Aalto University
School of Electrical
Engineering

SOFIE

Interledger: Theory and practice

Santeri Paavolainen, Tommi Elo & Pekka Nikander
ICBC 2019, Seoul, Korea

Introduction and background

Motivation: Why interledger?

Interledger in practice: an example

Different interledger approaches

Typical use cases

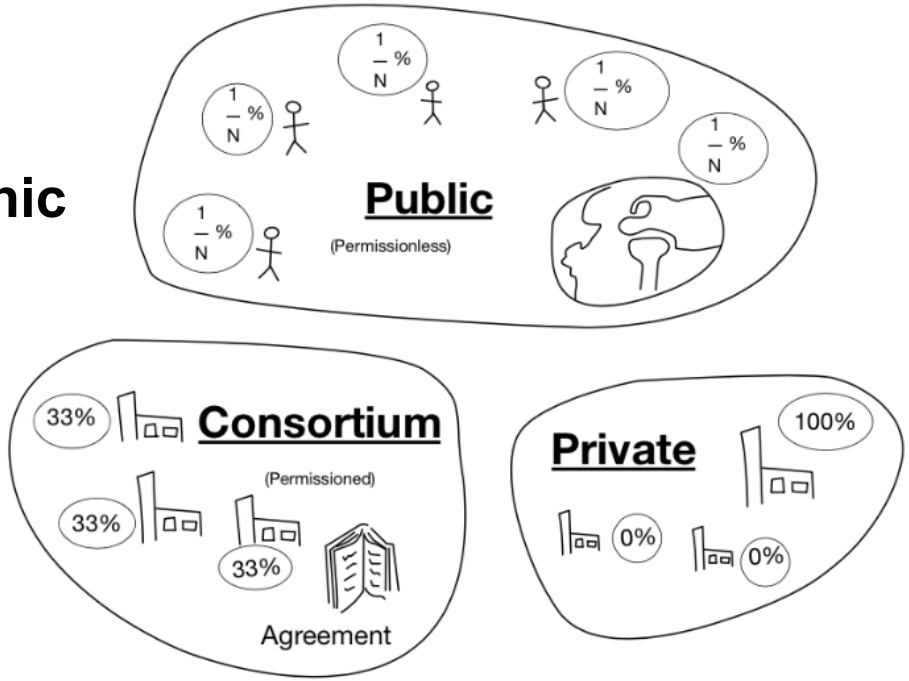
Summary

Introduction

- **This presentation goes through interledger approaches and presents examples of use cases**

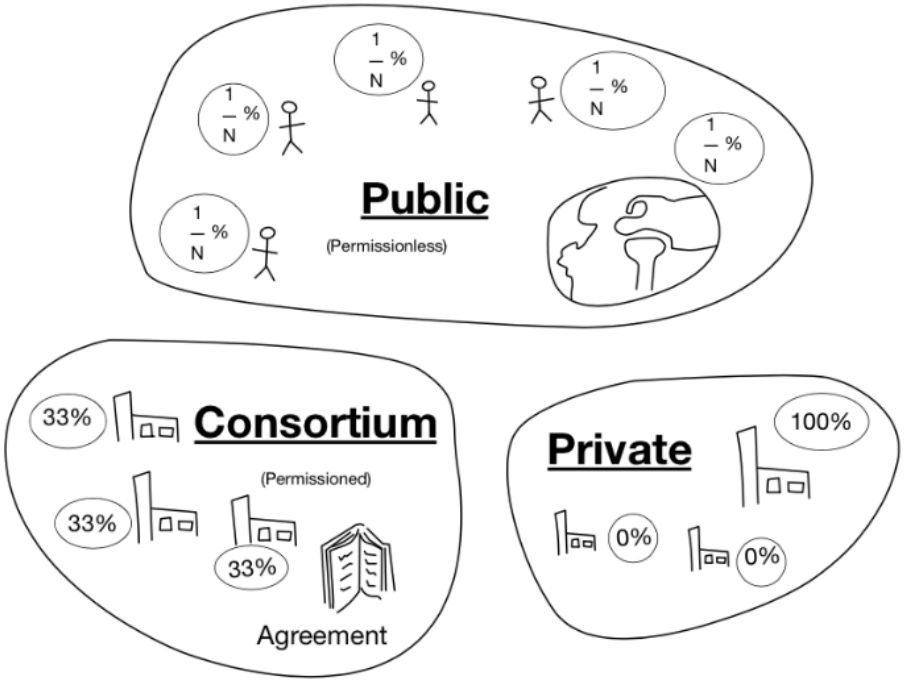
Background

- Overview of DLT landscape
- Brief introduction to smart contracts
- Recap of needed cryptographic primitives

