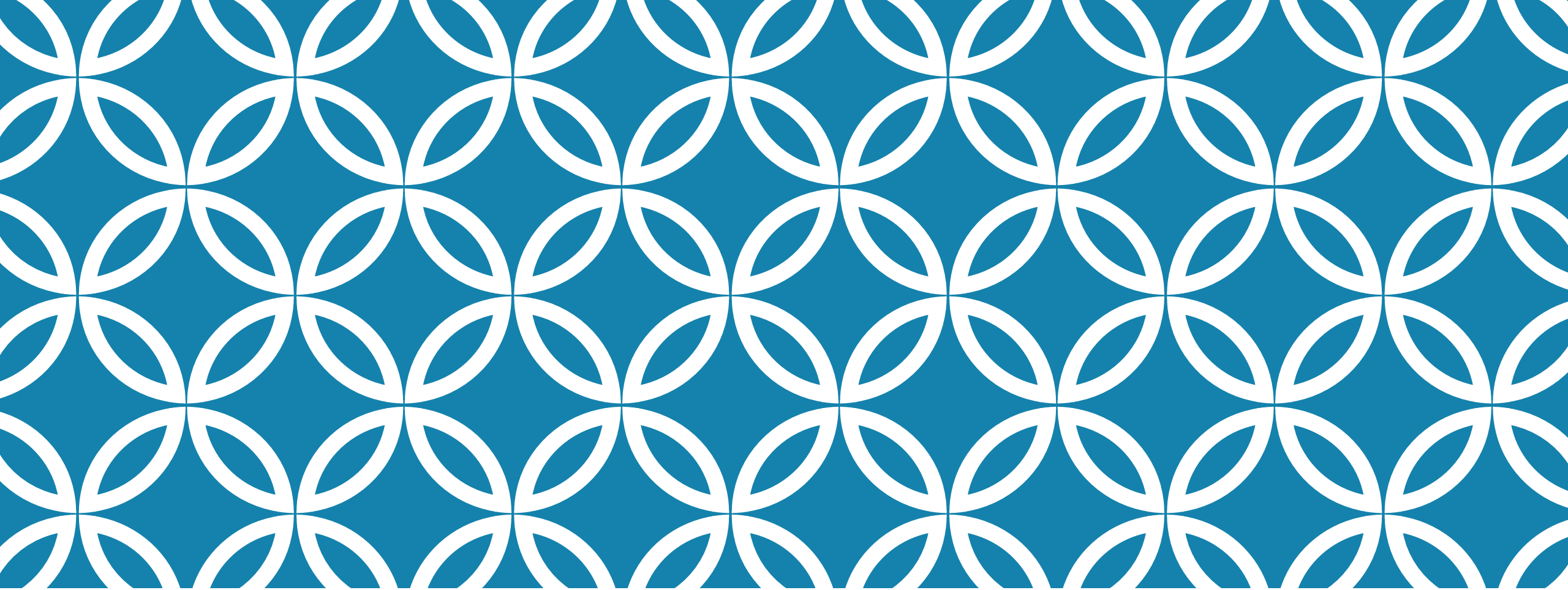


BLOCKCHAIN AND SMART CONTRACTS

Introduction for Software Developers and Architects

WHY BLOCKCHAIN IS A BIG DEAL

“Bitcoin is a technological tour de force.” – Bill Gates

”I think the fact that within the bitcoin universe an algorithm replaces the function of the government …[that] is actually pretty cool.” – Al Gore

“[Bitcoin] is a remarkable cryptographic achievement… The ability to create something which is not duplicable in the digital world has enormous value…Lot’s of people will build businesses on top of that.” – Eric Schmidt

