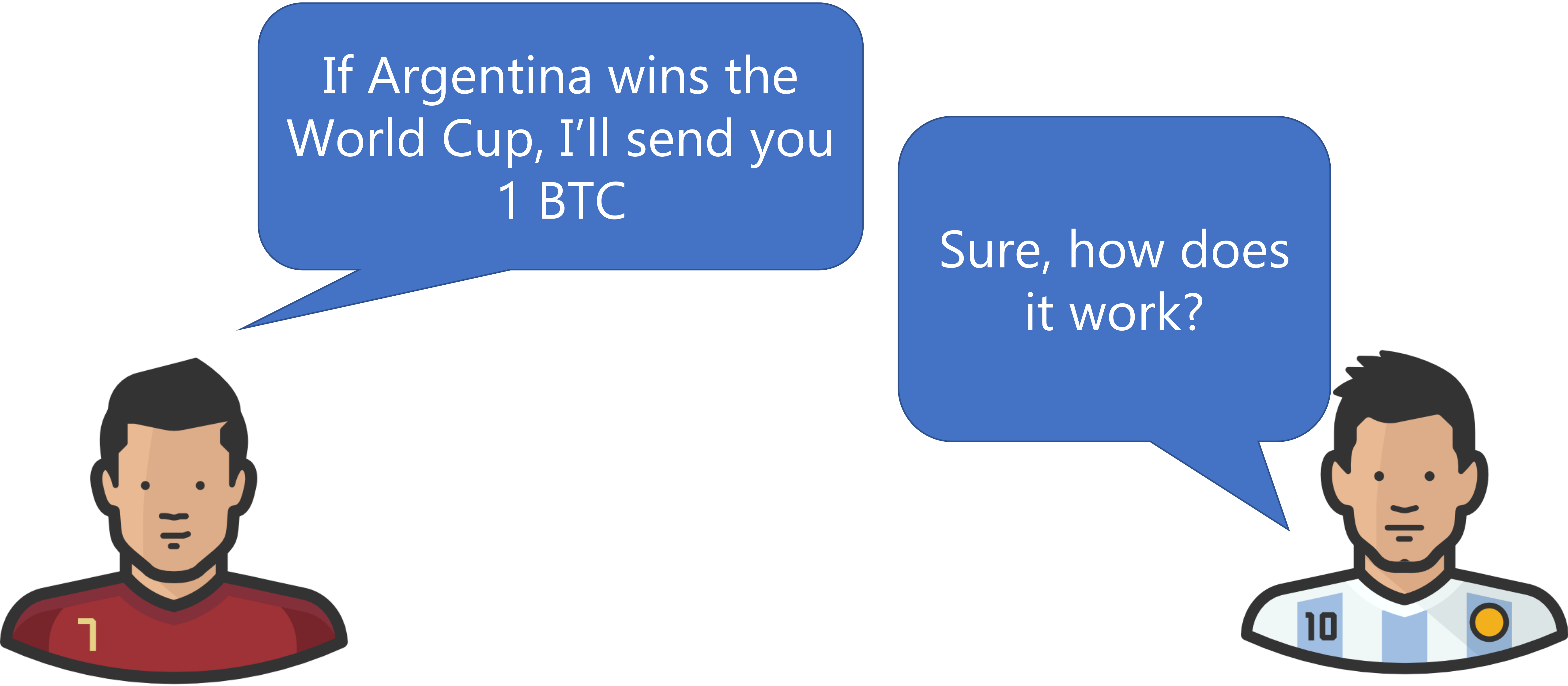
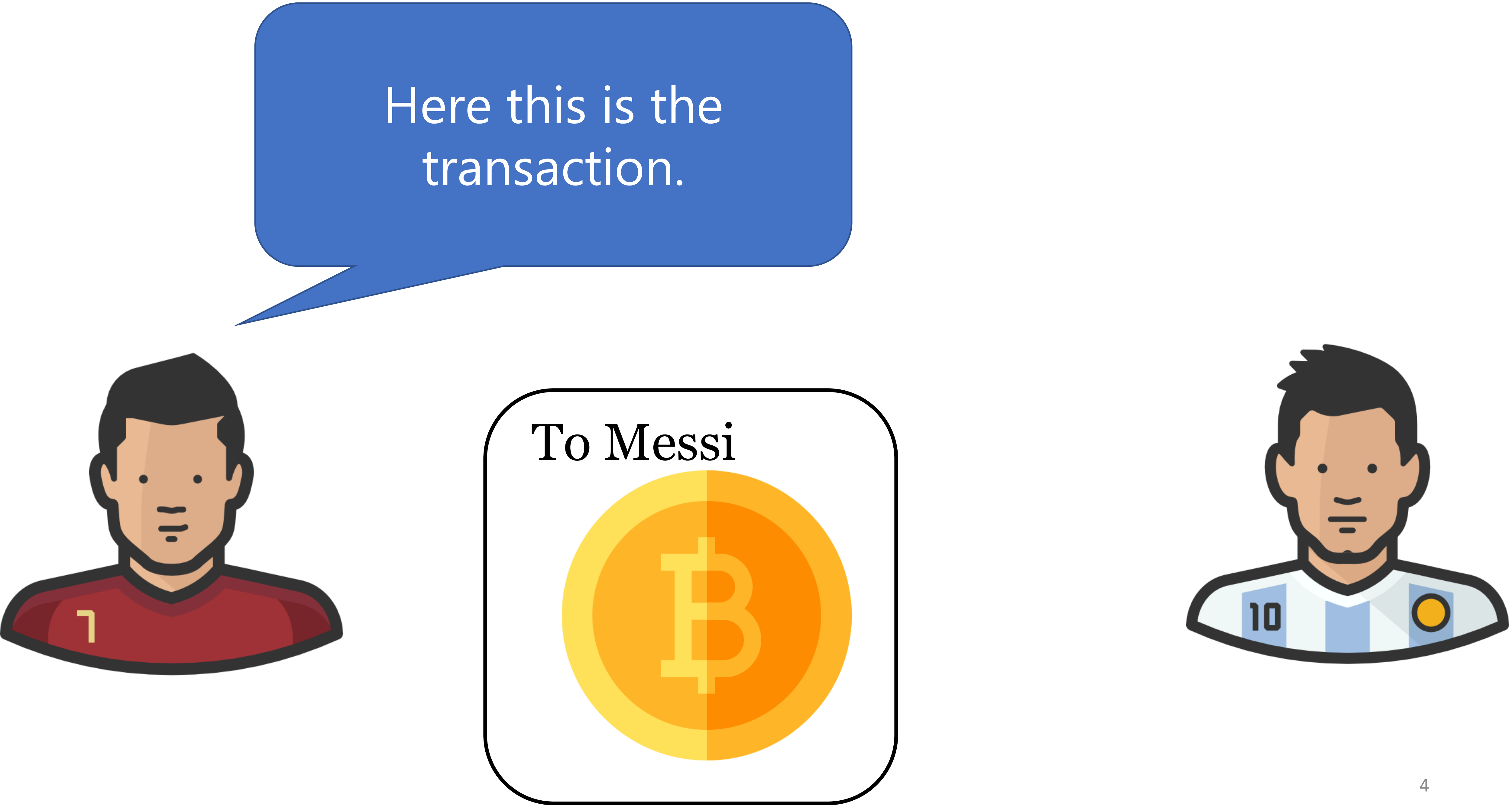
Cryptographic Oracle-based Conditional Payments

- **Varun Madathil,** Sri AravindaKrishnan Thyagarajan, Dimitrios Vasilopoulos, Giulio Malavolta , Lloyd Fournier, Pedro Moreno-Sanchez