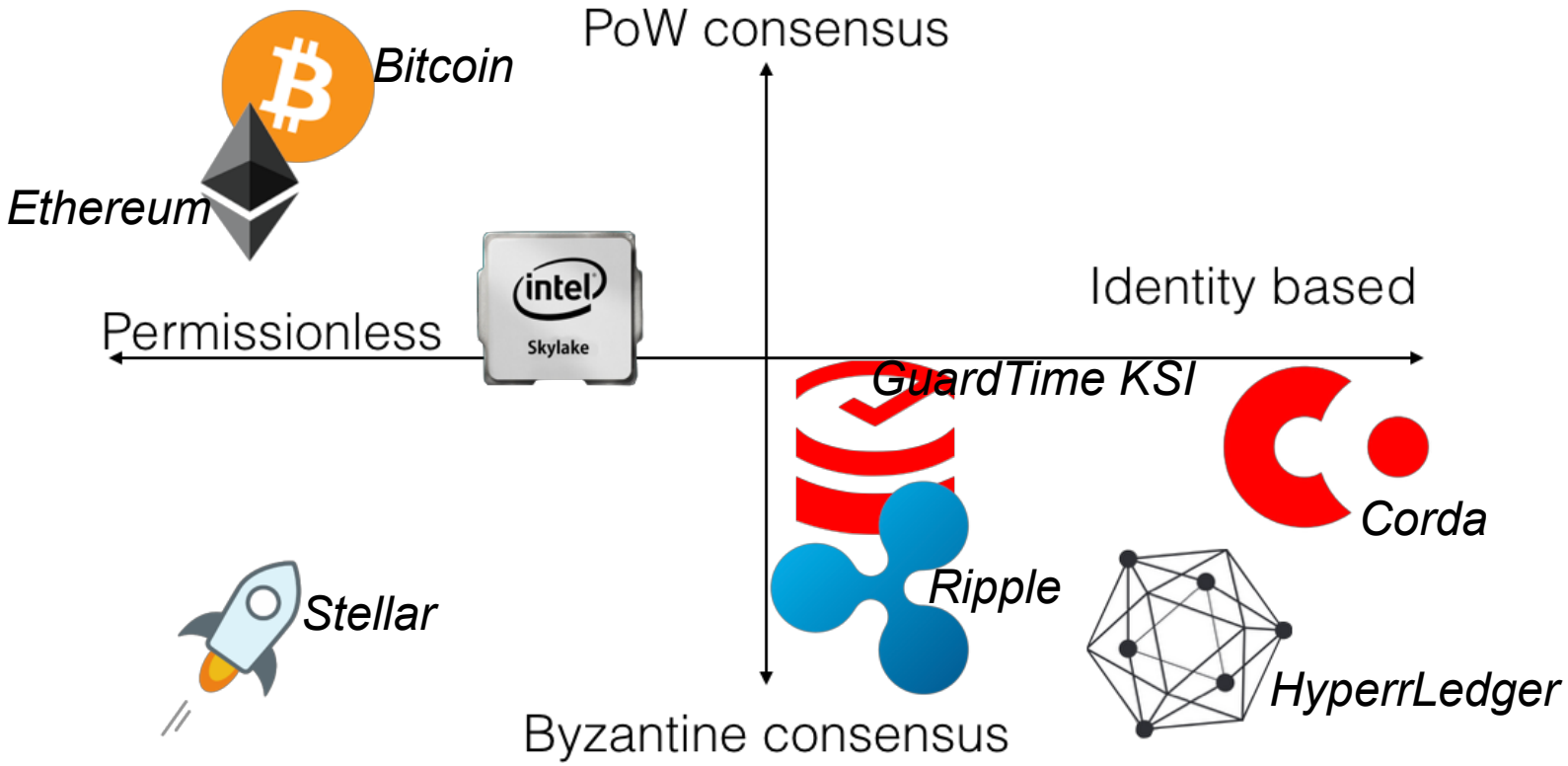


DLT landscape 1/2

- **Public permissionless DLTs are blockchains**
  - Typically nakamoto blockchains
  - Decentralisation: n >> 1000
- **Permissioned DLTs**
  - Typically Byzantine consensus based
  - Requires an identity (usually from a centralised source e.g. state registry. There is no such thing as “real identity”)
  - Decentralisation: n ~ 10, n < 100.



