Decoupling Digital Currency Authenticity and Value with Certified Digital Tokens

Derk Norton
Founding Partner
Crater Dog Technologies™

March 24, 2015

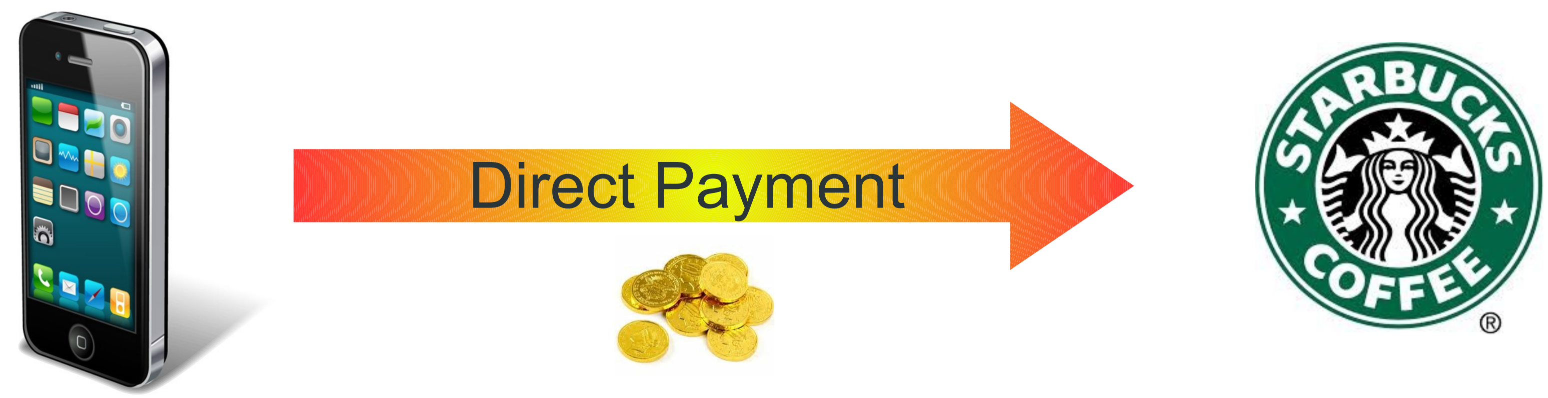
A Hypothesis

BitCoin may not become a true digital currency because...

- it won't be able to scale up to billions of wallets,
- transactions take too long to confirm for most consumer interactions,
- and the authenticity and value of each coin are inseparable.

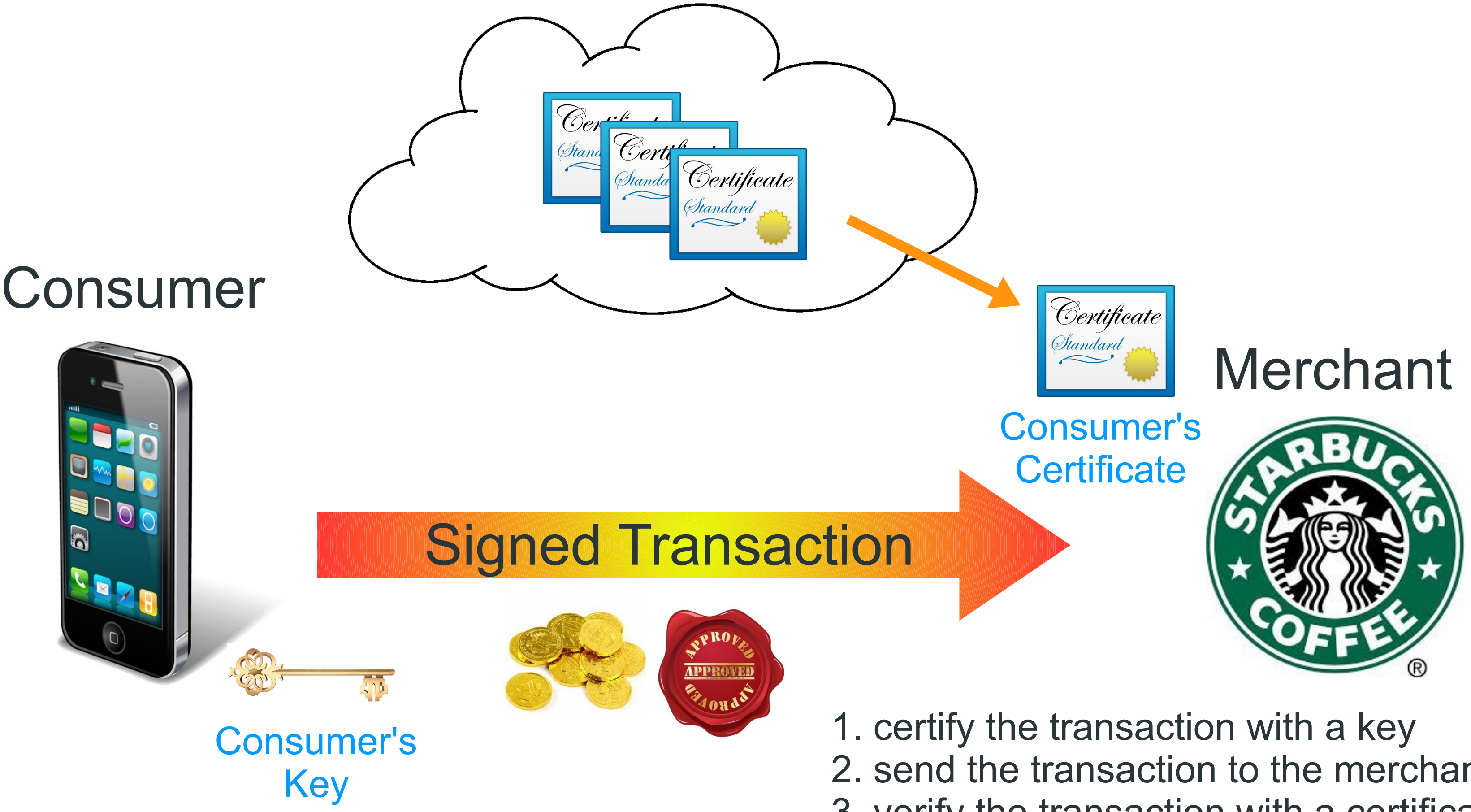
A *certified digital token* (CDT) based approach may address these issues, we will explore that here today...