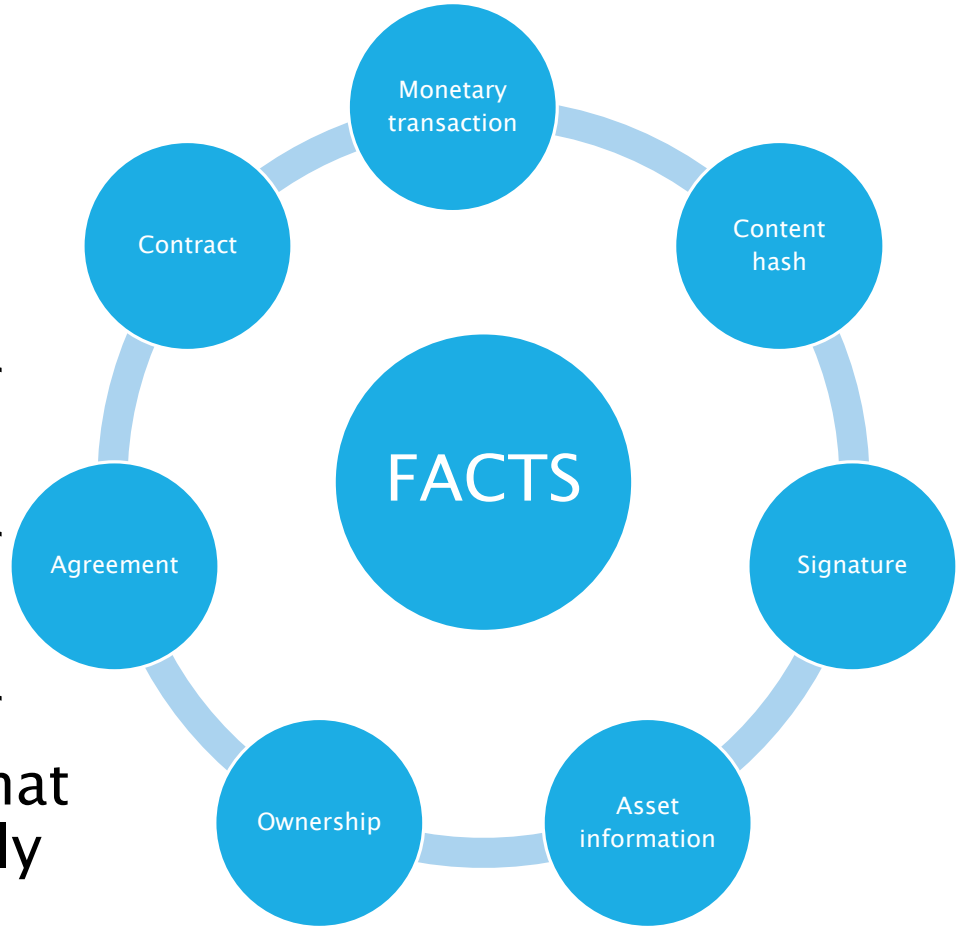
BLOCKCHAIN IS

Ledger of facts

Ledger of facts replicated across large number of computers

Ledger of facts replicated across large number of computers connected as peer-to-peer network

Ledger of facts replicated across large number of computers connected as peer-to-peer network that implements consensus algorithm that can securely identify sender and receiver of facts



IS IT JUST ANOTHER SHARED DATABASE?

NOT JUST ANOTHER DATABASE

Multiple Writers

Non-trusting writers

Disintermediation

Interaction between transactions

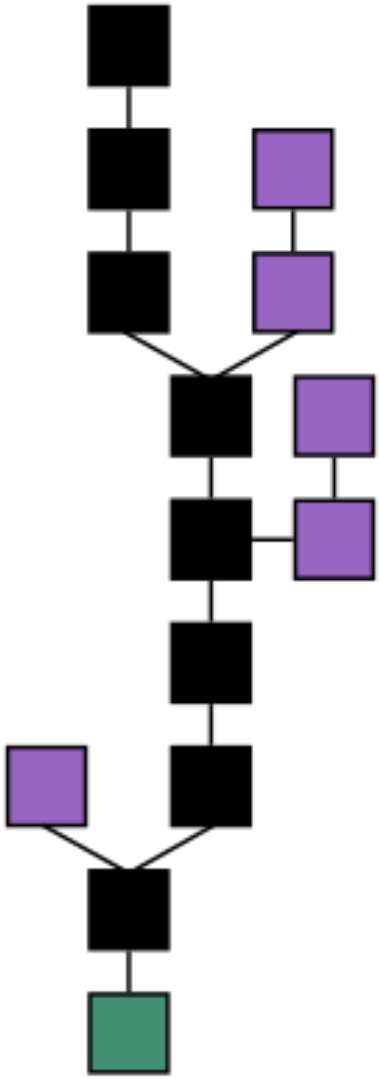
Conflict resolution

HOW?