DLT landscape 2/2

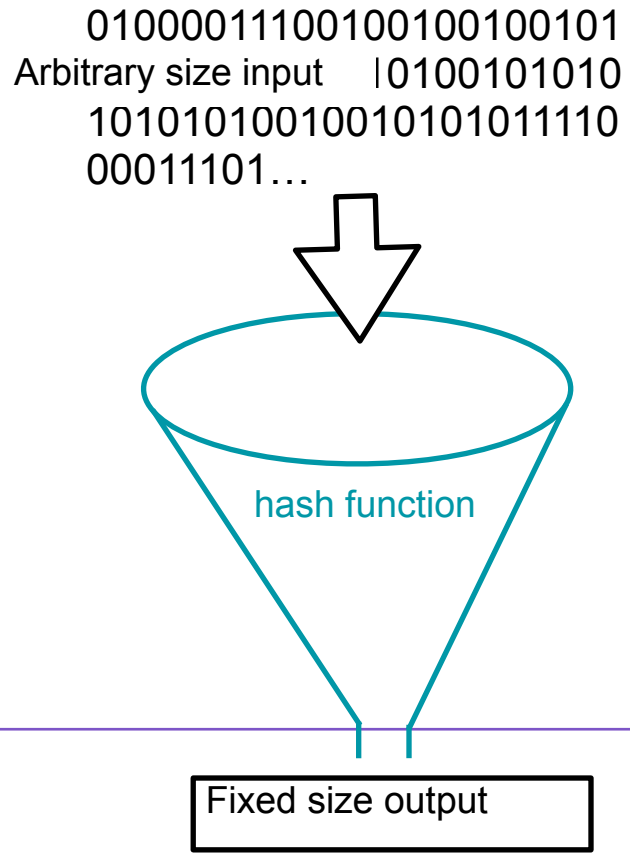


Brief introduction to smart contracts

- **Smart Contracts are programs, which run on a decentralised computer**
  - In Ethereum, referred to as *running on the blockchain*
- **In HyperLedger, smart contracts are known as Chaincode and they are of installed in the validator nodes at the time a Fabric network is launched**

Cryptographic hash functions

- **Cryptographic hash functions provide a small *fixed size collision resistant one-way* output of an input of undetermined size**
- **Basis for digital signatures and blockchains**
- **Examples:**
  - SHA-256, SHA-512, RIPEMD-160



Cryptographic signatures

- **Way to sign and verify contracts between parties**
- **Requires public key cryptography**
  - The correct party can sign, everyone with public key can verify the signature
  - Encrypting the hash with the private key
  - Decrypting the encrypted hash with the public key

Introduction and background

Motivation: Why interledger?

Interledger in practice: an example

Different interledger approaches

Typical use cases

Summary

Why interledger?

- Why multiple DLTs?
- DLTs vs. typical application requirements

Why multiple DLTs?

- One ledger cannot achieve dominance easily
- Different accounting needs will work on different ledger technologies
- Complex applications will need to work with different ledgers
- Performance is also a factor…

DLTs vs. typical requirements

	Price of write operation	First Confirmation delay	High confidence confirmation delay	Publicity	Capability to force ledger to forget
Bitcoin	~1 $ / tx	10 min	1 h	Public	No
Ethereum	~0.12 $ / tx	15 s	10 min	Public	No
HyperLedger Fabric	HW ownership cost	seconds	No high confidence	Customisable	Via governance
R3 Corda	HW ownership cost	subsecond	No high confidence	Customisable	Via governance
SQL Database	HW ownership cost	No confirmations, authority	No confirmations, authority	Private	Via superuser

Introduction and background

Motivation: Why interledger?