Direct Payments



Direct Payment

Digitally Signed Transactions



Consumer

Merchant

Consumer's Certificate

Signed Transaction

Consumer's Key

1. certify the transaction with a key
2. send the transaction to the merchant
3. verify the transaction with a certificate

Benefits

Consumer

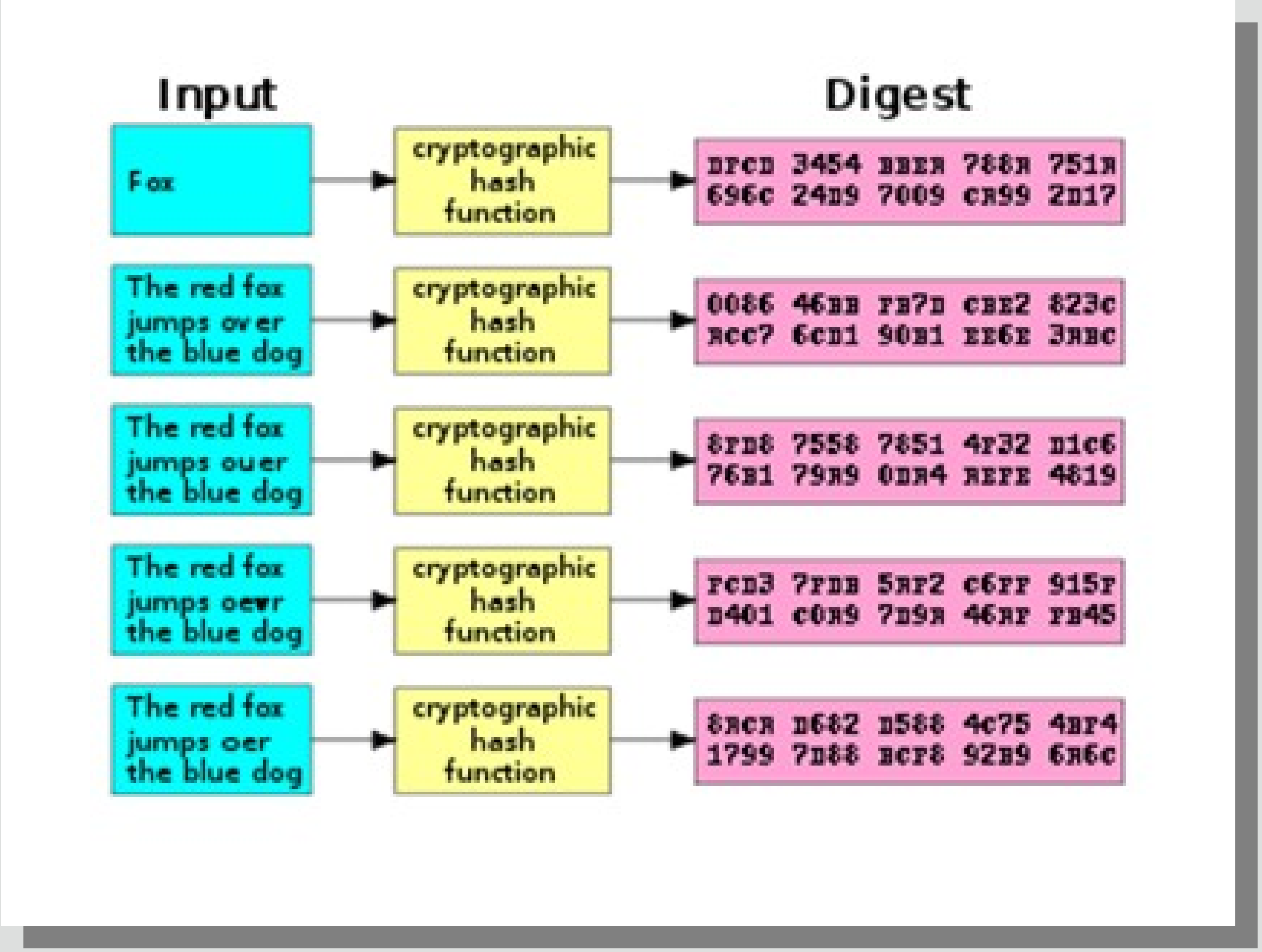
- convenient
- no credit card fees
- no theft or loss

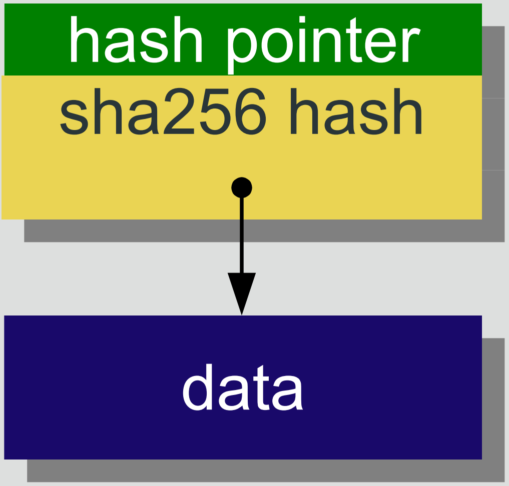
Merchant

- no processor fees
- immediate settlement
- no fraud or forgery

Direct Payment
STARBUCKS COFFEE

Cryptographic Hashing


Input
Digest
Fox
cryptographic hash function
DFcD 3454 BBEA 788A 751A
696c 24D9 7009 cA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D cBE2 823c
Acc7 6cD1 90B1 EE6E 3ABc
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1c6
76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FcD3 7FDB 5AF2 c6FF 915F
D401 c0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8AcA D682 D588 4c75 4BF4
1799 7D88 BcF8 92B9 6A6c