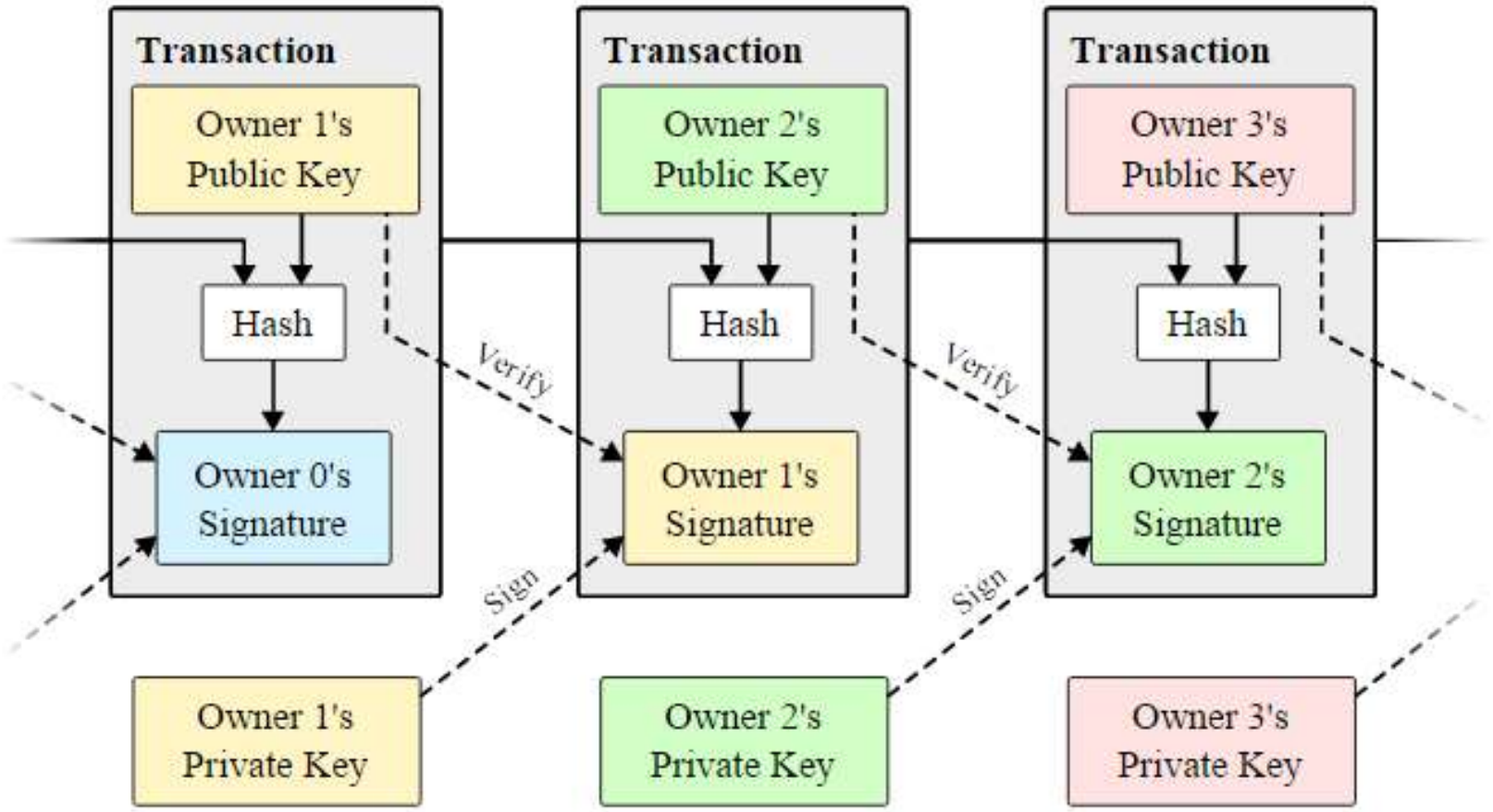
Blocks

Decentralized consensus

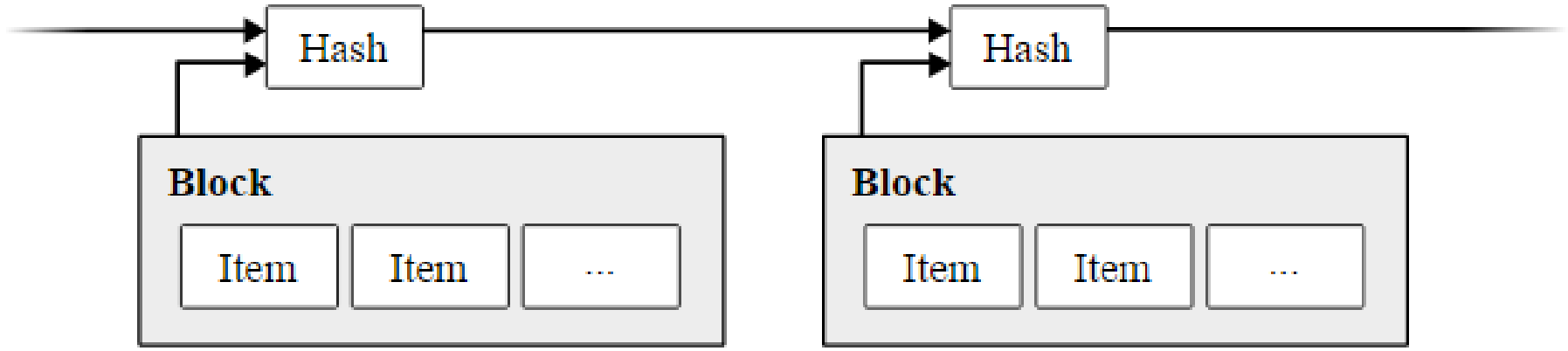
Byzantine fault tolerance.



