development of renewable energy ⇒ Multiplication of local producers



Decentralisation VS Privacy, the example of bank system and Bitcoin

Central Authority



Decentralisation VS Privacy, the example of bank system and Bitcoin

Three different types of issues: Control, Single point vulnerability, Privacy:

Decentralisation VS Privacy, the example of bank system and Bitcoin

Three different types of issues: Control, Single point vulnerability, Privacy:

Control issues

Can refuse some transactions from your account

Can block some transaction from / to your account

Decentralisation VS Privacy, the example of bank system and Bitcoin

Three different types of issues: Control, Single point vulnerability, Privacy:

Control issues

Can refuse some transactions from your account
Can block some transaction from / to your account

Single point vulnerability issue

If the bank server is attacked, the whole history of transaction may be lost.

Decentralisation VS Privacy, the example of bank system and Bitcoin

Three different types of issues: Control, Single point vulnerability, Privacy:

Control issues

Can refuse some transactions from your account
Can block some transaction from / to your account

Single point vulnerability issue

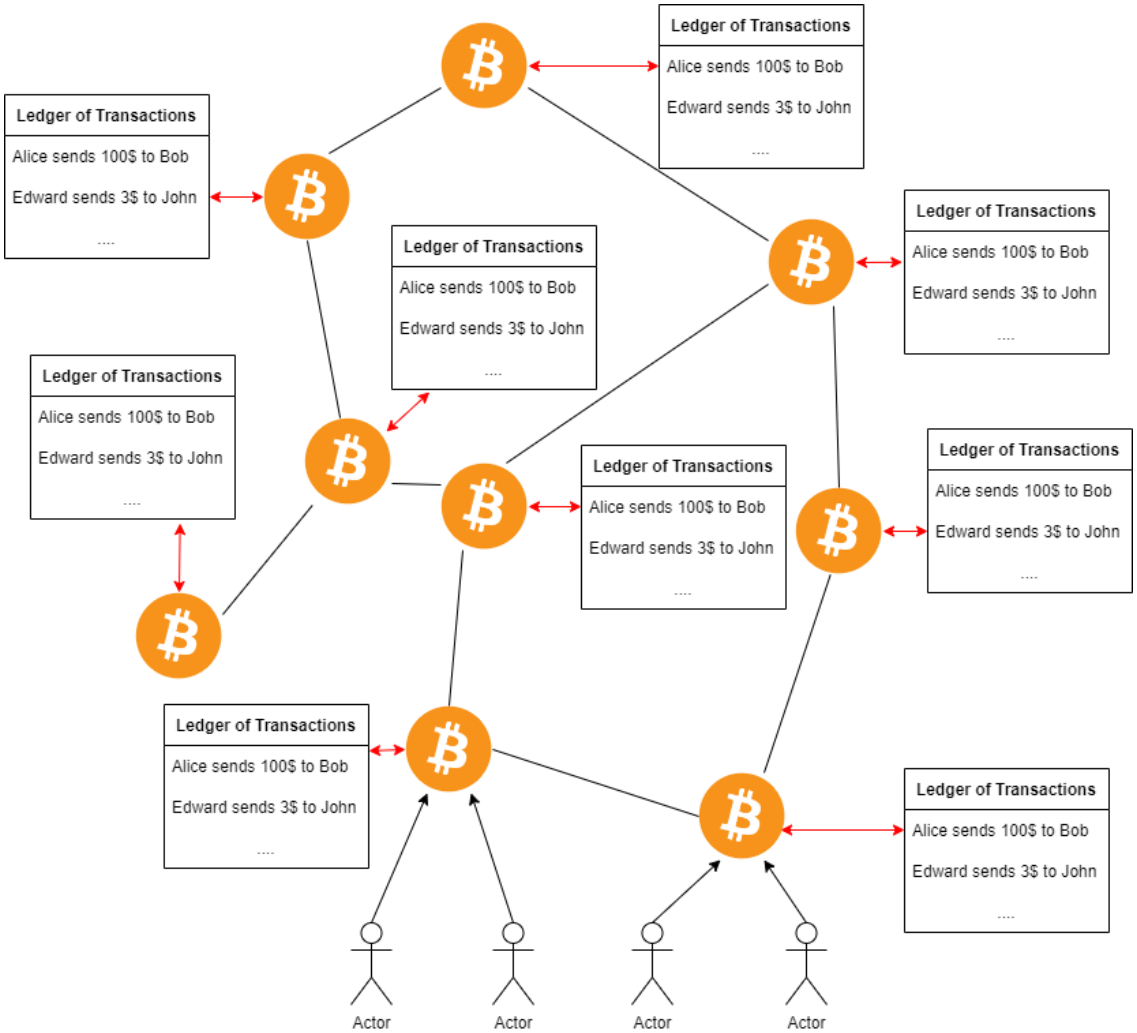
If the bank server is attacked, the whole history of transaction may be lost.

Privacy issues

Your assets and holdings
Your family and professional activities
Your habits
The diseases you suffer