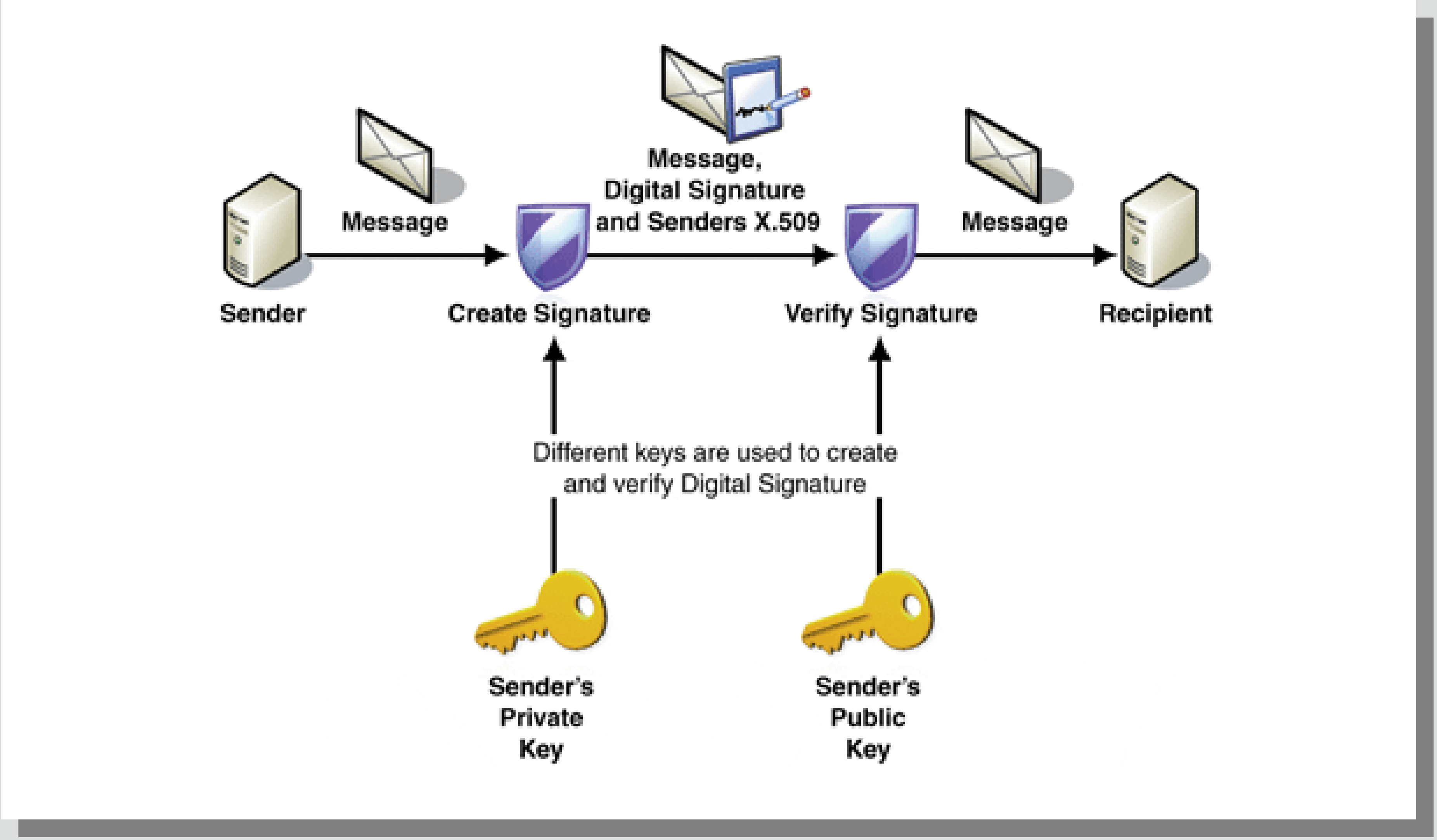
hash pointer

sha256 hash

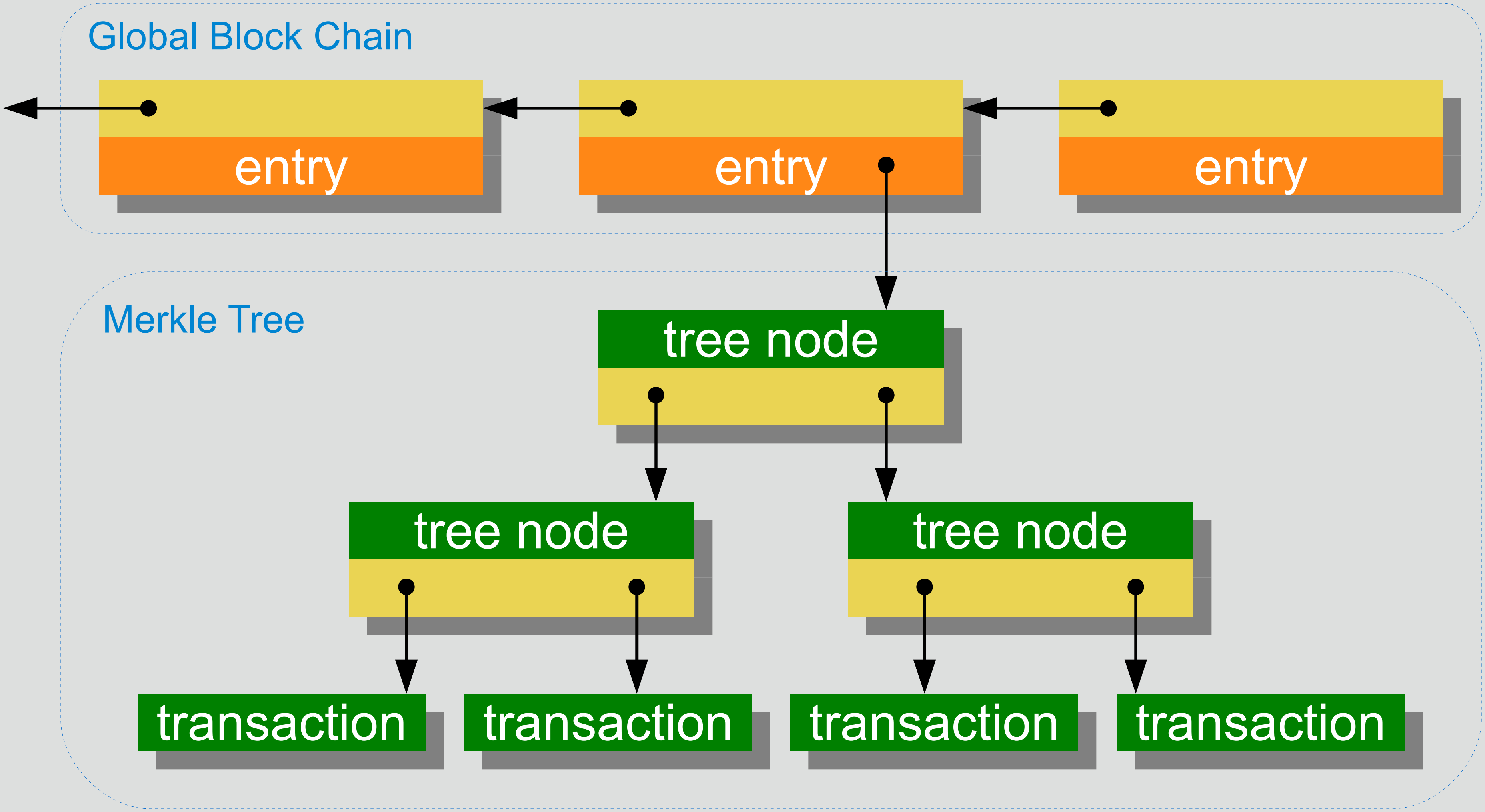
data

- if data changes...
- hash is invalid

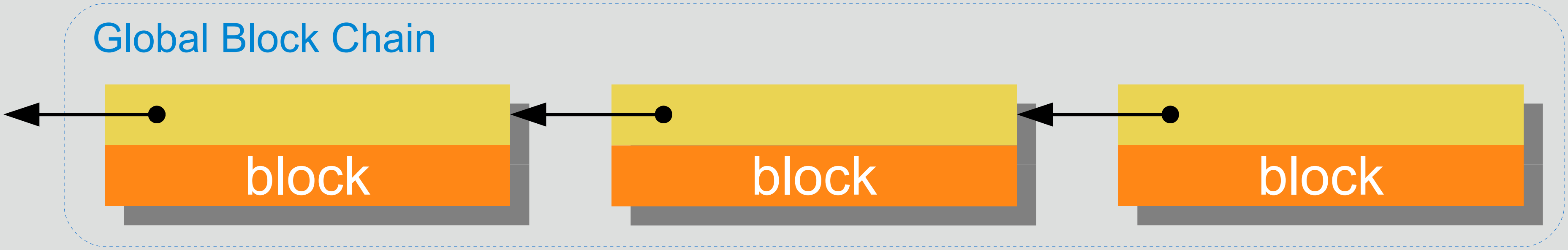
Digital Signatures


Message
Message, Digital Signature and Senders X.509
Message
Sender
Create Signature
Verify Signature
Recipient
Different keys are used to create and verify Digital Signature