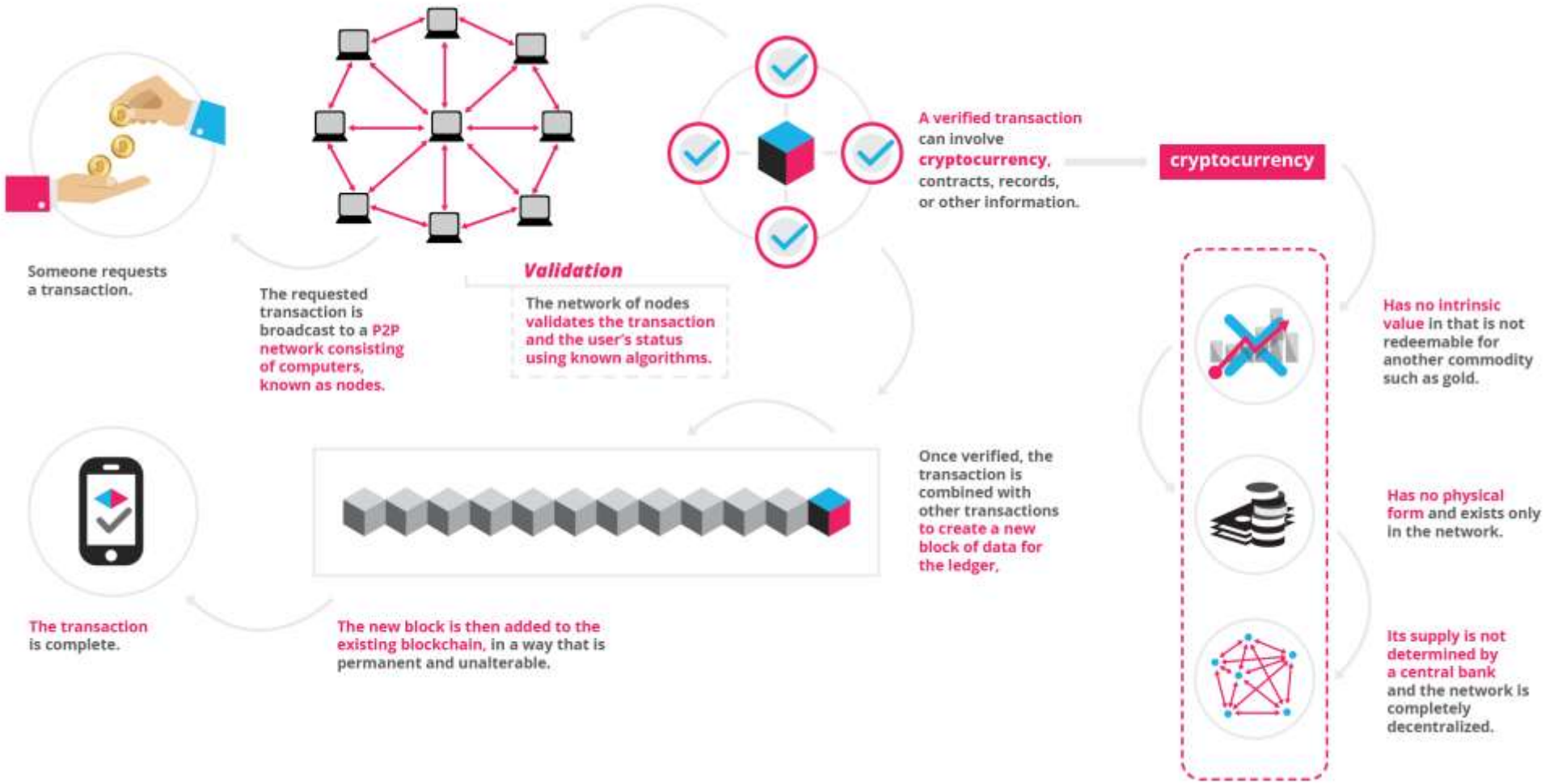
CHAIN OF TRANSACTIONS



TIMESTAMPS



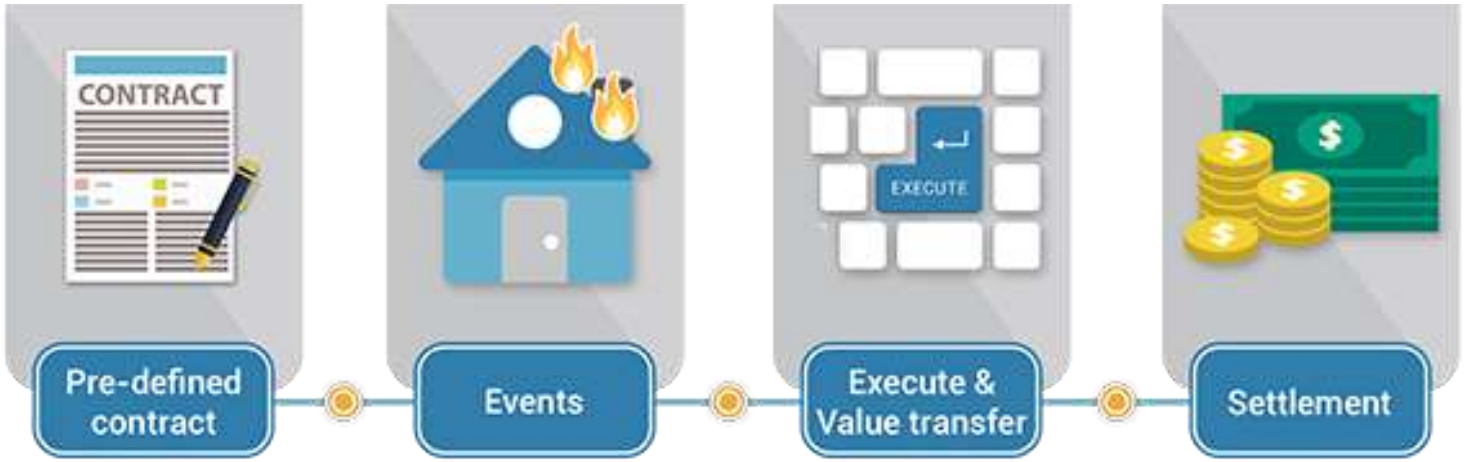
RECORDING TRANSACTION



SMART CONTRACTS

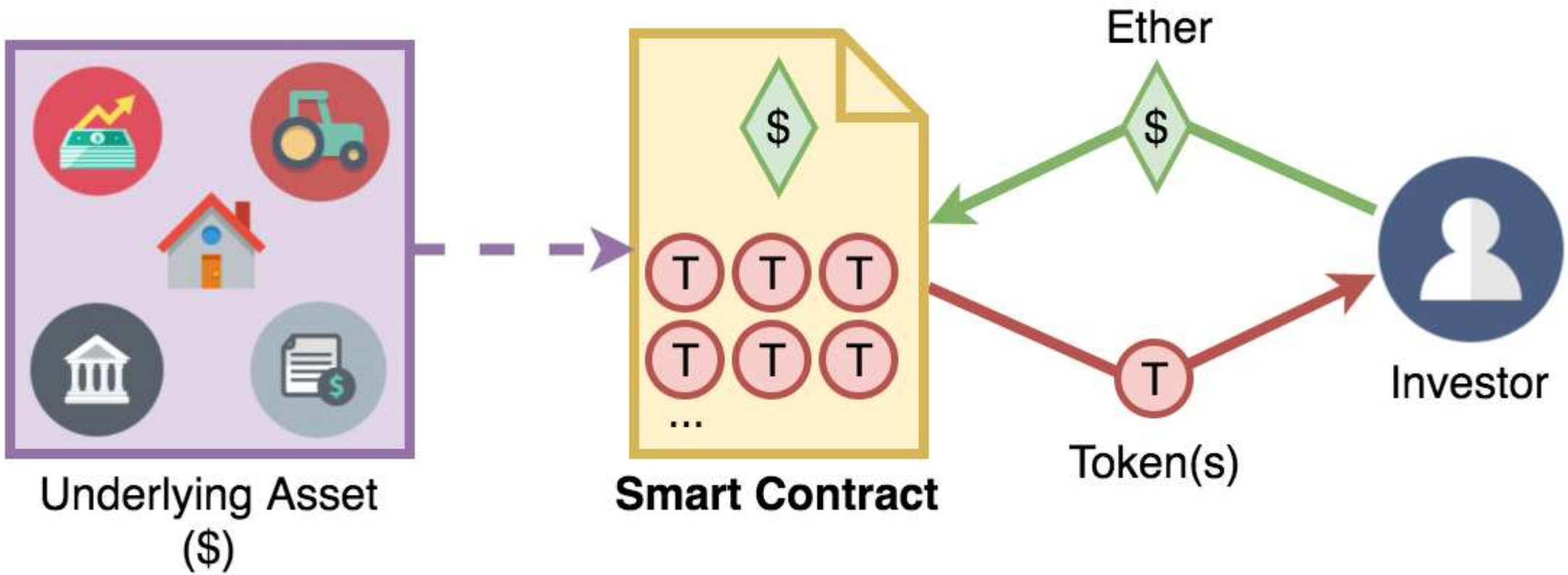
Introduction to Smart Contracts

EXAMPLE OF A CONTRACT



- Terms of the policy are agreed by all counterparties
- These are hard coded into the smart contract and cannot be chan-ged without all parties knowing
- Event triggers insurance policy execution
- The smart contract policy is automatically executed based on the pre-agreed terms
- Payout / other settlement completed instantly and efficiently