Interledger in practice: an example

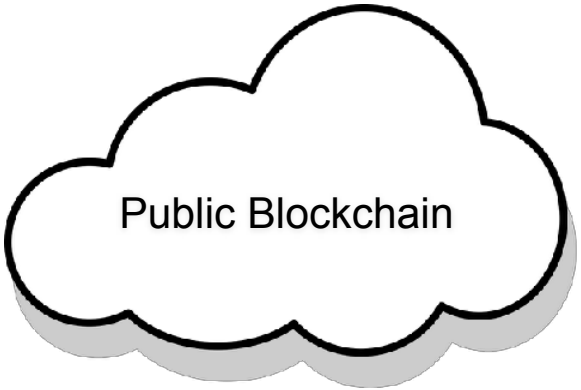
Different interledger approaches

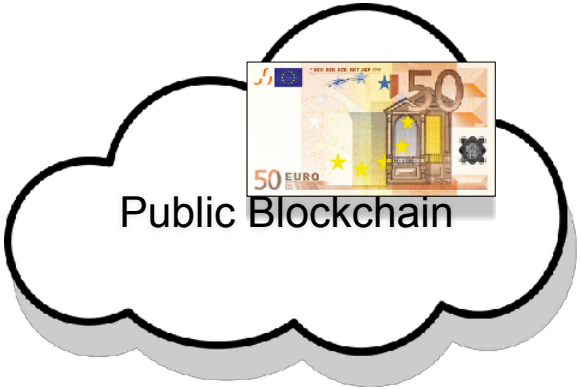
Typical use cases

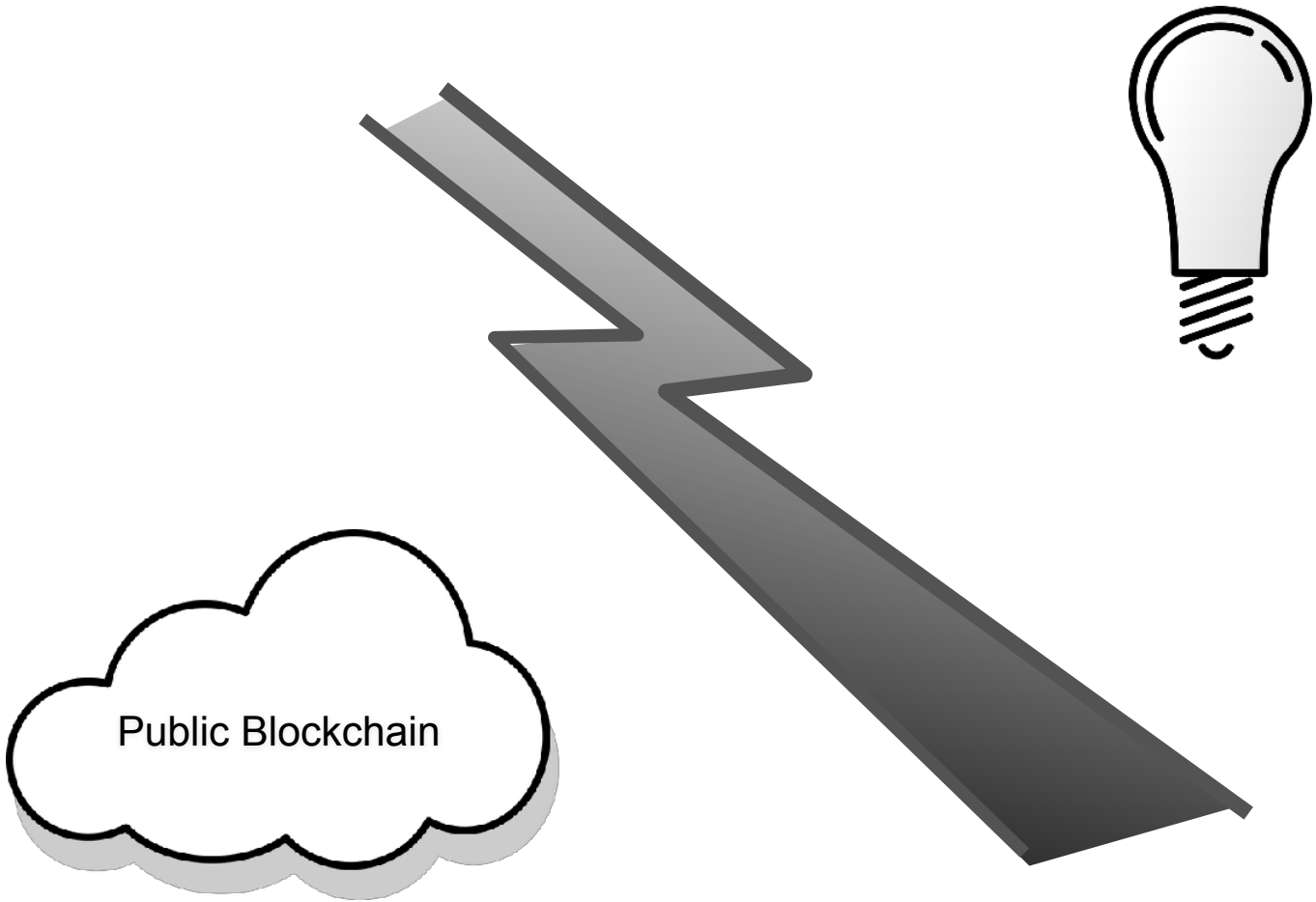
Summary

Interledger in practice: an example

- **We want to pay for using an IoT device**
  - Essentially rent a device for money on the fly
- **We use a lamp connected to a private ledger**
  - … and pay via public ledger
- **Ledgers are interconnected via a gateway**