Sender's Private Key
Sender's Public Key

BitCoin Global Ledger



BitCoin Model



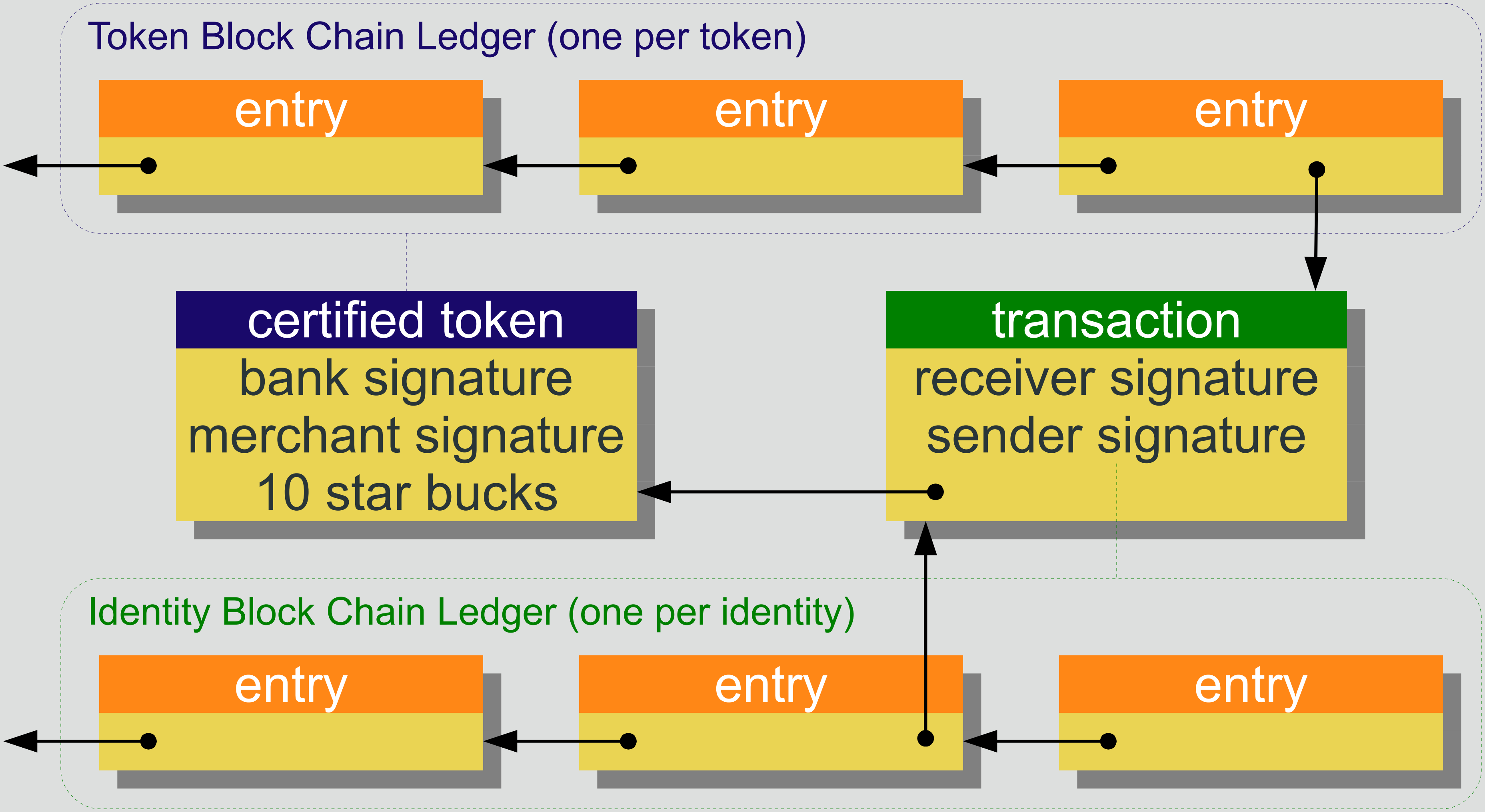
Advantages

- incentive driven
- no central anything
- assumes no one is trusted
- public verifiable ledger
- limited supply of coins

Challenges

- doesn't scale
- long confirmation times
- no value guarantor
- complex protocol
- block chain forking
- coins outlive algorithms