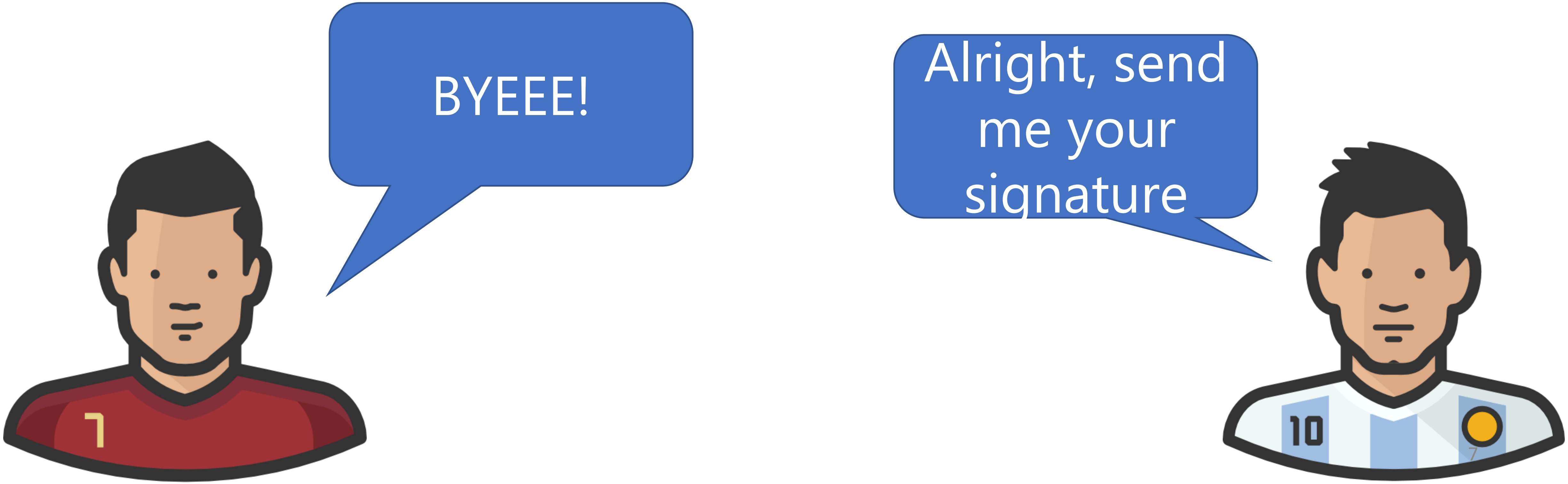
Conditional Payments


If Argentina wins the World Cup, I'll send you 1 BTC
Sure, how does it work?


Here this is the transaction.
To Messi
10


You just need my signature on this transaction.
To Messi


But I will sign this only after you win the cup!
To Messi
7
10


BYEEE!
Alright, send me your signature

Parties are mutually distrustful!

THIS WORK:

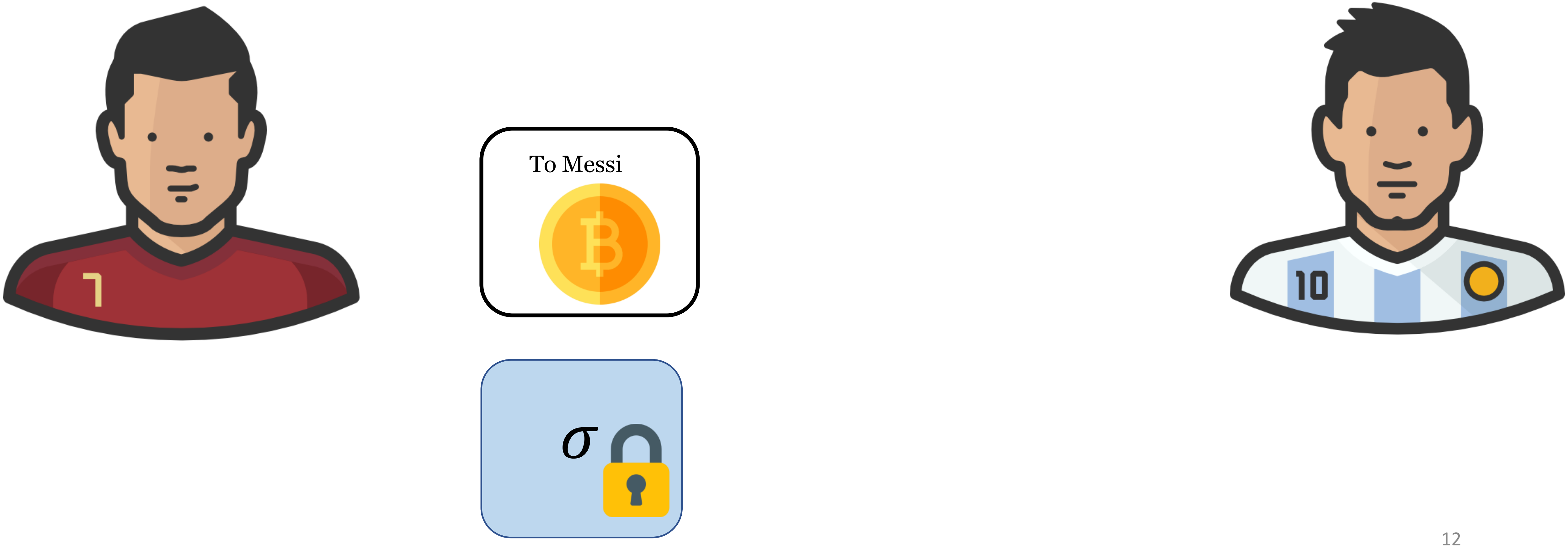
Enabling secure conditional payments where oracle(s) attest to a real-world outcome