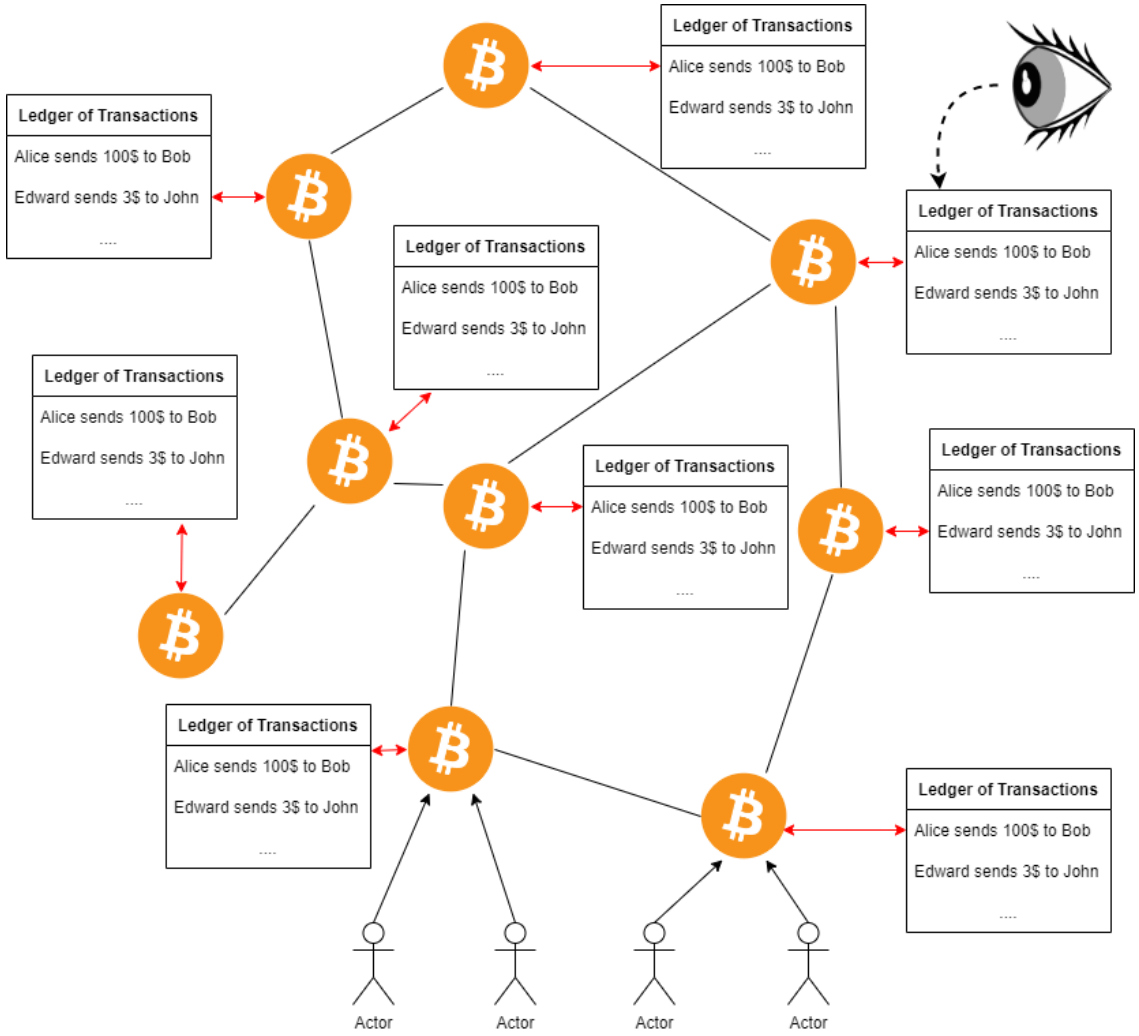
Decentralisation VS Privacy, the example of bank system and bitcoin

Bitcoin avoids centralised authority



Decentralisation VS Privacy, the example of bank system and bitcoin

Permissionless ledger ⇒ Everybody has access to transaction data!



Solution to the privacy-decentralisation dilemma ?

Solution to the privacy-decentralisation dilemma ?

Zero-Knowledge Proofs !

Or: How to prove that you know the solution to a certain problem without revealing it.

Zero-Knowledge Proof

Given a certain y and a program P, allows a Prover to prove to a Verifier:

"I know x such that $y = P(x)$"

Zero-Knowledge Proof

Given a certain y and a program P, allows a Prover to prove to a Verifier:

"I know x such that $y = P(x)$"

- Prover produces a proof π, concretely a string of bits.

Zero-Knowledge Proof

Given a certain y and a program P, allows a Prover to prove to a Verifier:

"I know x such that $y = P(x)$"

- Prover produces a proof π, concretely a string of bits.
- Verifier applies a specific algorithm to π and y, returning 1 if the proof is valid; 0 otherwise.

Zero-Knowledge Proof

Given a certain y and a program P, allows a Prover to prove to a Verifier:

"I know x such that $y = P(x)$"

- Prover produces a proof π, concretely a string of bits.
- Verifier applies a specific algorithm to π and y, returning 1 if the proof is valid; 0 otherwise.
- Prover can produce a valid proof if and only if he knows x.

Zero-Knowledge Proof

Given a certain y and a program P, allows a Prover to prove to a Verifier:

"I know x such that $y = P(x)$"

- Prover produces a proof π, concretely a string of bits.
- Verifier applies a specific algorithm to π and y, returning 1 if the proof is valid; 0 otherwise.
- Prover can produce a valid proof if and only if he knows x.
- The proof leak 0-information about x.

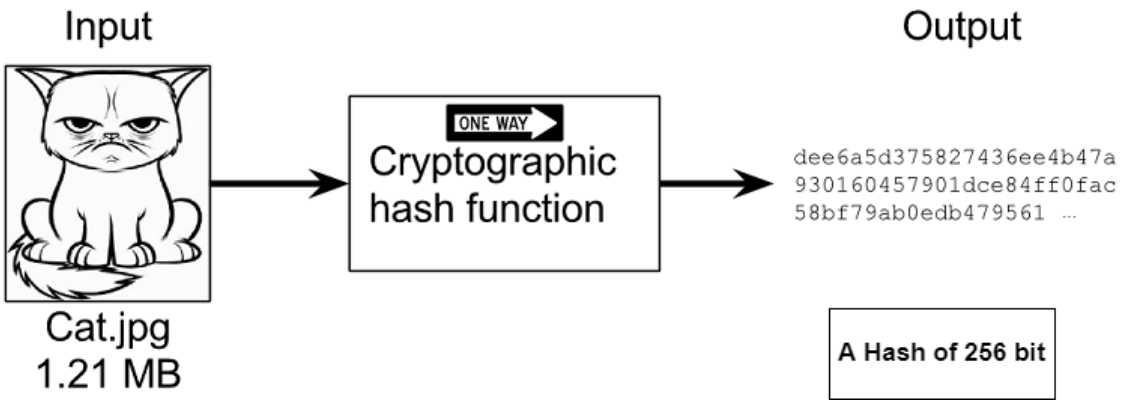
Zero-Knowledge Proof

Given a certain y and a program P, allows a Prover to prove to a Verifier:

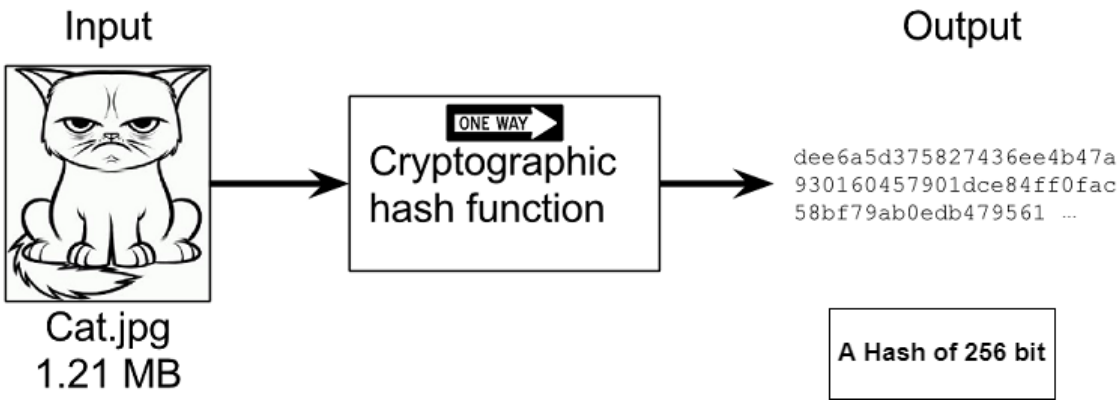
"I know x such that $y = P(x)$"

- Prover produces a proof π, concretely a string of bits.
- Verifier applies a specific algorithm to π and y, returning 1 if the proof is valid; 0 otherwise.
- Prover can produce a valid proof if and only if he knows x.
- The proof leak 0-information about x.
- Bonus: efficiency. It is exponentially faster to verify a succinct ZKP than to compute P knowing x

Building block: Hash functions H()



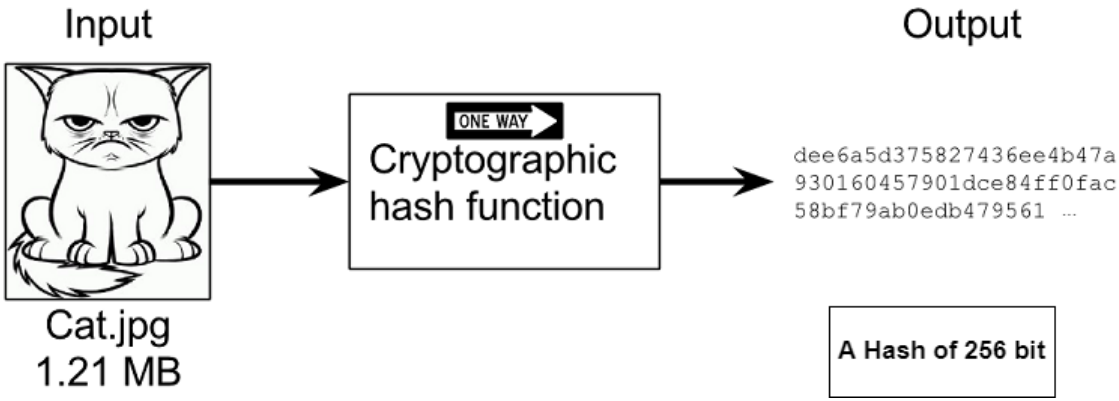
Building block: Hash functions H()



Essentials properties

Any size input $\rightarrow$ 256 bit output

Building block: Hash functions H()

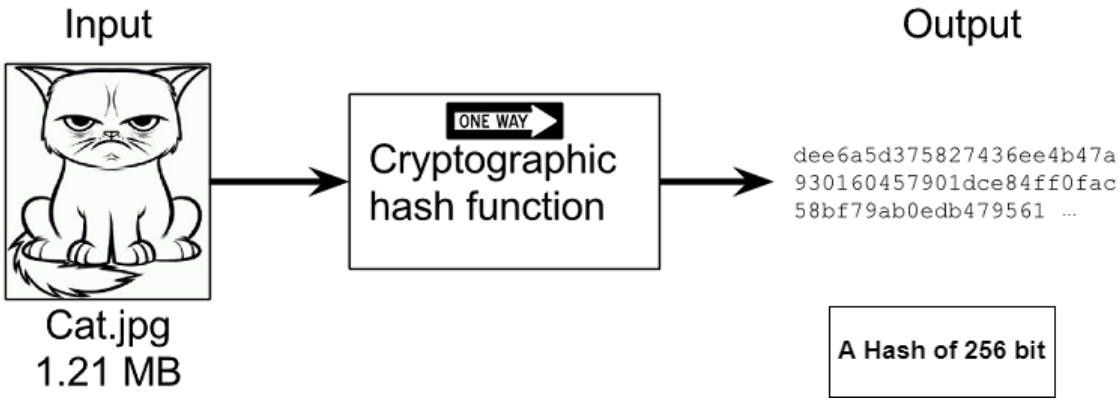


Essentials properties

Any size input $\rightarrow$ 256 bit output

Any little change in the input $\rightarrow$ completely different output

Building block: Hash functions H()