CDT Ledgers



Token Block Chain Ledger (one per token)

certified token

bank signature

merchant signature

10 star bucks

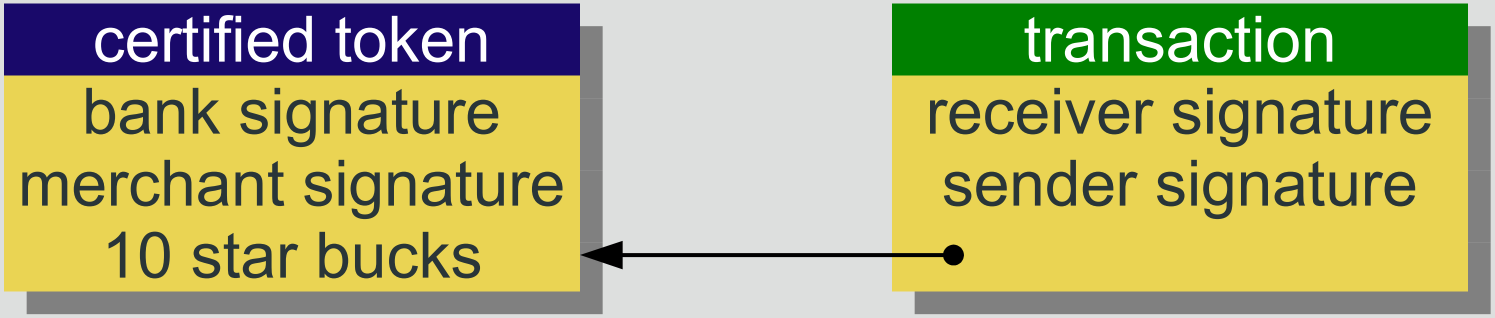
transaction

receiver signature

sender signature

Identity Block Chain Ledger (one per identity)

CDT Model



certified token

bank signature
merchant signature
10 star bucks

transaction

receiver signature
sender signature

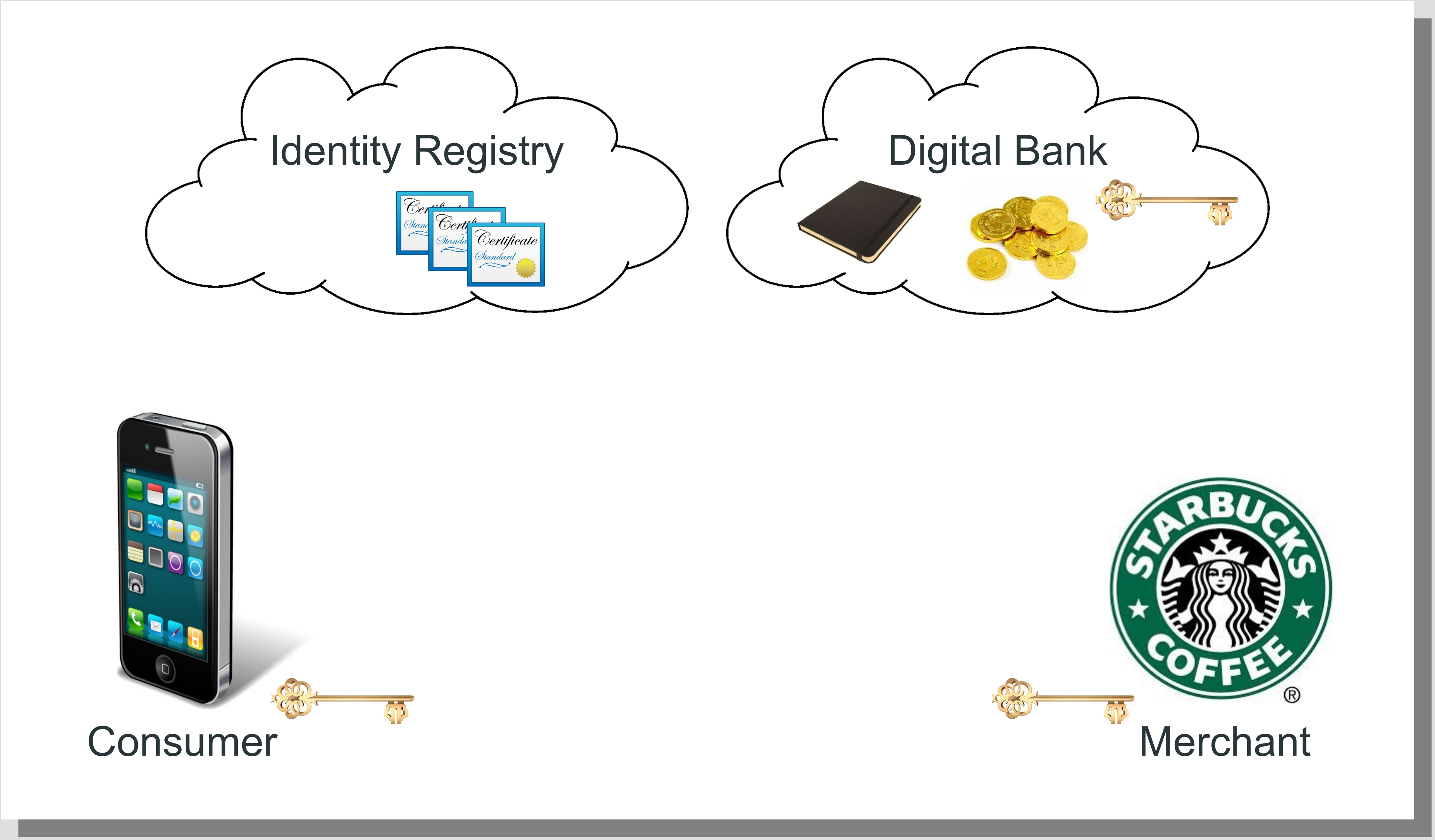
Advantages

- highly scalable
- token value is guaranteed
- all parties sign transaction
- immediate confirmation
- separate verifiable ledgers
- renewable tokens

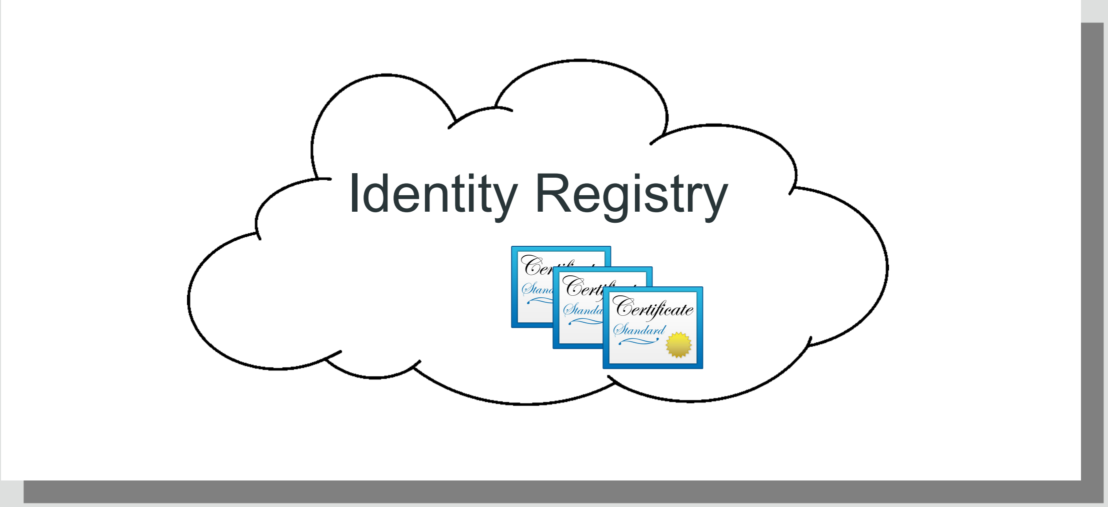
Challenges

- no partial transfers
- must trust guarantors
- open transactions?

