Dario Crippa
10529288@mail.polimi.it

CRYPTO CONDITIONS.

Introduction.

Crypto Conditions in brief

Crypto Conditions defines a set of encoding formats and data structures for conditions and fulfillments

combining existing signature schemes or hash functions

Condition.

Fingerprint of a circuit

Users or developers define a set of conditions that need to be satisfied

for a particular action or transaction to occur

Fulfillment.

Circuit structure

Represents the cryptographic proof or evidence

provided to satisfy the conditions

Validation.

Evaluation of the fulfillment

A fulfillment is considered valid if it matches the fingerprint

In other words the condition is satified

Preimage SHA256.

TYPE_ID : 0

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


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

Ed25519 SHA256.

TYPE_ID : 4

```
ed25519SHA256 CONDITION ::= {
    fingerprint    SHA256(publicKey.encode)
    cost           INTEGER
}


ed25519SHA256 FULFILLMENT ::= {
    publicKey    ED25519 publicKey
    signature    ED25519 privateKey.sign(secret_message)
}
```

Threshold SHA256.

TYPE_ID : 2

```
ThresholdSHA256 CONDITION ::= {
    fingerprint      SHA256(fingerprint_content.encode)
    cost             INTEGER
}


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


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

Questions?

THANK YOU.