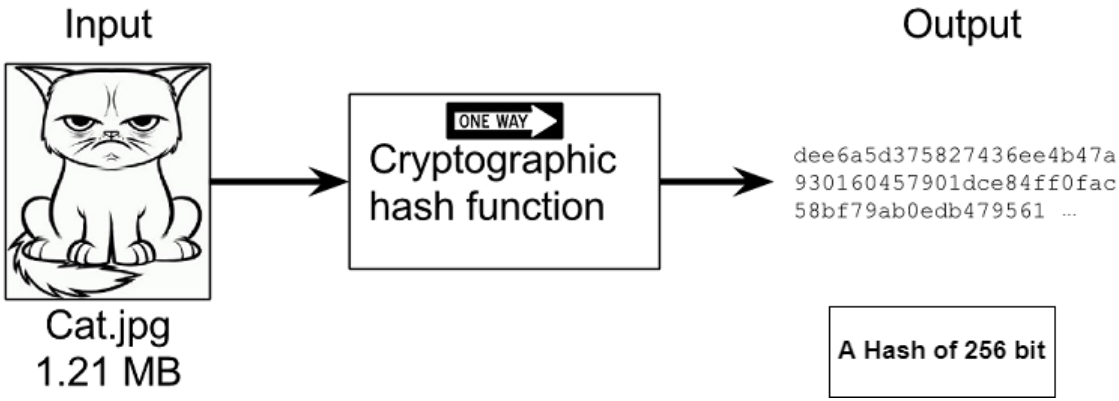
Essentials properties

Any size input $\rightarrow$ 256 bit output

Any little change in the input $\rightarrow$ completely different output

Easy: given x, computes $y = H(x)$

Building block: Hash functions H()



Essentials properties

Any size input $\rightarrow$ 256 bit output

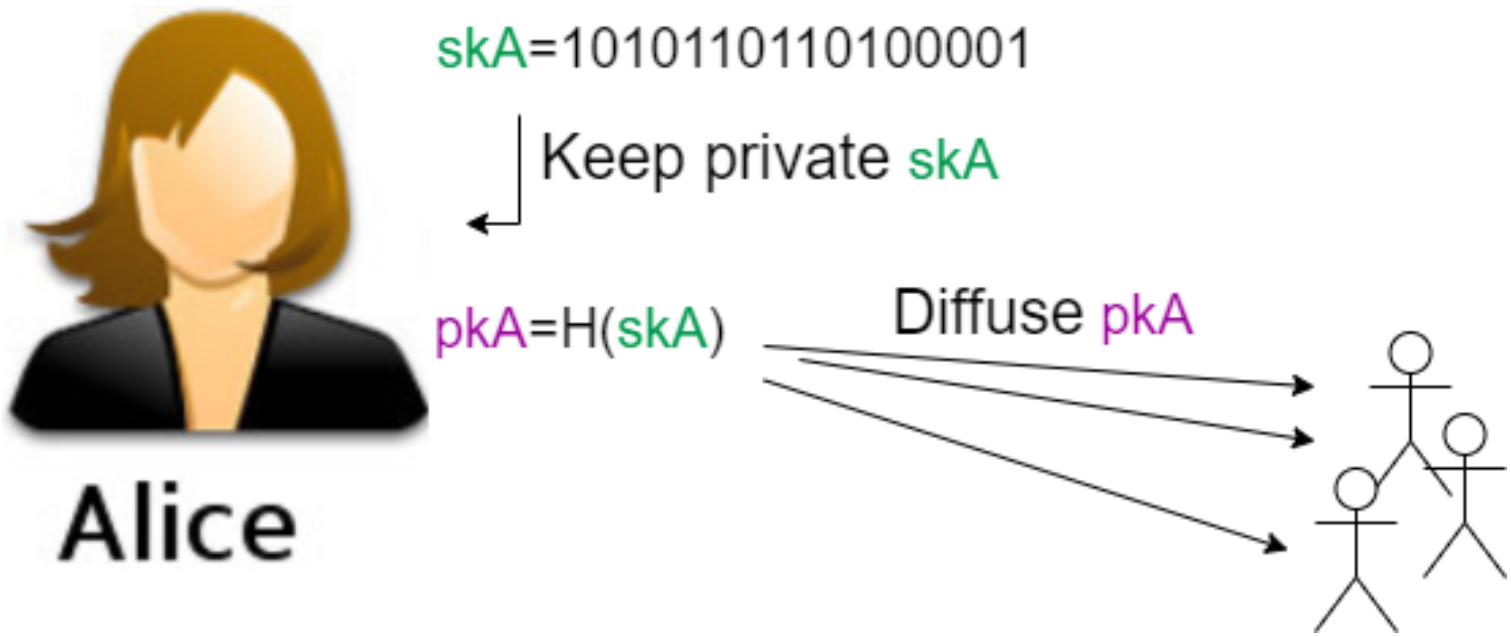
Any little change in the input $\rightarrow$ completely different output