CDT Architecture



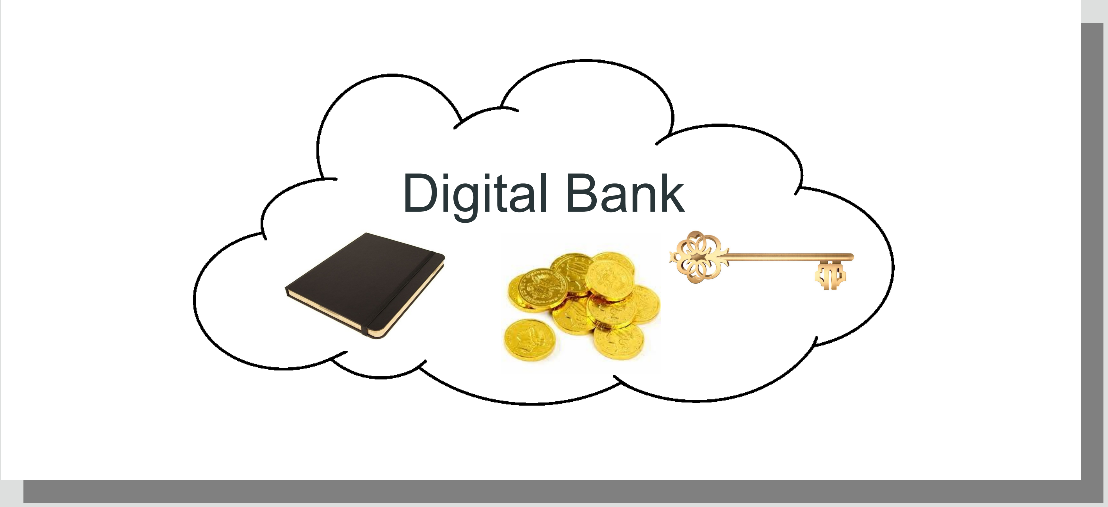
Identity Registry



- Maintains a public list of pseudo-anonymous* identities.
- Maps a list of public certificates to each identity.
- Certificates are used to verify digital signatures.

*complete anonymity is probably not possible

Digital Bank



- Maintains a public list of all certified digital tokens.
- Maintains a public ledger for each token.
- Maintains a public ledger for each identity.

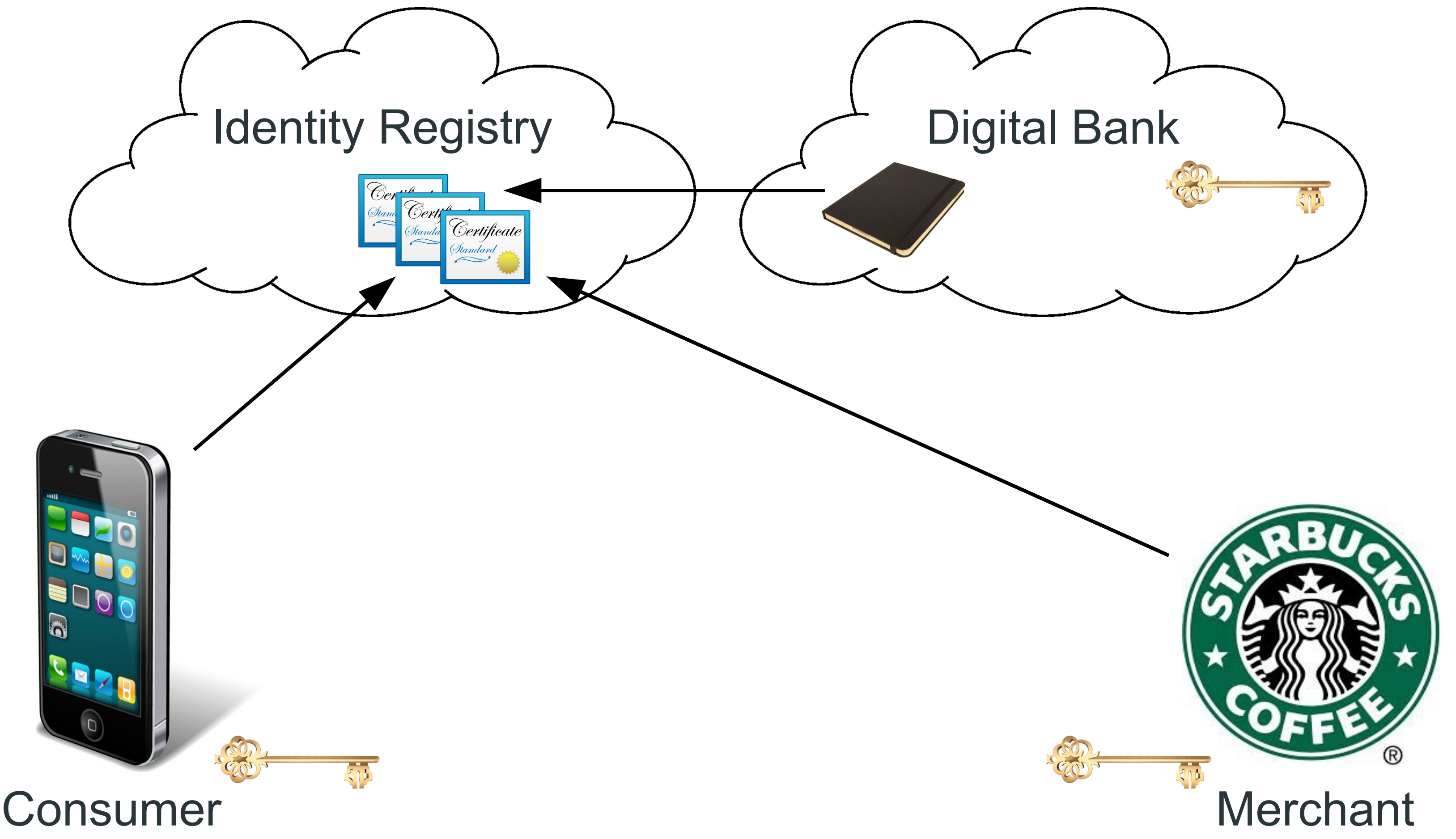
Merchant

- Has a private signing key.
- May ask a bank to certify a batch of digital tokens.
- May initiate or receive payment transactions.
- Verifies transactions using public certificates.