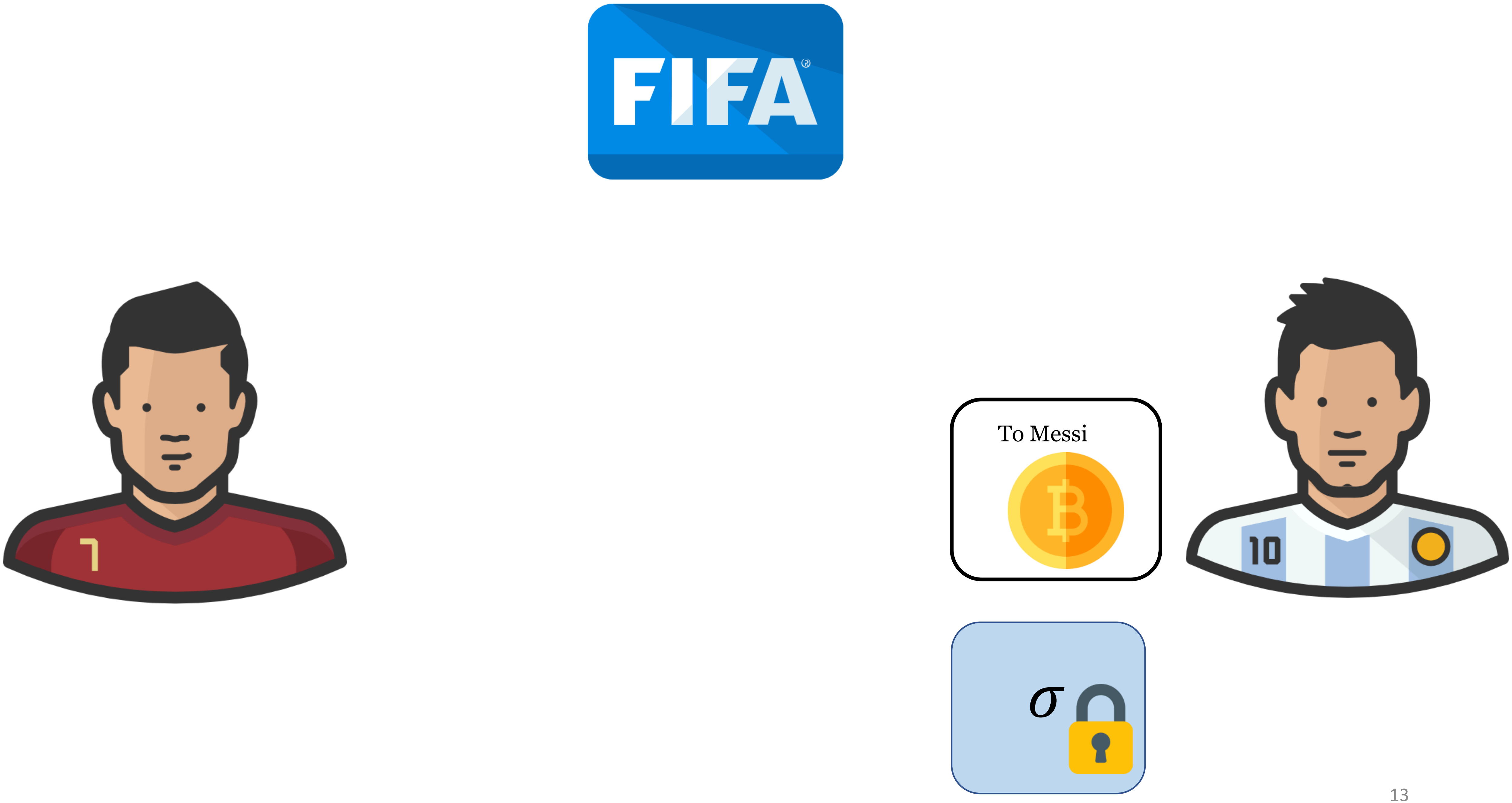
Oracle based conditional payments

The Setting


7

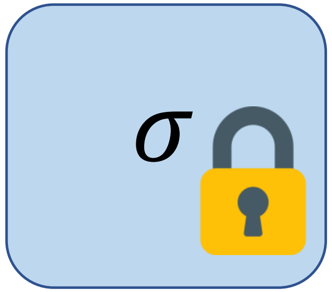

10

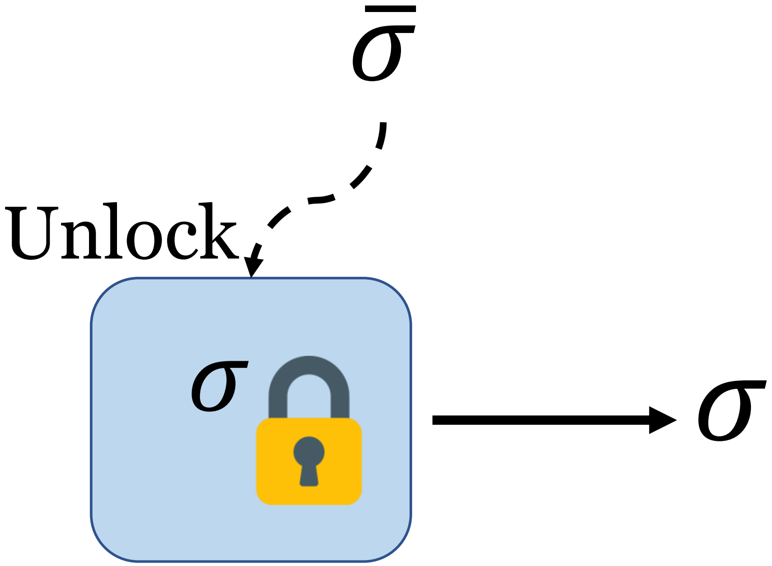

To Messi
σ

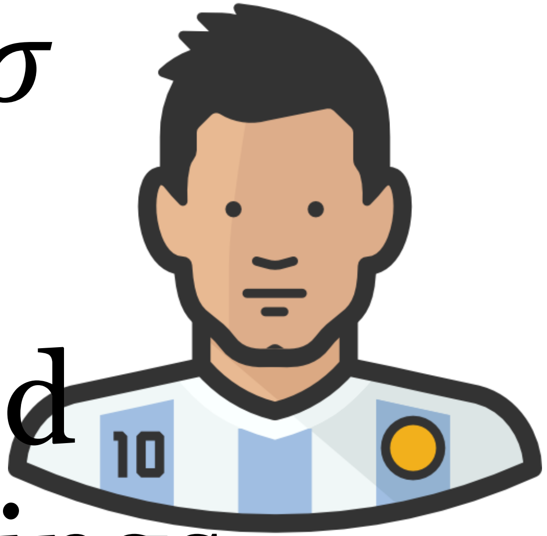

To Messi
σ

Attest to outcome : 