Public Blockchain


50
50 EURO
Public Blockchain


Public Blockchain


Permissioned Ledger

Permissioned Ledger

Public Blockchain

Gateway

Permissioned Ledger

Public Blockchain

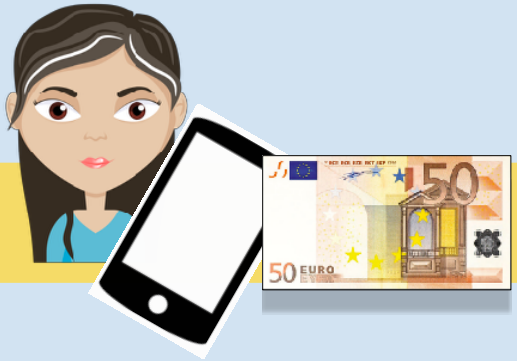
Gateway

Permissioned Ledger

Public Blockchain

Gateway

Permissioned Ledger



Public Blockchain

Gateway

Permissioned Ledger

Public Blockchain

Gateway

Permissioned Ledger

Public Blockchain

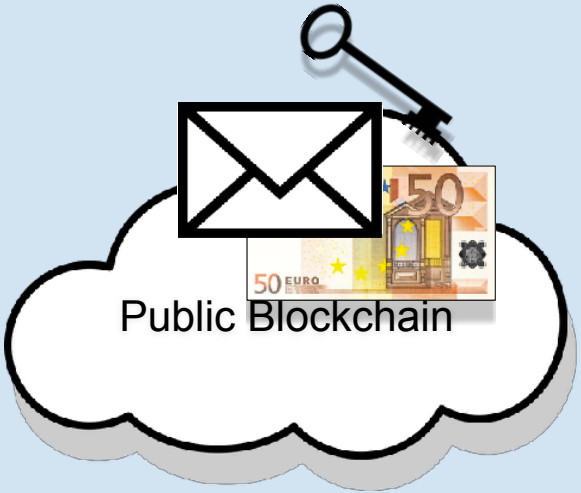
Gateway

Permissioned Ledger

Public Blockchain

Gateway

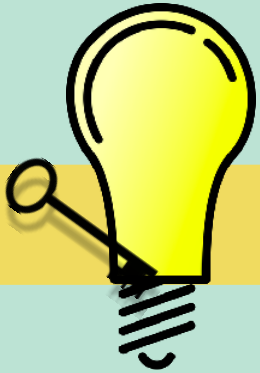
Permissioned Ledger



Public Blockchain

Gateway

Permissioned Ledger



Public Blockchain

Gateway

Permissioned Ledger

Introduction and background

Motivation: Why interledger?

Interledger in practice: an example

Different interledger approaches

Typical use cases

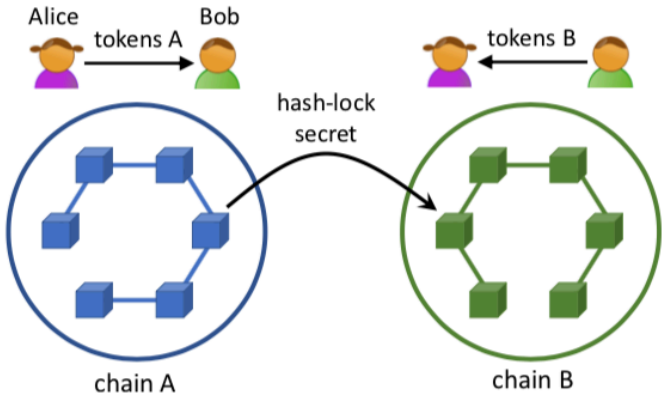
Summary

Interledger approaches

- Atomic cross chain transactions
- Sidechains
- Bridging
- Payment channels
- Ledgers of ledgers
- Interledger Protocol (ILP)