Easy: given x, computes $y = H(x)$

Hard(i.e, practically infeasible): given y, find x such that $y = H(x)$

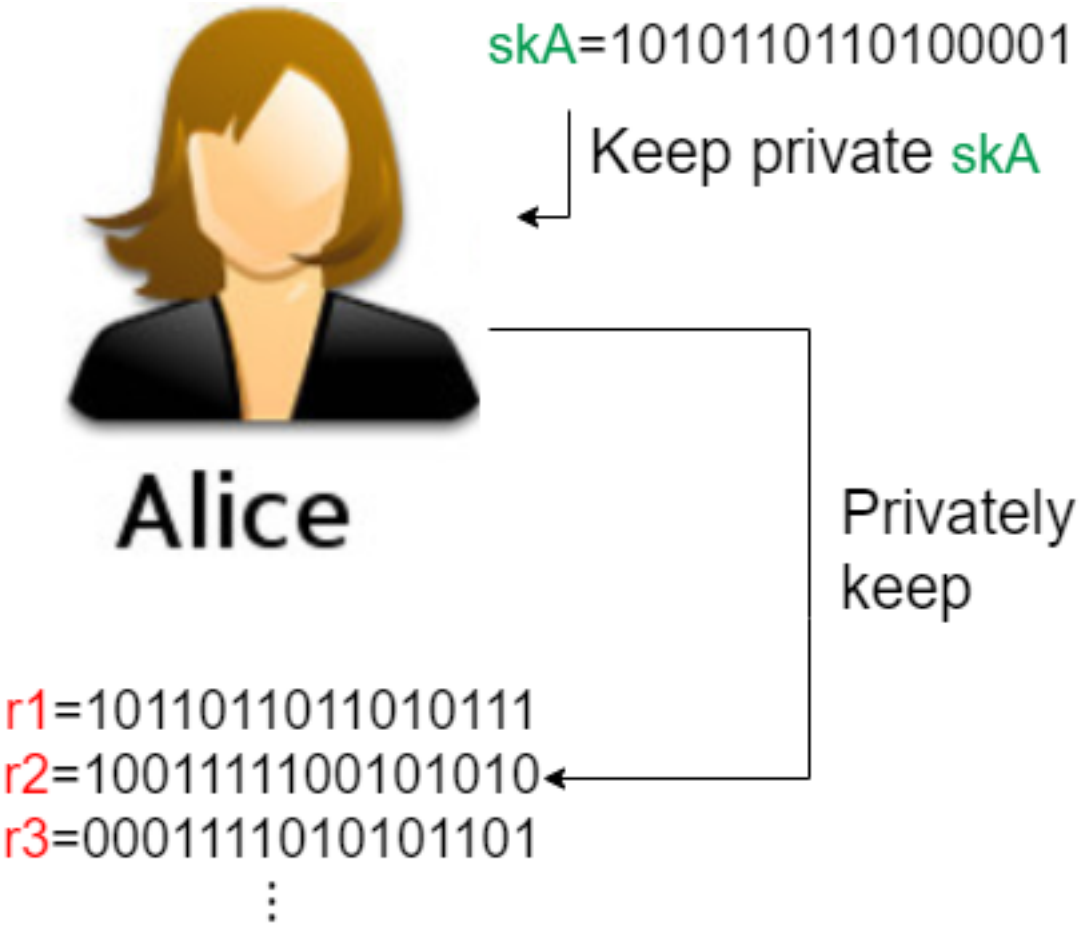
Anonymous Cruptocurrency on Public Ledger

Secret identifier (skA) to spend coins
Public identifier (pkA) to receive coins



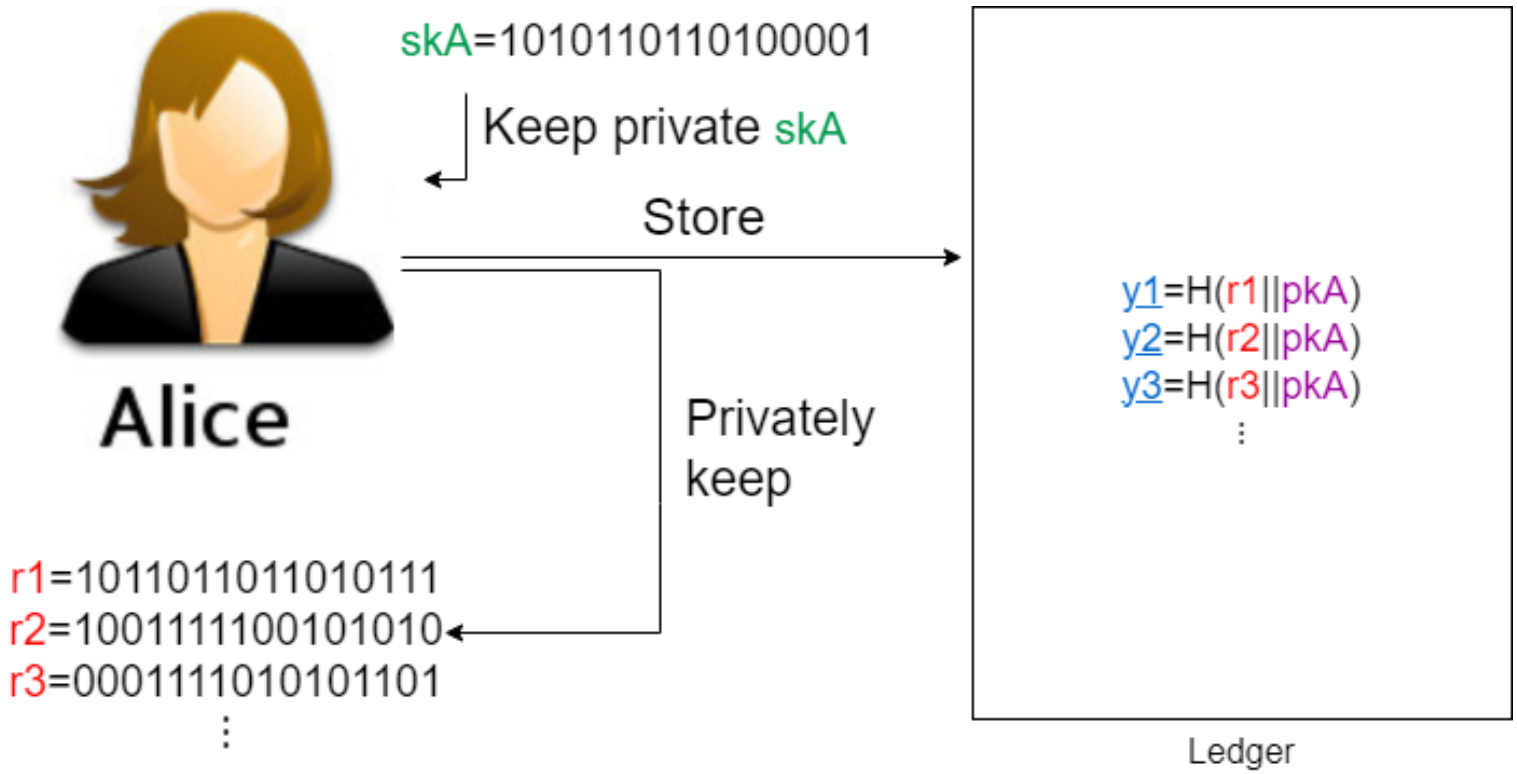
Anonymous Cruptocurrency on Public Ledger