$\bar{\sigma}$ = Signature that Argentina wins the Cup







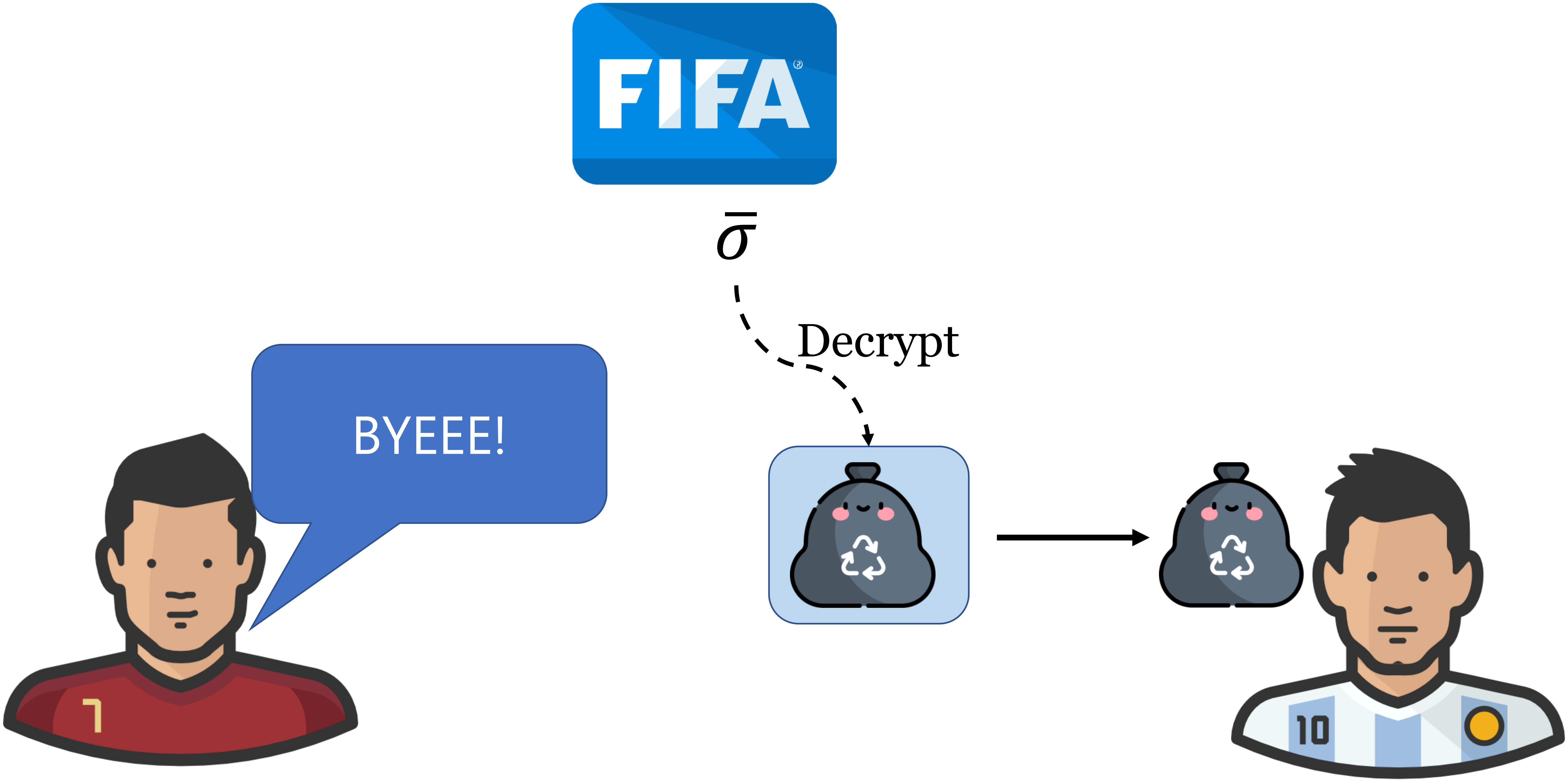
Broadcast σ and claim the winnings

Oracle based conditional payments

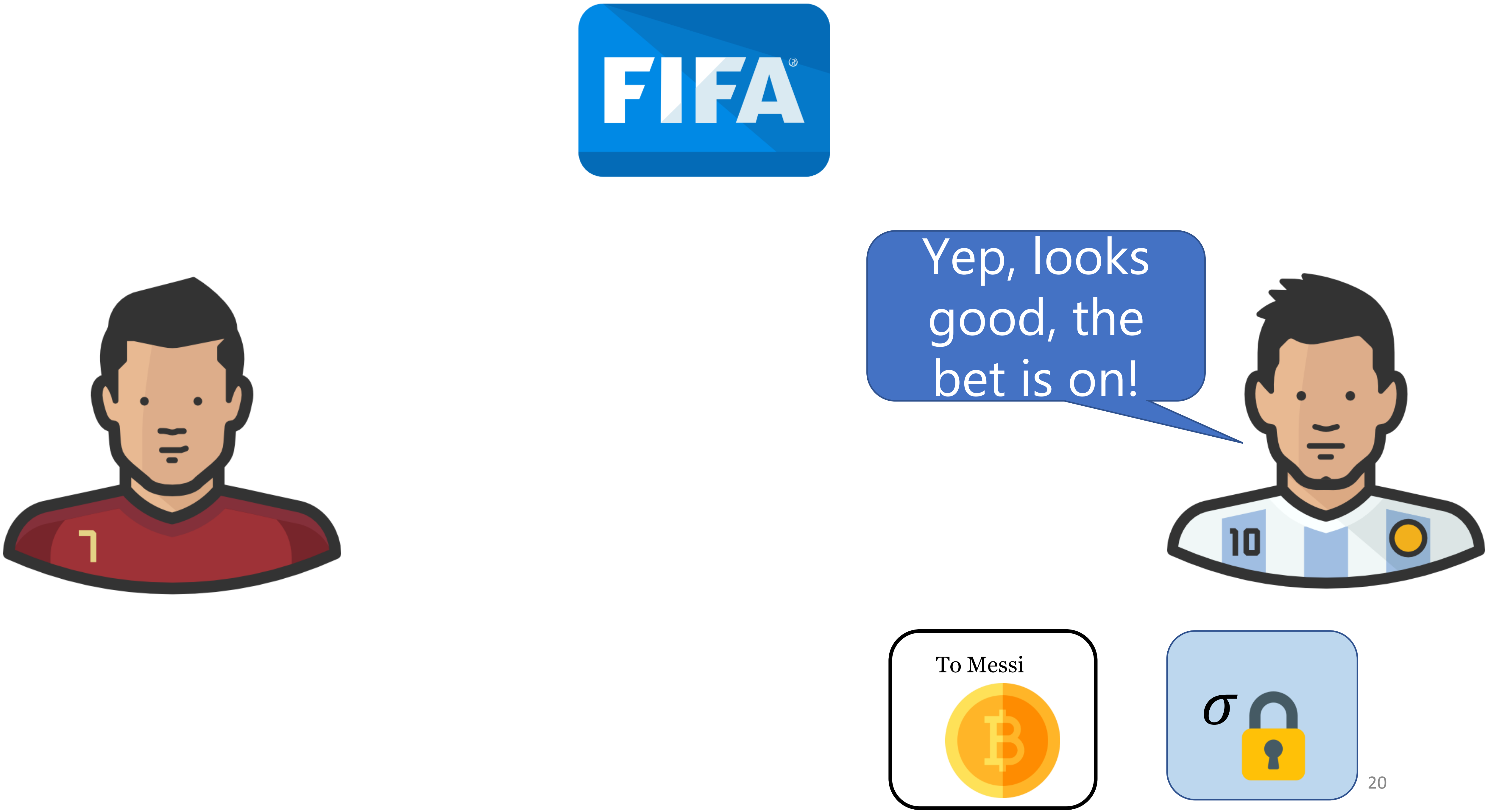
Security Guarantees

What if

To Messi


FIFA
$\bar{\sigma}$
Decrypt
BYEEE!