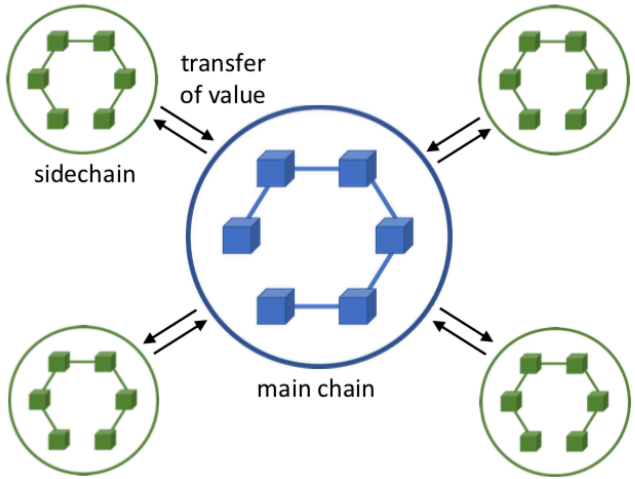
Atomic cross chain transactions

- **General technology to achieve transaction atomicity between two ledgers**
  - Requires primitive scripting from the ledger
  - Does not require a trusted third party



Sidechains

- **We lock assets in the main chain**
  - Collateral like
- **Transactions happen in the sidechain**
- **Updates can be made rarely to main chain**
  - Efficiency gains
  - Sidechains can have different security and different cost

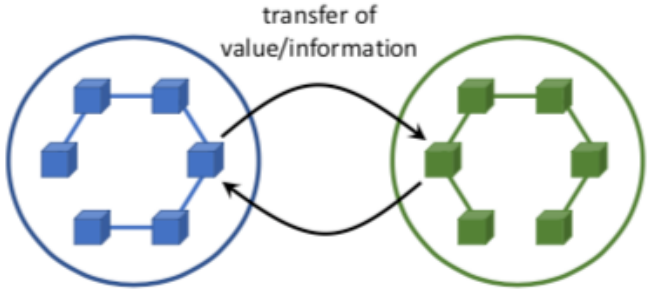


Sidechain approaches

- **Federated pegs**
  - Original side chain proposal
  - Byzantine agreement of multiple parties
  - Requires multisig ledgers and gateways
- **Merged mining**
  - Simultaneous PoW calculation for different blockchains with same hash function
- **Plasma**
  - Enables hierarchical tree of Proof-of-Stake sidechains with smart contracts
- **Cardano Settlement Layer**
  - Cardano CSL utilises sidechains and enables efficient sidechain proofs

Bridging

- **Bridging refers to approaches that aim to provide one or two-way transfer of both data or value between blockchains that are considered somewhat equal**
- **Bridging approaches**
  - Blocknet XBridge
  - ARK Smart Bridges
  - Ethereum BTC Relay
  - Parity POA Network



Transaction & payment channels: Lightning and Raiden

- **The Lightning Network is a decentralised system of micropayment channels whose transfer of value occurs off-chain.**
  - Micropayment channels are two-party accounts which contain an initial deposit made by the two parties.
  - Parties agree on a new balance
  - Utilises HTLCs
- **Raiden is similar to Lightning but for Ethereum**

Hash Time-Lock Contract (HTLC)

- **Payment method where**
  - *Receiver must acknowledge payment* has been received *by generating a cryptographic proof of payment before deadline* or loose the ability to claim the payment
  - Cryptographic proof of payment can be used to trigger other automation, even payment automation
- **Required ledger capabilities**
  - hash-lock support
  - time-locking support
- **Useful for *cross-chain atomic swaps* ie. Inter-ledger transactions**

Hash Time-Lock Agreement (HTLA)