Coins represented as random numbers



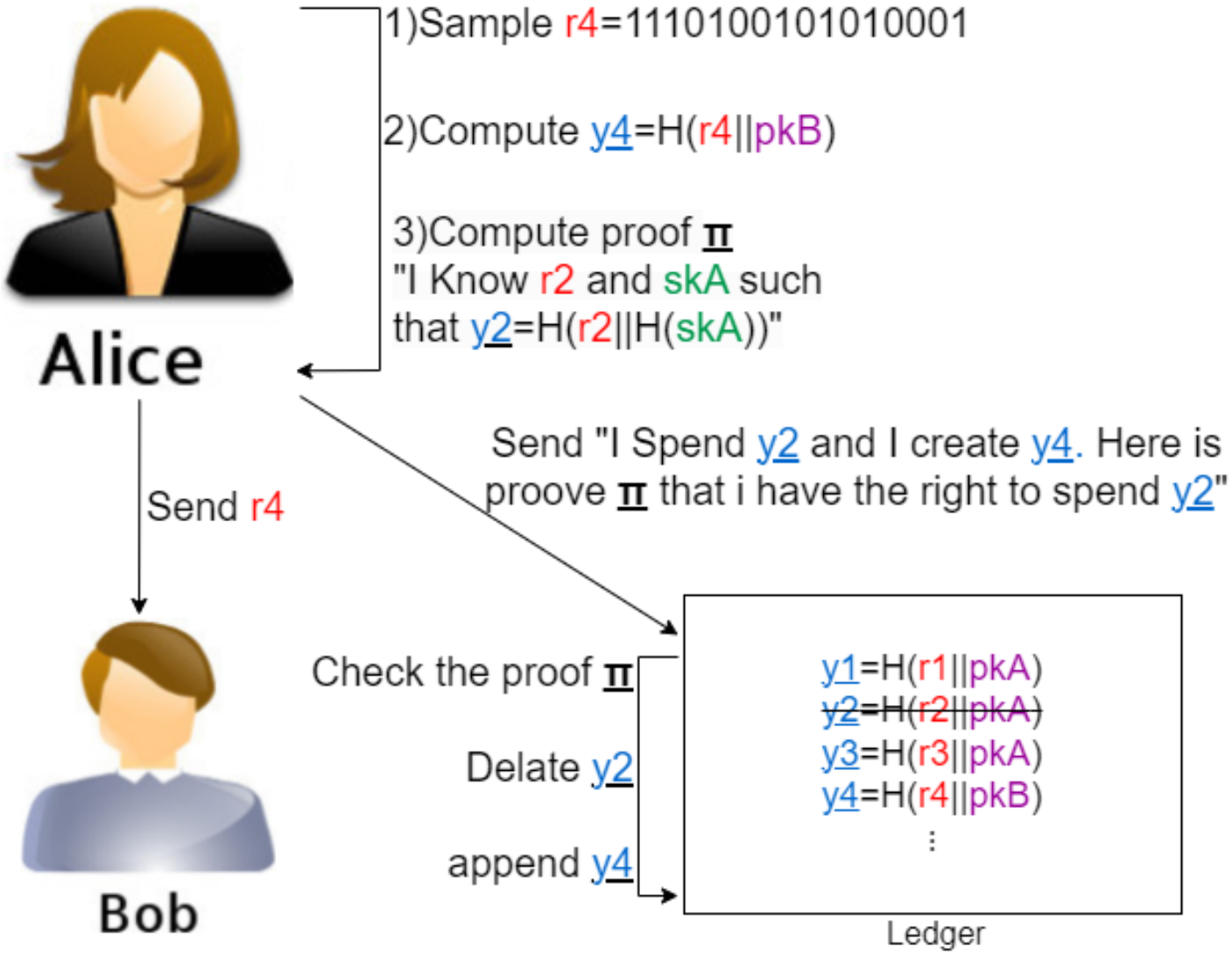
Anonymous Cruptocurrency on Public Ledger

Hash of existing coins are stored on the ledger



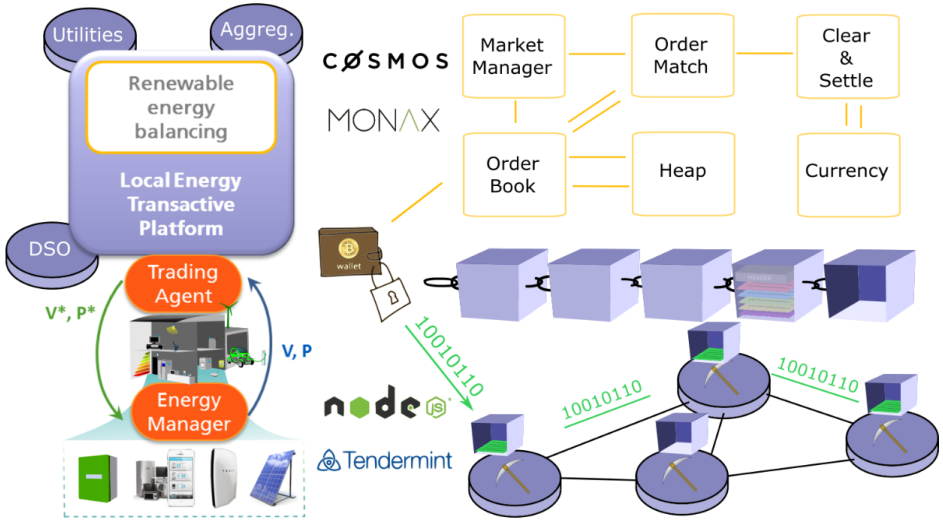
Anonymous Cruptocurrency on Public Ledger

Transaction from Alice to Bob = Destruction of one Alice's coin and creation to one Bob's coin.