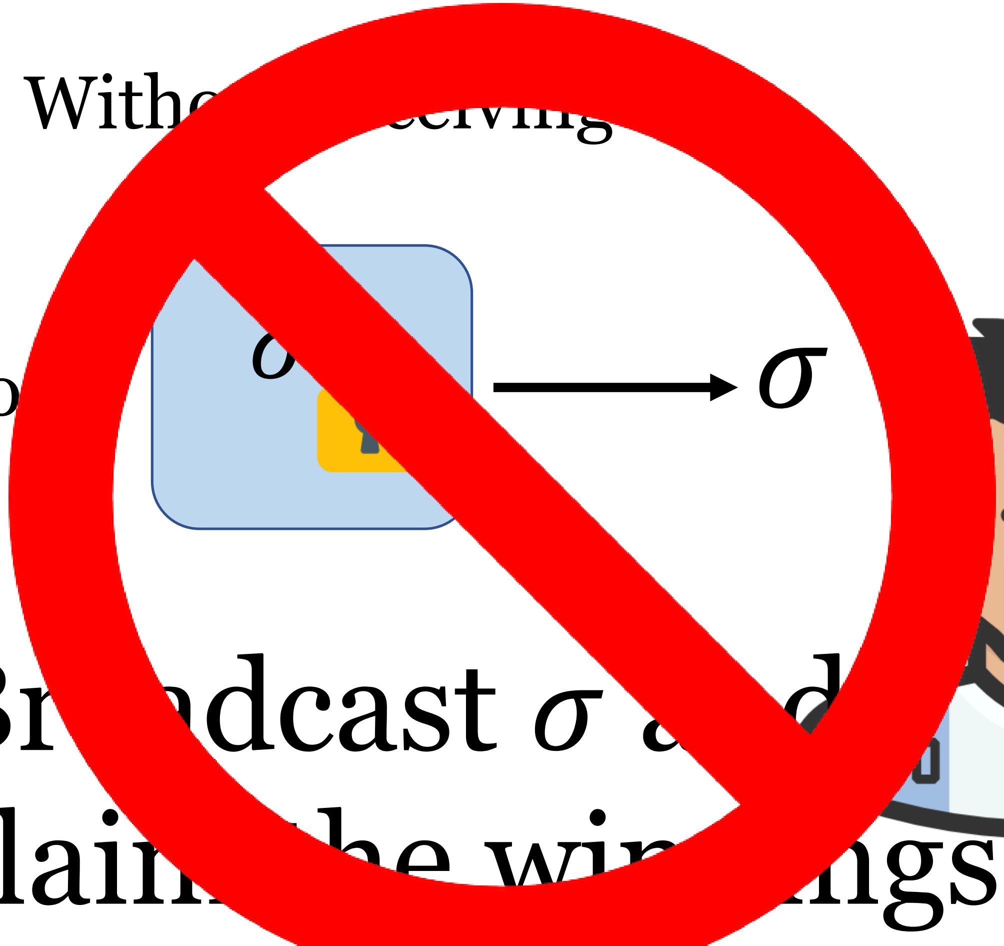
Verifiabilit y


FIFA
Yep, looks good, the bet is on!
To Messi
σ

One-wayness

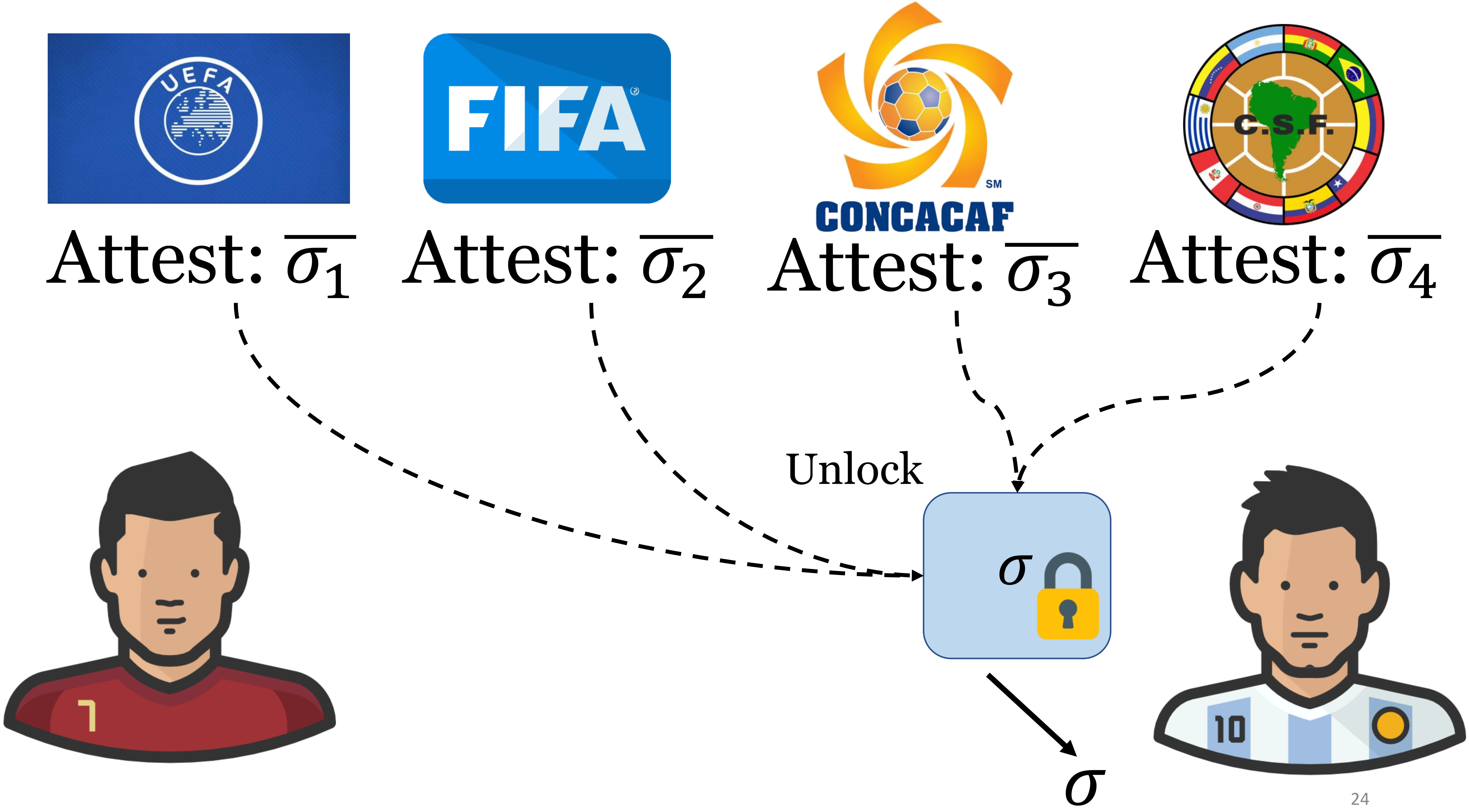
Witho ceiving

Unlo



Br dcast σ a d
clai he win ngs

Distribute trust

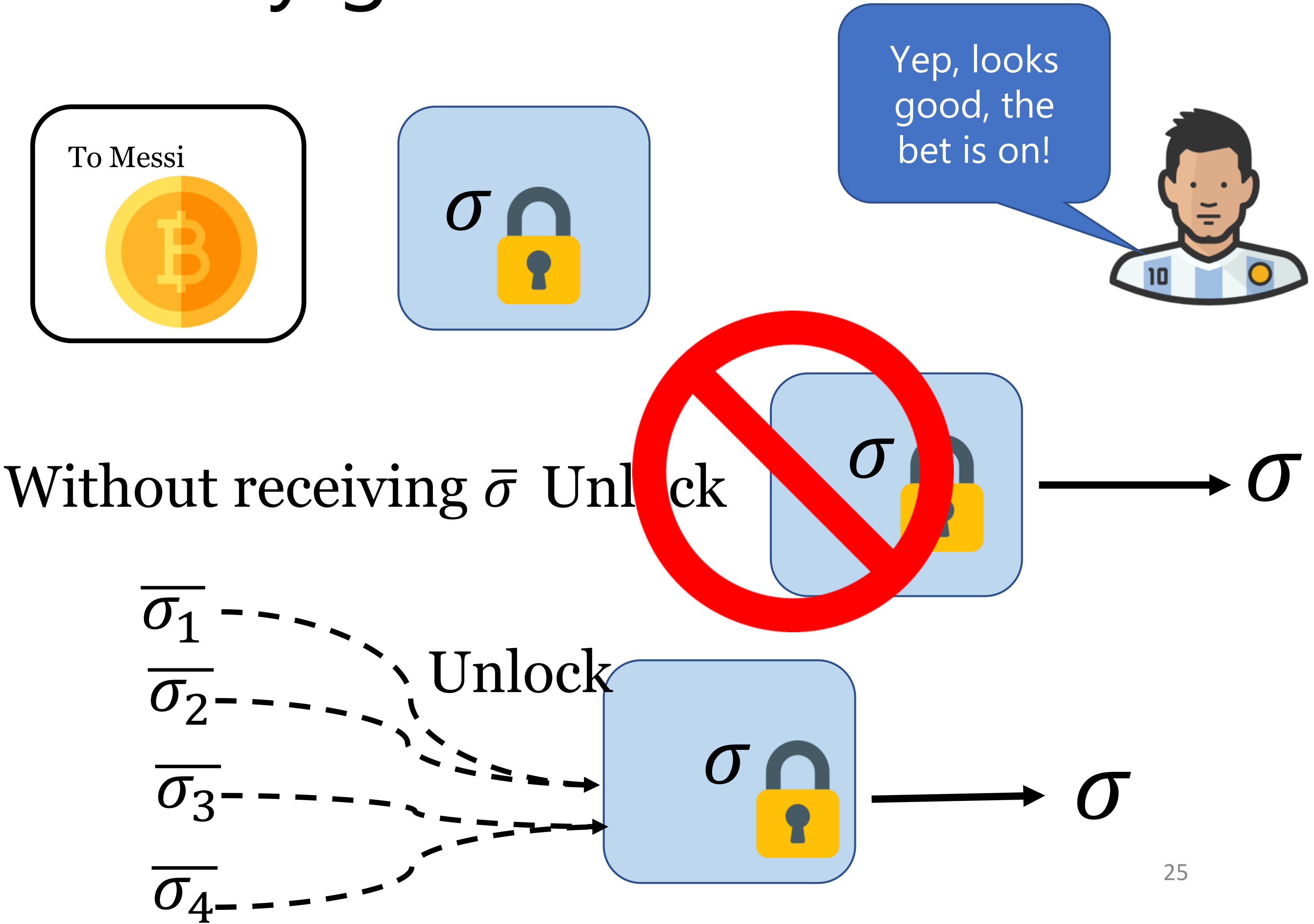

UEFA
FIFA
CONCACAF
C.S.F.
Attest: $\overline{\sigma_1}$
Attest: $\overline{\sigma_2}$
Attest: $\overline{\sigma_3}$
Attest: $\overline{\sigma_4}$
Unlock
σ
σ
7
10

Summary of security guarantees

Verifiabilit
y

One-
wayness

Distribute
trust



Oracle based conditional payments

Our techniques

A new cryptographic primitive:

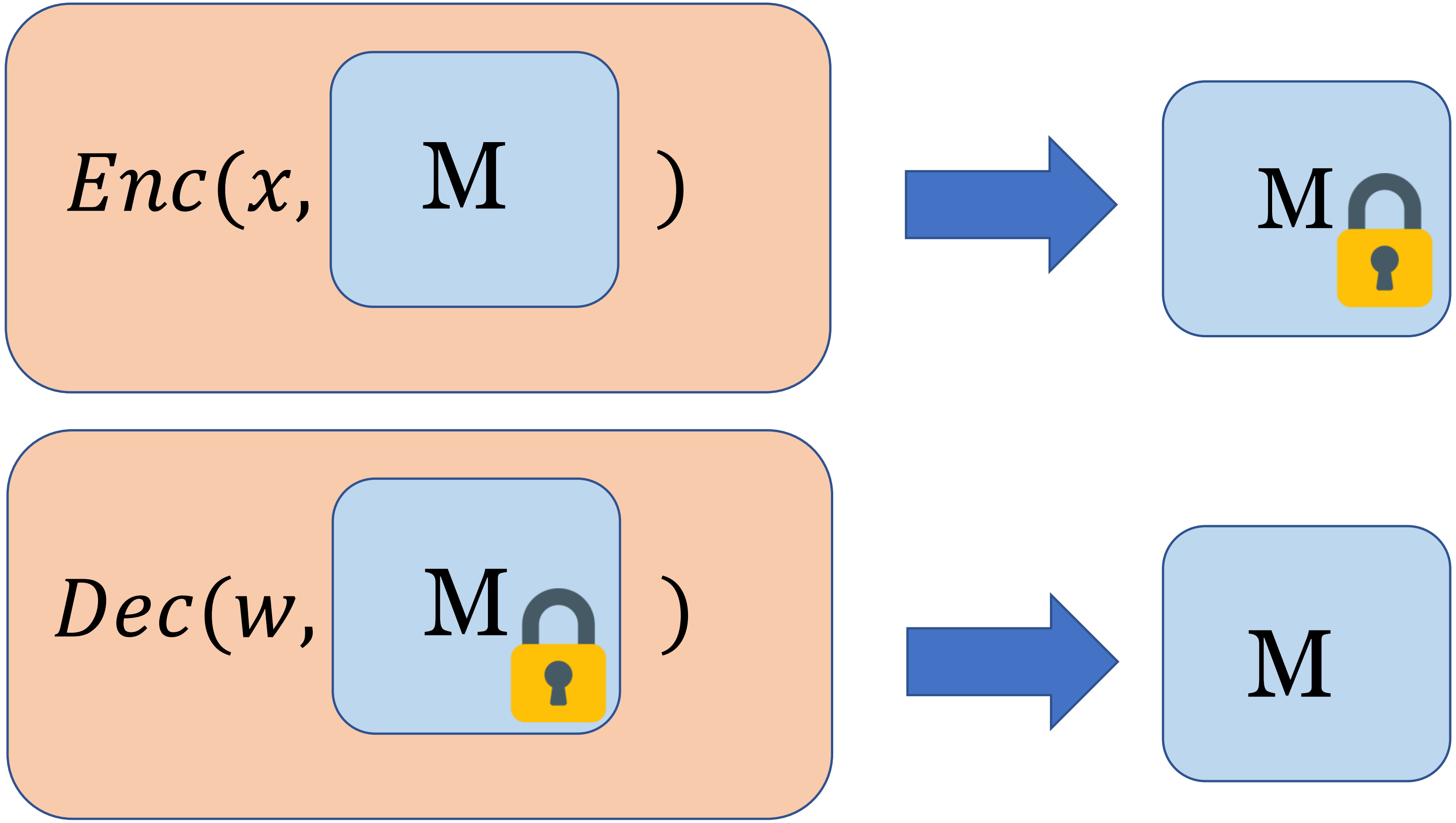
Verifiable **w**itness **e**ncryption based on **T**hreshold **S**ignatures (VweTS)