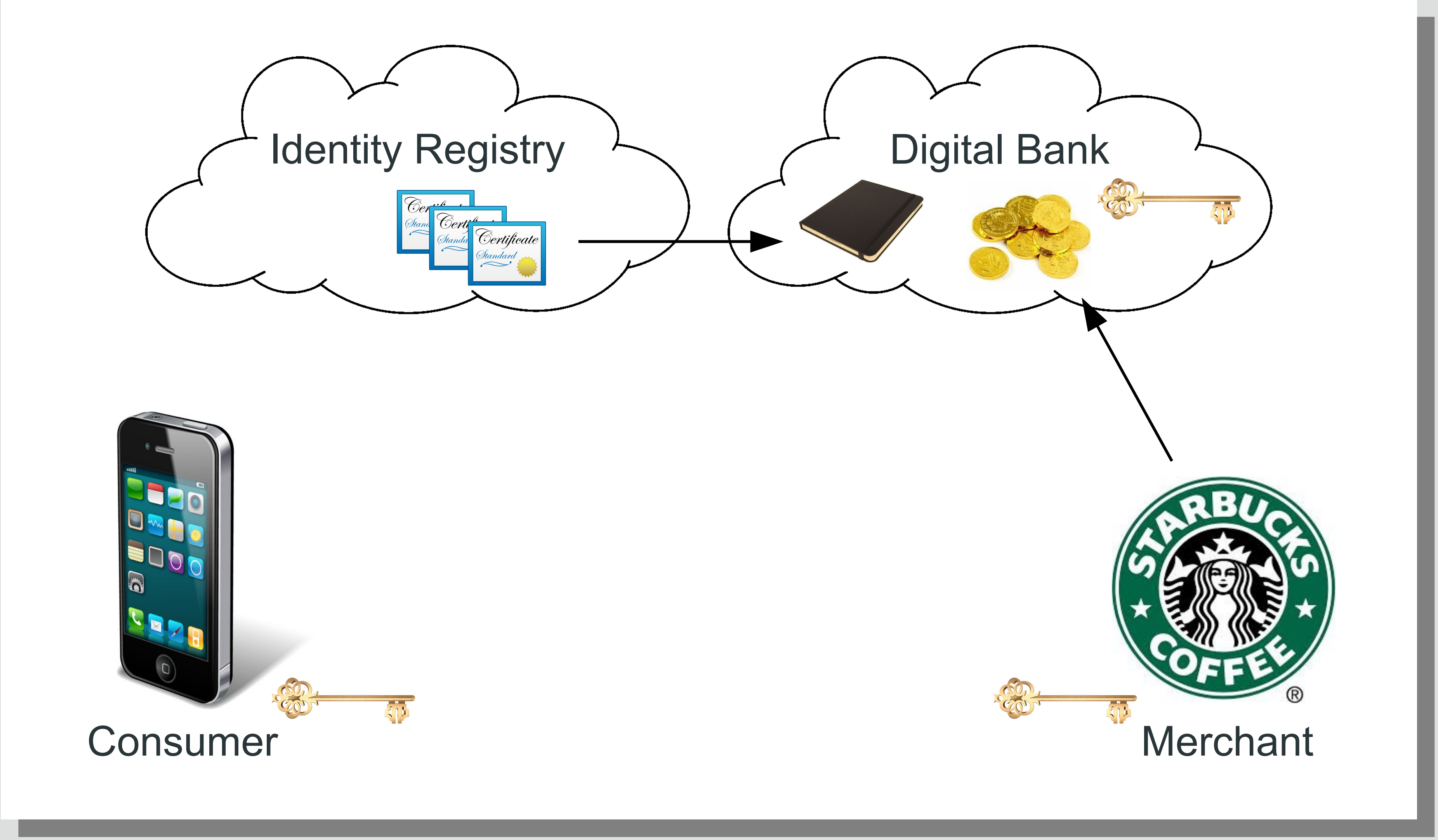
Consumer

- Has a private signing key.
- May initiate or receive payment transactions.
- Verifies transactions using public certificates.
- May ask a digital bank to make change.