EXAMPLE OF SMART CONTRACT

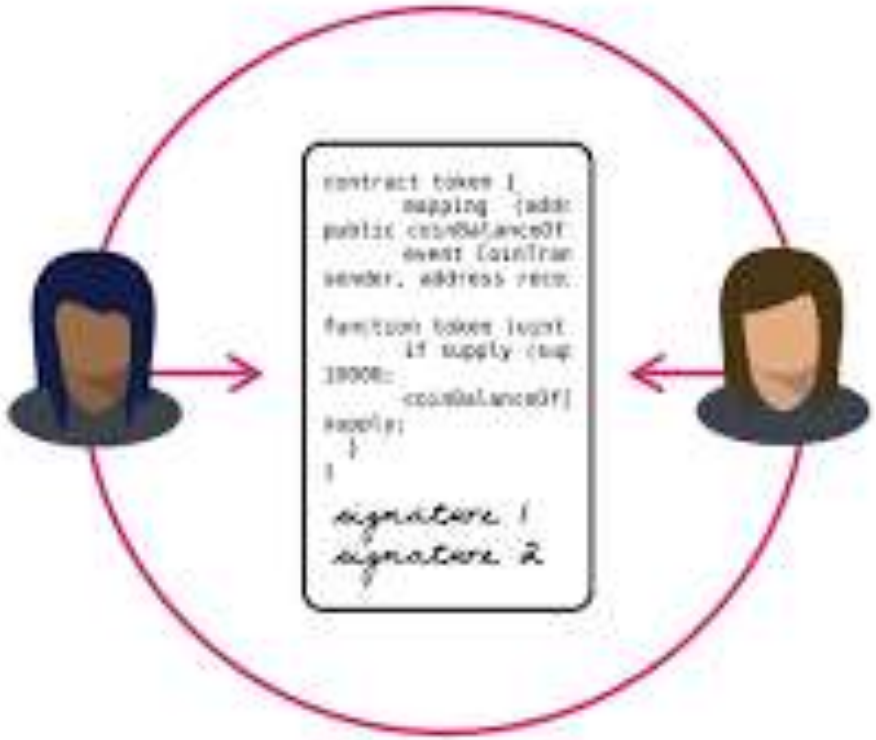


SMART CONTRACT USE CASES

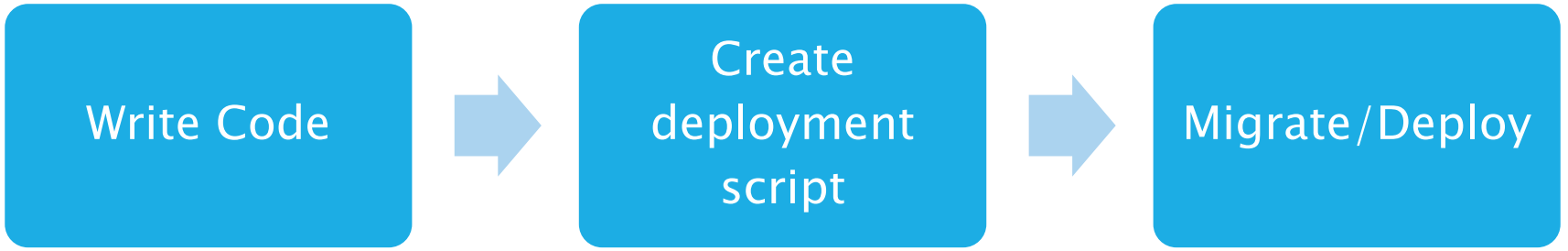
ICO	Digital Identity	Public records
Securities	International trade	Derivatives
Mortgages	Land title	Supply chain

HANDS-ON INTRODUCTION TO SMART CONTRACTS

With Etherium and Solidity



DEVELOPING SMART CONTRACT WITH TRUFFLE



PREREQUISITES

Truffle Framework

- $ sudo npm install -g truffle
- $ mkdir solidity-experiments
- $ cd solidity-experiments/
- $ truffle init

Etherium test network

- $ sudo npm install -g ethereumjs-testrpc
- $ testrpc &

Configure truffle.js

```
module.exports = {
 networks: {
 development: {
 host: "localhost",
 port: 8545,
 network_id: "*" // Match any network id
 }
 }
}
```

HELLO WORLD CONTRACT (SOLIDITY CODE)

```
pragma solidity ^0.4.4;

contract Hello {
  function Hello() public {
    // constructor
  }

  function sayHello() public pure returns
(string) {
      //console.log("sayHello() function
called...");
      return 'Hello World!';
  }
}
```

DEPLOYMENT SCRIPT

```
var Hello1 =
artifacts.require("./Hello.sol");

module.exports =
function(deployer) {
  deployer.deploy(Hello1);
};
```