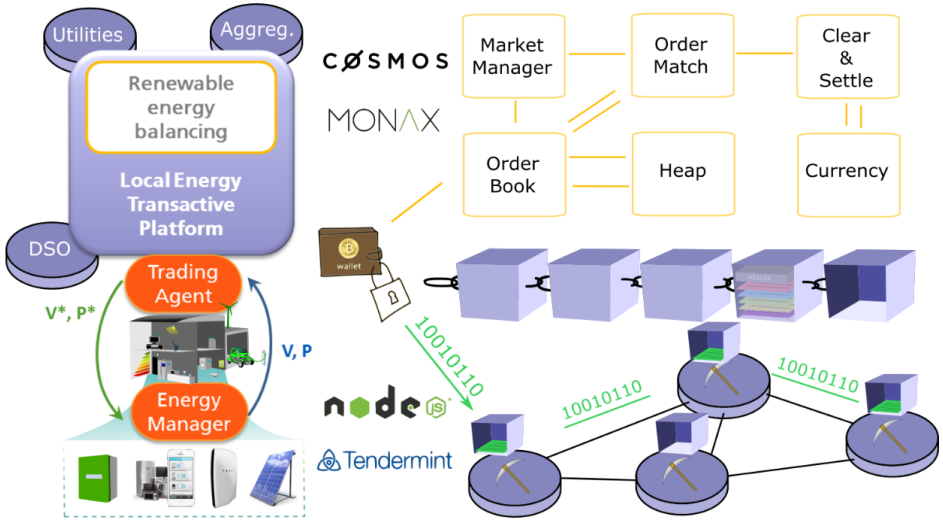
Anonymous sealed bid exchange mechanism

Energy market use case by José Horta [**horta**].

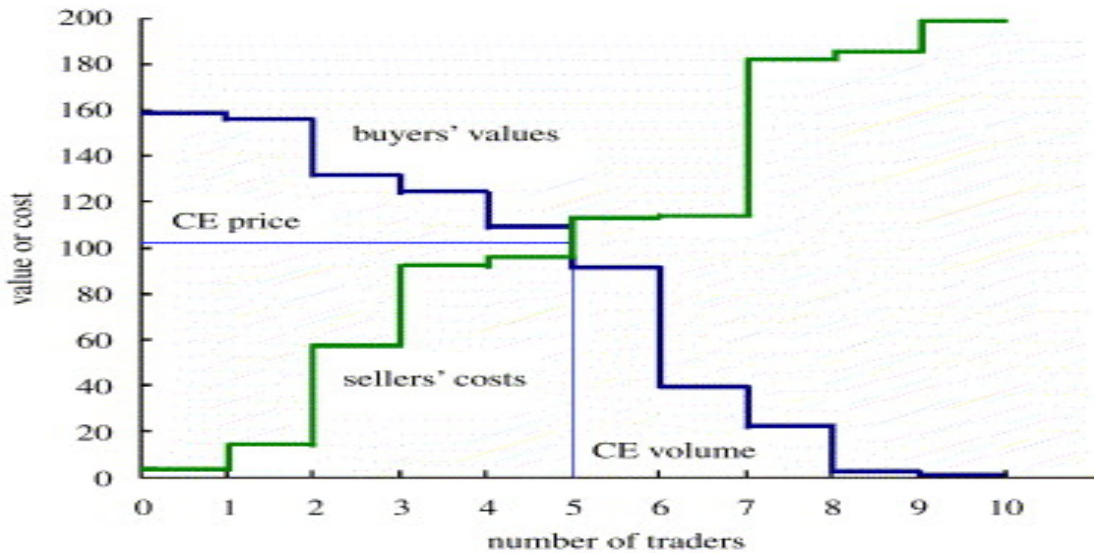


Anonymous sealed bid exchange mechanism

Energy market use case by José Horta [**horta**].