Verifiable **w**itness **e**ncryption based on **T**hreshold **S**ignatures

Witness Encryption : Consider a language L with relation R

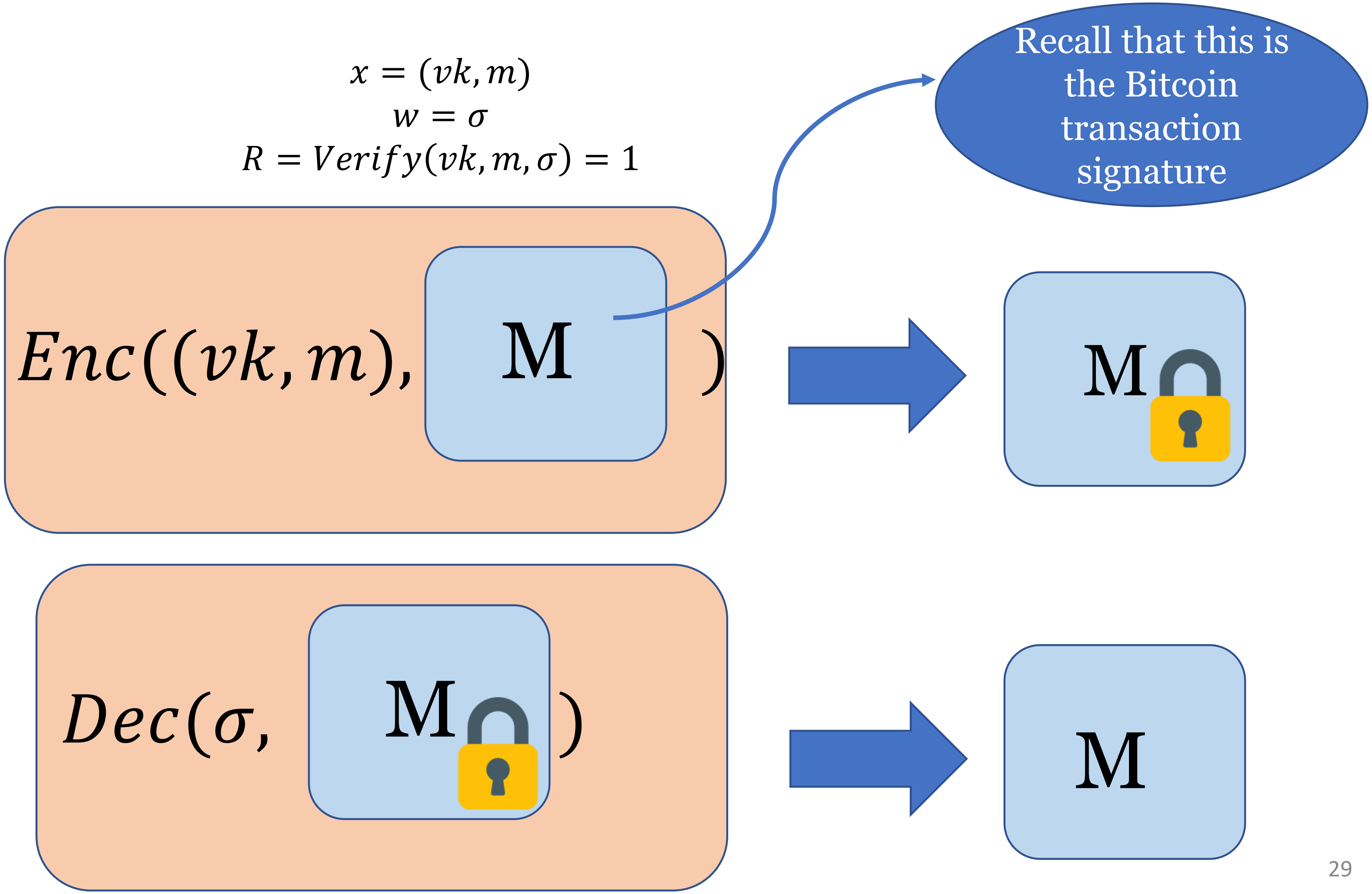
Let $x \in L$

Let w be such that $R(x, w) = 1$



Verifiable witness encryption based on Threshold Signatures

$$x = (vk, m)$$
$$w = \sigma$$
$$R = Verify(vk, m, \sigma) = 1$$



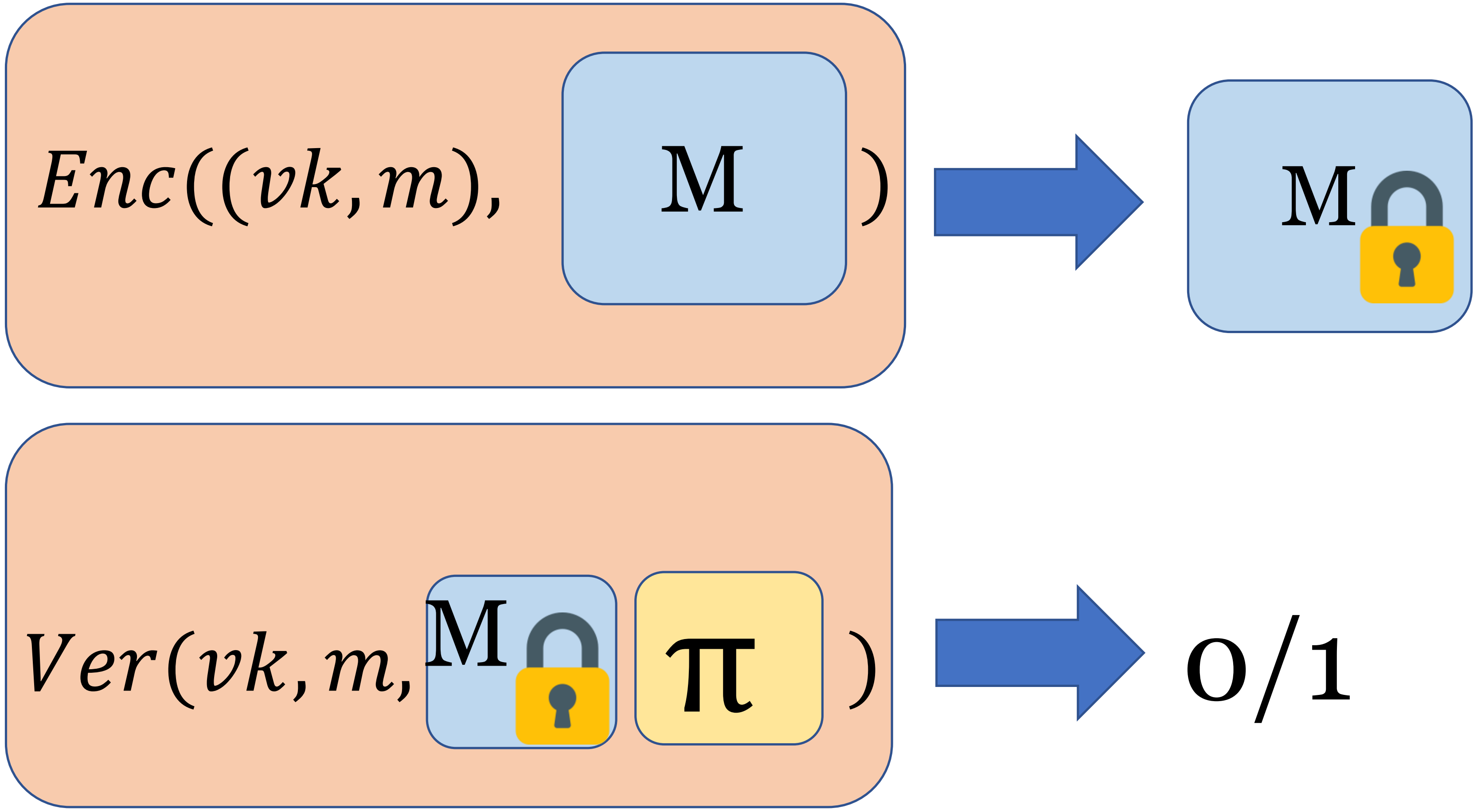
Verifiable witness encryption based on Threshold Signatures

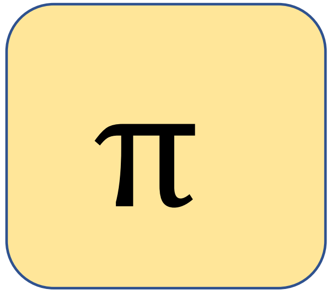
$$x = (vk_1, vk_2, \ldots, vk_n, m)$$

$$w = \sigma_1, \sigma_2, \ldots, \sigma_k$$

$$R = Verify(vk_1, m, \sigma_1) = 1$$
$$Verify(vk_2, m, \sigma_2) = 1$$
.
.
.
$$Verify(vk_k, m, \sigma_k) = 1$$
$$k \geq \rho$$

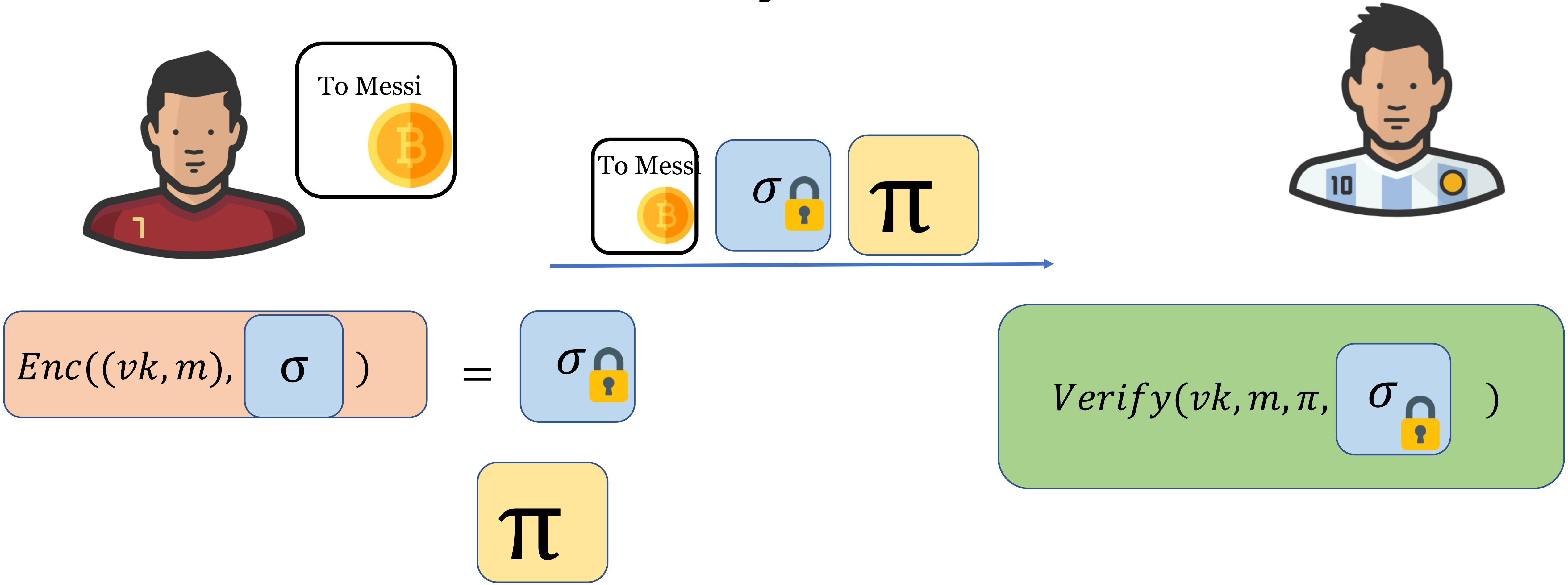
Verifiable witness encryption based on Threshold Signatures





Computed using NIZK cut-and-choose techniques

Oracle-based Conditional Payments



“Argentina won the world cup”

