Dario Crippa

10529288@mail.polimi.it

CRYPTO CONDITIONS.

Introduction.

Presenting Crypto Conditions

Crypto conditions define a set of encoding formats and data structures used to describe conditions and fulfillments

combining existing signature mechanisms and hash functions

- **Context**
  Application domain
- **Purpose**
  What are they used for?
- **Features**
  Main characteristics

Condition.

Fingerprint of a circuit

Agents can define a condition that must be satisfied

in order for a particular action or transaction to occur

- **Types**

  Condition types

- **Fingerprint**

  Circuits identification

Fulfillment.

Circuit input

Constitutes the cryptographic proof or evidence provided to validate the condition

data structure that holds the information required to satisfy a condition

- **Payload**

  Fulfillment content

Validation.

Evaluation of the fulfillment

A fulfillment is considered valid if it matches the fingerprint and if the circuit output is TRUE

it meets the given condition

- **Messages**

  Signature schemes

PreimageSHA256.

Type_ID : 0

```
PreimageSHA256 CONDITION ::= {
    fingerprint     SHA256(preimage=secret_message)
    cost            INTEGER
}

PreimageSHA256 FULFILLMENT ::= {
    preimage    secret_message
}
```

Ed25519SHA256.

Type_ID : 4

```
Ed25519SHA256 CONDITION ::= {
    fingerprint     SHA256(publicKey.encode)
    cost            INTEGER
}

Ed25519SHA256 FULFILLMENT ::= {
    publicKey     ED25519 publicKey
    signature     ED25519 privateKey.sign(secret_message)
}
```

ThresholdSHA256.

Type_ID : 2

```
ThresholdSHA256 CONDITION ::= {
    fingerprint         SHA256(fingerprint_contents.encode)
    cost                INTEGER
    subtypes            ConditionTypes
}


ed25519SHA256 FINGERPRINT_CONTENTS ::= {
    threshold           INTEGER
    subconditions       SET of subconditions
}


ed25519SHA256 FULFILLMENT ::= {
    subfulfillment      SET of subfulfillments
    subconditions       SET of subconditions
}
```

Questions?

THANK YOU.