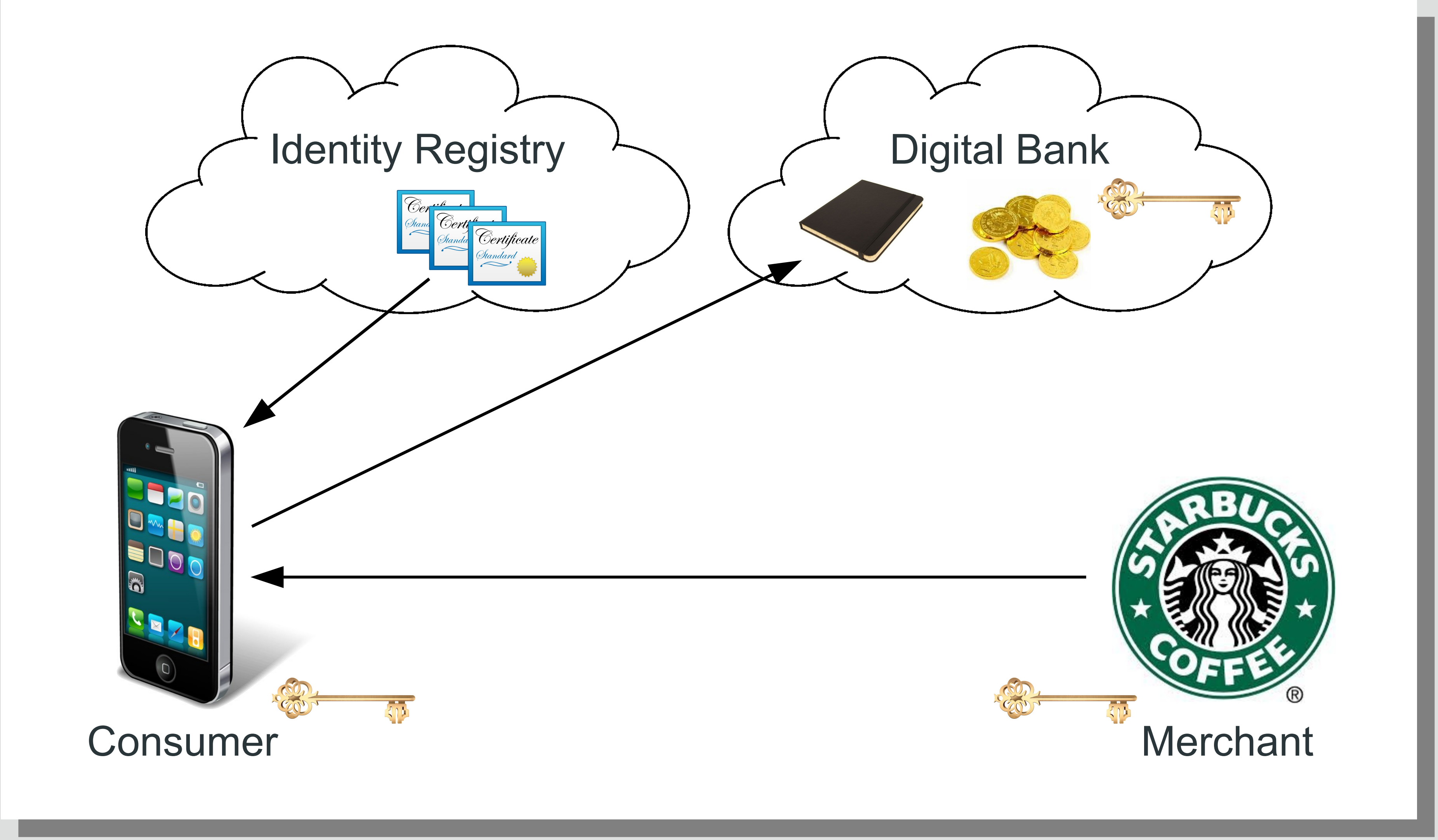
Registering Identities



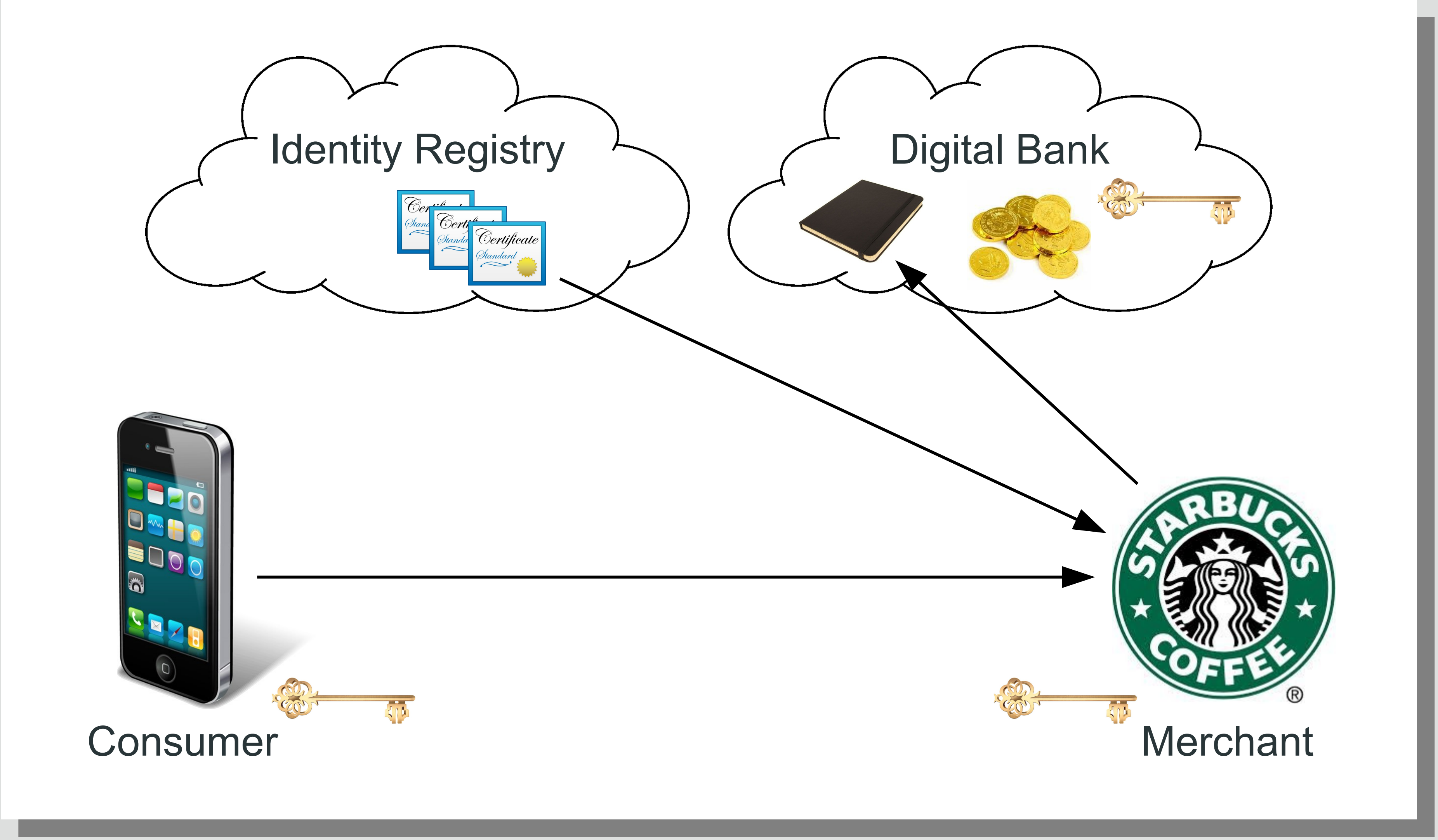
Certifying Tokens



Awarding Tokens



Paying with Tokens



Demo

- Scenario
  - a merchant wants to reward its faithful consumers with CDTs in the form of "star bucks"
- Identity Registry and Digital Bank
  - each is a RESTful web service
  - both are running in the Amazon cloud
- Consumer and Merchant
  - each has its own laptop
  - both run RESTful clients to access services

Possible Conclusions

- Scalability
  - may be many digital banks
  - no single block chain as a bottleneck
- Settlement
  - near instantaneous transactions
  - 100% verifiable
- Value and Authenticity
  - token value is guaranteed by the merchant
  - token authenticity is certified by the digital bank