Compute $\bar{\sigma} = Sign(sk, m)$

To Messi σ

$\bar{\sigma}$

$Dec(\bar{\sigma}, \sigma)$ → σ

Broadcast To Messi σ and claim the winnings

Multiple Outcomes

Naïve idea:
Repeat the
above protocol
N times

M_1 M_2

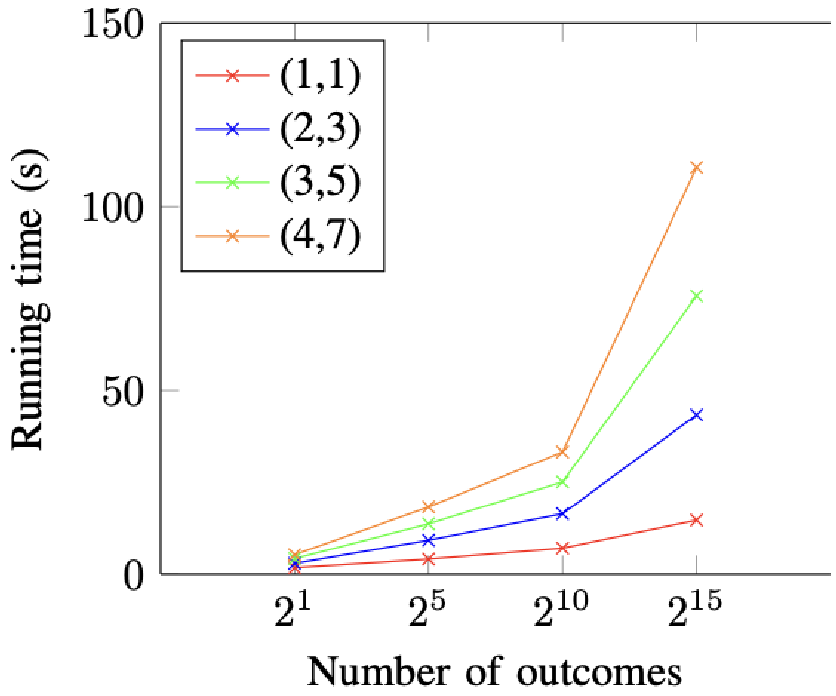
M_3 M_4

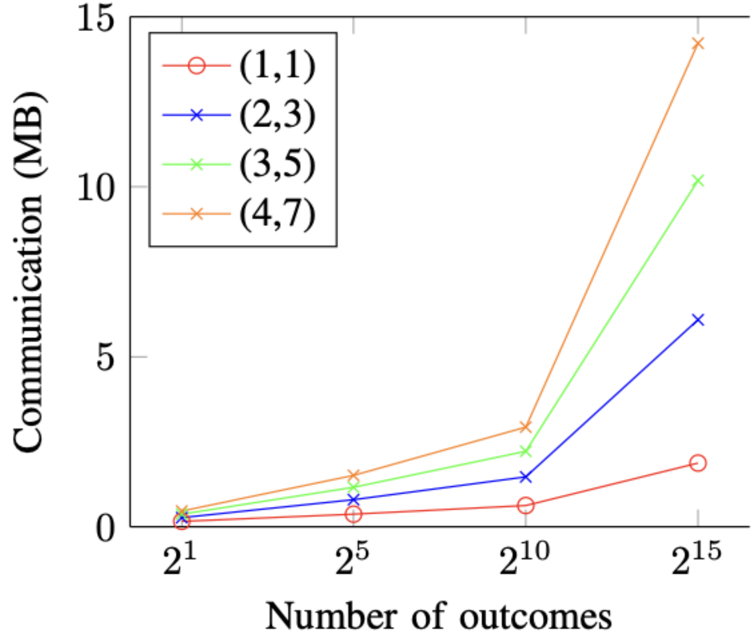
....

M_{N-1} M_N

Optimization: Use Lindell-Riva's technique to amortize the cost of cut-and-choose

Performance





Security parameter: 128

For a threshold of 4 out of 7 oracles and a payment conditioned on up to 2^{15} different real-world event outcomes, the computation overhead is less than 150 seconds and the total communication overhead is below 15 MB.

Comparison with smart contracts

	Smart Contracts	Cryptographic Oracle-Based Contracts
Works only with cryptocurrencies that support Turing-complete scripting languages	Yes	No
Scalable	No	Yes
Fungibility	No	Yes
High on-chain costs	Yes	No

Some applications

- Financial Adjudication
- Pre-scheduled payments
- Trading
- Encryption to the future

In Summary

Contribution: A new cryptographic tool VweTS

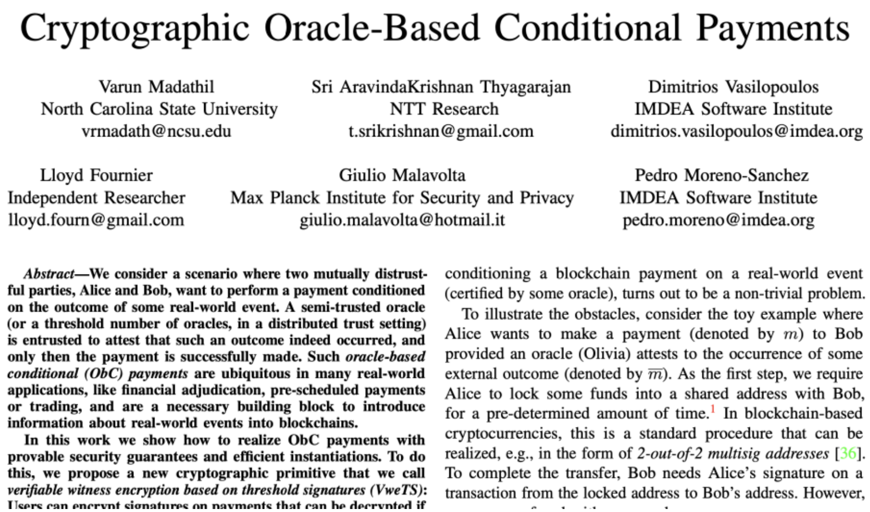
Application: Oracle-based conditional payments

Implication: Scalable, cheaper, distributed trust, compatibility for cryptocurrency payments

Ground for future work: more complex policies than threshold, further speed ups

Full version: *https://eprint.iacr.org/2022/499*

Email : vrmadath@ncsu.edu



Cryptographic Oracle-Based Conditional Payments

Varun Madathil
North Carolina State University
vrmadath@ncsu.edu

Sri AravindaKrishnan Thyagarajan
NTT Research
t.srikrishnan@gmail.com

Dimitrios Vasilopoulos
IMDEA Software Institute
dimitrios.vasilopoulos@imdea.org

Lloyd Fournier
Independent Researcher
lloyd.fourn@gmail.com

Giulio Malavolta
Max Planck Institute for Security and Privacy
giulio.malavolta@hotmail.it

Pedro Moreno-Sanchez
IMDEA Software Institute
pedro.moreno@imdea.org

***Abstract*—We consider a scenario where two mutually distrustful parties, Alice and Bob, want to perform a payment conditioned on the outcome of some real-world event. A semi-trusted oracle (or a threshold number of oracles, in a distributed trust setting) is entrusted to attest that such an outcome indeed occurred, and only then the payment is successfully made. Such *oracle-based conditional (ObC) payments* are ubiquitous in many real-world applications, like financial adjudication, pre-scheduled payments or trading, and are a necessary building block to introduce information about real-world events into blockchains.**

In this work we show how to realize ObC payments with provable security guarantees and efficient instantiations. To do this, we propose a new cryptographic primitive that we call *verifiable witness encryption based on threshold signatures (VweTS)*:

conditioning a blockchain payment on a real-world event (certified by some oracle), turns out to be a non-trivial problem.

To illustrate the obstacles, consider the toy example where Alice wants to make a payment (denoted by m) to Bob provided an oracle (Olivia) attests to the occurrence of some external outcome (denoted by $\overline{m}$). As the first step, we require Alice to lock some funds into a shared address with Bob, for a pre-determined amount of time.[1] In blockchain-based cryptocurrencies, this is a standard procedure that can be realized, e.g., in the form of *2-out-of-2 multisig addresses* [36]. To complete the transfer, Bob needs Alice's signature on a transaction from the locked address to Bob's address. However,

Thank You!