CONTRACT DEPLOYMENT

```
$ truffle console
truffle(development)>  truffle migrate --reset
Using network 'development'.

Running migration: 1_initial_migration.js
  Deploying Migrations...
  ...
0xb6bbeaaf3649ecb38d548cba96f681682dad9e0225726924fbee3ce36eff94e3
  Migrations: 0xc08c46796ba0edc0bebbbd0d90868c010055cb0e
Saving successful migration to network...
  ...
0x16fe364b9f2c3e8f07fa1ebd6b84b8ad9b4e750d8698a7e920d824ebd019dd80
Saving artifacts...
Running migration: 2_deploy_contracts.js
  Deploying Hello...
  ...
0xfe120836b2d7395bd988104feff018fe352f93555f71003bbf1a64671cca9ba1
  Hello: 0x2b649a87d20ce1ac3b6a0218e911165fa0f095f0
Saving successful migration to network...
  ...
0x1a09073a3b3f7996f3d63a81a99d8cd09198ad7b467f35f7ddc500a4291332b9
Saving artifacts...
truffle(development)>
```

CONTRACT TEST

```
truffle(development)> var he = Hello.at(Hello.address)
Undefined

truffle(development)> he.sayHello()
'Hello World!'
```

STAY IN TOUCH

Gene Leybzon

https://www.linkedin.com/in/leybzon/

https://www.meetup.com/members/9074420/

https://www.Leybzon.com

ANNOUNCEMENTS

Blockchain and Crypto "Unconference" this Sunday 1/28 from 3-5PM in room Z301 at the GSB Stanford