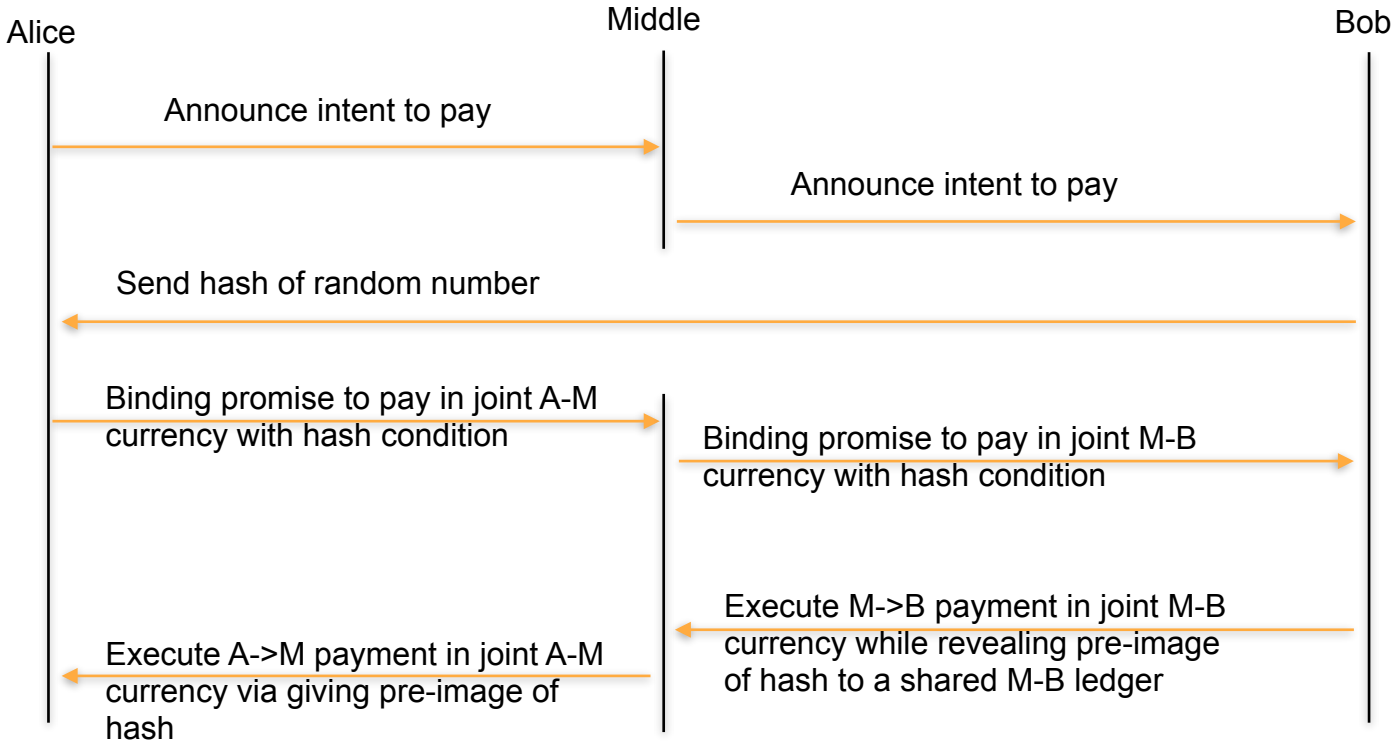
- **Hash Time-Lock Agreements are a generalisation of HTLCs across ledgers, first introduced in Inter-Ledger Protocol (ILP)**
  - Smart contract capability not required
  - Works with even *manual* ledgers
- **Different types of HTLA**
  1. Conditional Payment Channels (with HTLCs)
  2. On-Ledger Holds/Escrow (using HTLCs)
  3. Simple Payment Channels
  4. Trustlines

HTLA classification

	Conditional Payment Channels (with HTLCs)	On-Ledger Holds/ Escrow (using HTLCs)	Simple Payment Channels	Trustlines
Ledger Support Required	High	High	Medium	Low
Implementation Complexity	High	Medium	Low	Low
Bilateral Risk	Low	Low	Medium	High

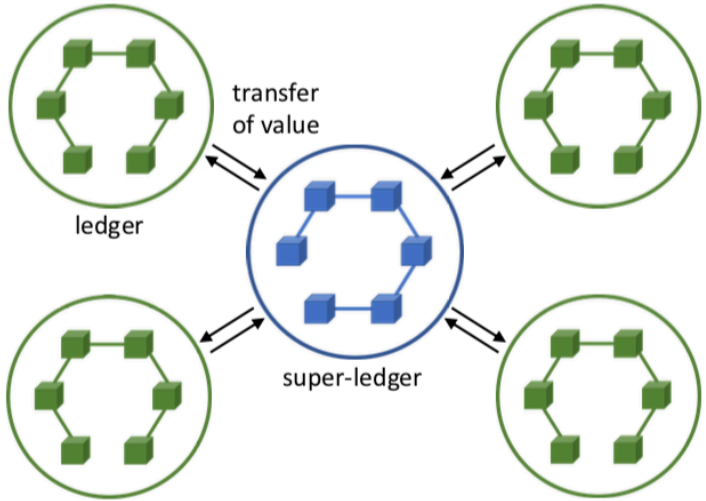
HTLC example: Alice needs pay to Bob but does not have a joint currency

- Middle shares the same currency with Alice, and another with Bob



Ledgers of ledgers

- **Ledger of ledger approach requires a single trusted ledger to pass the value or messages between others**
  - The questions are: Why would anyone care about the new super-ledger?
  - Why would anyone trust it
    - *The creation of this kind of trust is not via technical but political means*