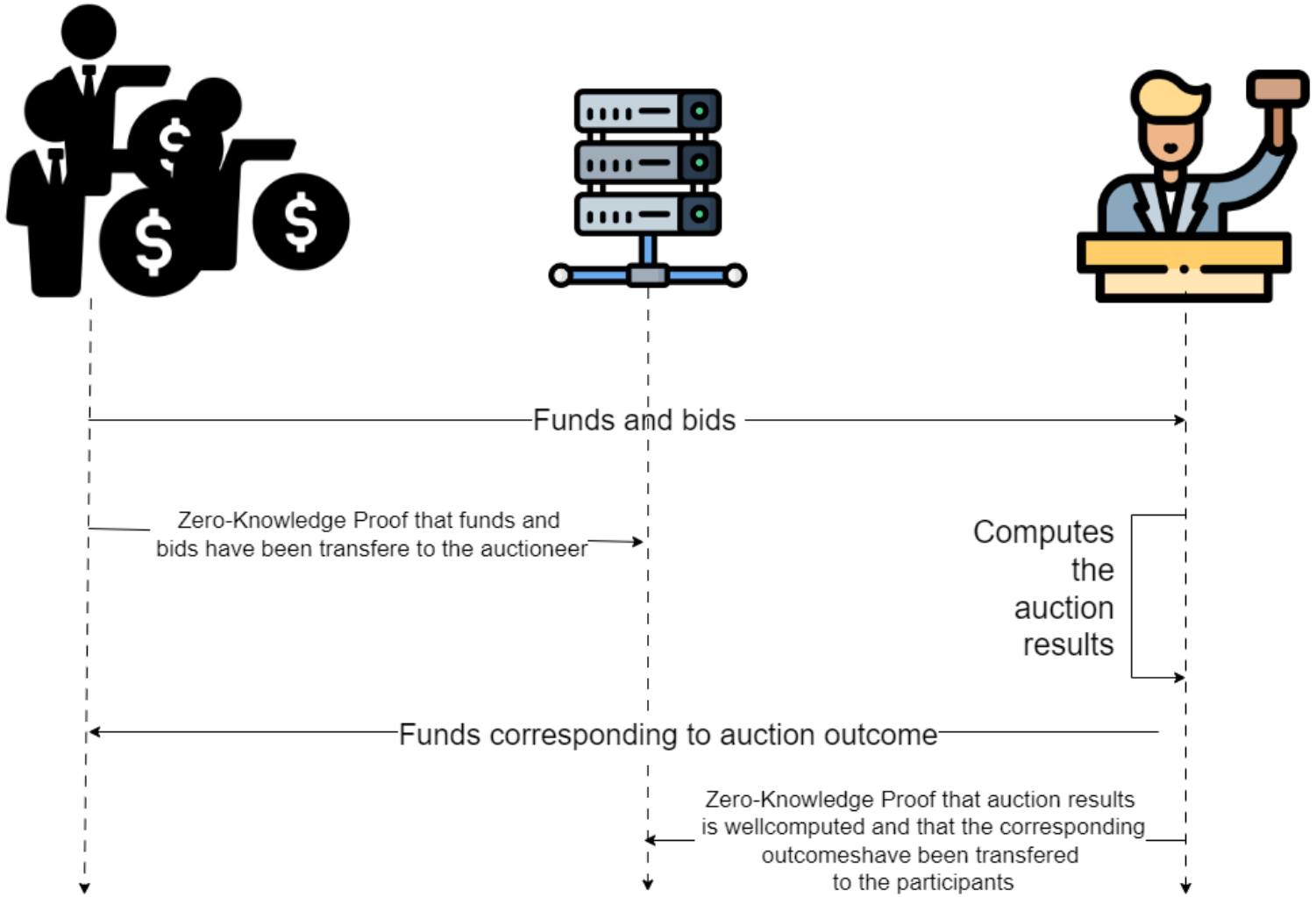


General auction mechanism (in particular multi unit double auction).



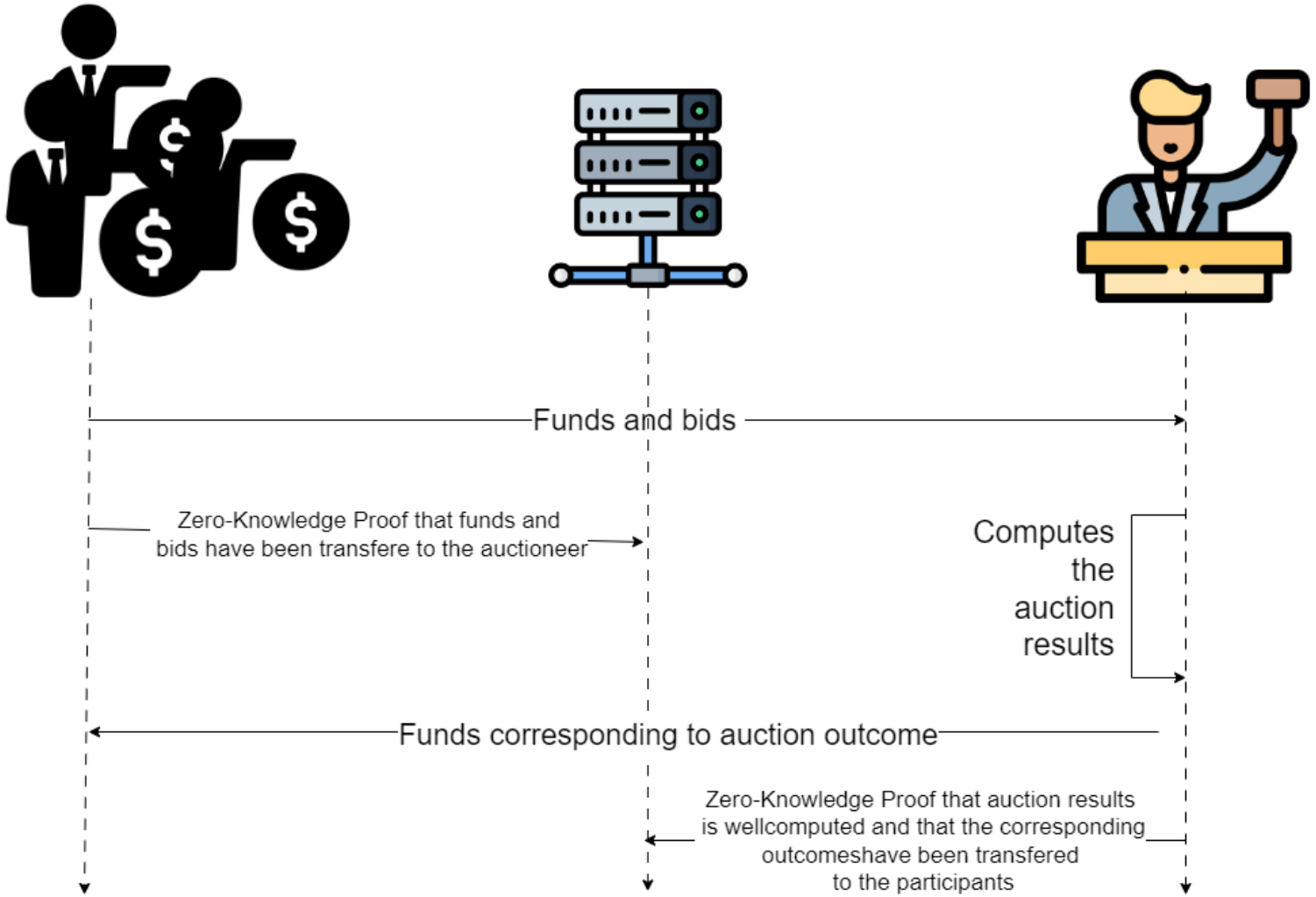
Anonymous sealed bid exchange mechanism

Proposed scheme based on an extension of Zerocash



Anonymous sealed bid exchange mechanism

Proposed scheme based on an extension of Zerocash



Anonymity against the auctioneer and the ledger. *Confidentiality* against the ledger.

Thank you for your attention.

Thank you for your attention.

Any question?