Interledger Protocol

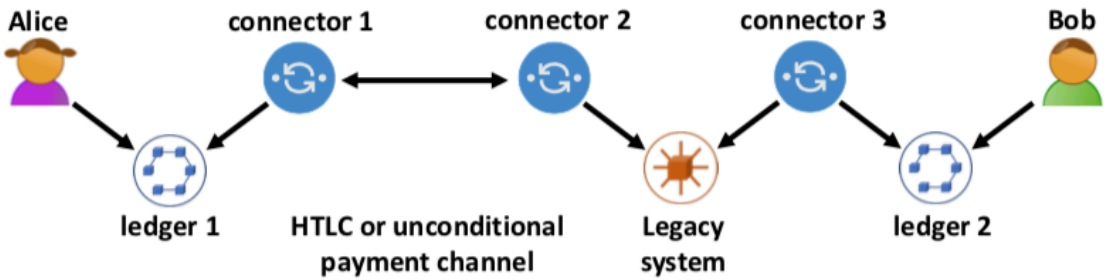


Figure displaying ILP protocol structure

- **Interledger protocols aims to combine different ledgers via connectors**
- **Minimum requirements are set for the ledgers to enable adoption**
  - Any kind of ledger is ok (along the lines of example “IP packets over avian carriers”)

Comparison of inter-ledger approaches

Approach	Handling of value	Trust mechanism	Transaction cost
Atomic cross-chain transactions	Exchange of value	Hash and time-locks	Transaction costs on both chains
Sidechains	Transfer of value	Federated functionaries and multiparty signatures, SPV proofs, or validators with hash and time-locks	Sidechains have smaller than main chain
Bridging	Transfer of value	Modules running on one or both of the interconnected chains	Transaction costs on both chains
Ledger-of- ledgers	Transfer of value	Requires an additional interconnection ledger	Transaction costs on yberledger is easily subject to monopoly pricing
ILPv1	Exchange of value and transfer of value	Hash and time-locks	Cost for opening and closing on-chain transaction; Subject to competitive pricing
ILPv4	Exchange of value and transfer of value	Unconditional payment channels, legacy payment systems	as above

Introduction and background

Motivation: Why interledger?

Interledger in practice: an example

Different interledger approaches

Typical use cases

Summary

Typical use cases

- Asset transfer or exchange
- Connecting consortium/private ledgers and public ledgers
- Synchronising two ledgers
- Moving digital collectibles

Asset transfer or exchange

- When one cryptocurrency is changed to another and currencies live in different ledgers

Connecting consortium ledgers and public ledgers

- **Both closed consortium and public ledgers are likely to exist**
  - Need to connect them and exchange information follows
- **For example, periodically updating a state of private ledger to a public ledger to guarantee integrity and auditability**

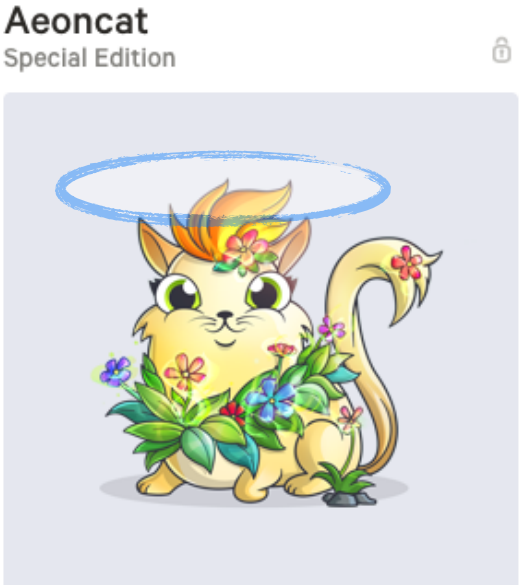
Synchronising two ledgers

- **A case of keeping the corresponding state in two different ledgers**
  - Two different consortium ledgers who want to share some state

Moving digital collectibles

- **Enabling unique digital goods**
  - Outliving the judicial person, who made them
  - New digital markets, which are not necessarily controlled by the market maker
- **Outliving also the ledger!**
  - “Felicus Deus”

01000
01001
01101
10101
01011



Introduction and background

Motivation: Why interledger?

Interledger in practice: an example

Different interledger approaches

Typical use cases

Summary

Summary

- **Interledger is important both for administrative and performance purposes**
- **There are many approaches to interledger**
  - HTLCs are important in a wide range of approaches because they provide atomic exchanges
  - Straightforward ledger-of-ledgers approach is unlikely to work as consensus is typically more difficult to reach administratively than via technology
- **Both public and consortium ledgers are important because confidentiality is important**