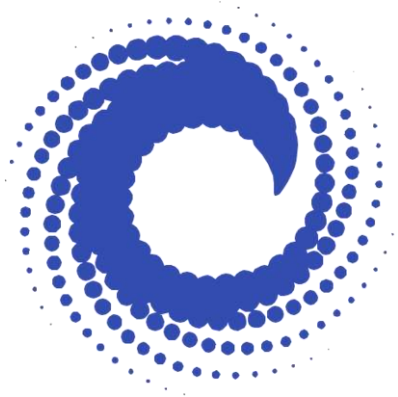
About ConsenSys

Solutions

Consult and deliver production ready blockchain solutions for organizations and governments

Infrastructure

Help grow the ecosystem by building and maintaining core developer tools and clients



Products

Incubate new companies developing decentralized applications on the Ethereum blockchain

Capital

Provides token services, crypto asset management and venture capital

Education

Educate developers and entrepreneurs about Ethereum through training programs

Our Mission

Scalability

Ease of Deployment

Stability

PEGASYS

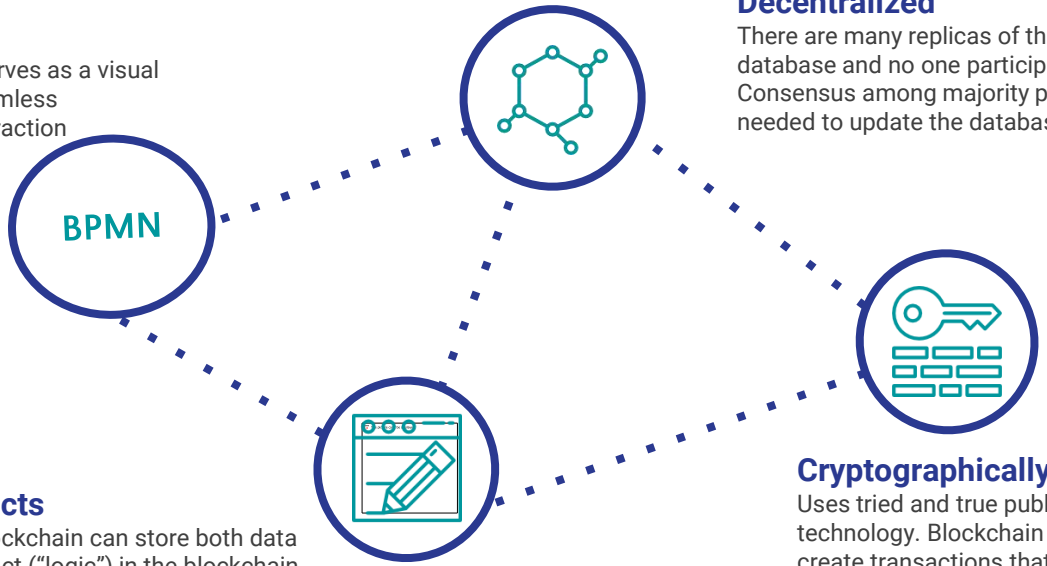
Privacy

Permissioning and Access Control

"Ethereum's intrinsically trusted system is the most promising solution for enterprise Blockchain adoption, given its maturity and multi-purpose design. Privacy and Performance improvements will be mandatory to achieve enterprise-ready status and will be the focus of Enterprise Ethereum's roadmap."

The Tool

BPMN 2.0
The standardized notation serves as a visual component that allows a seamless blockchain adoption and interaction

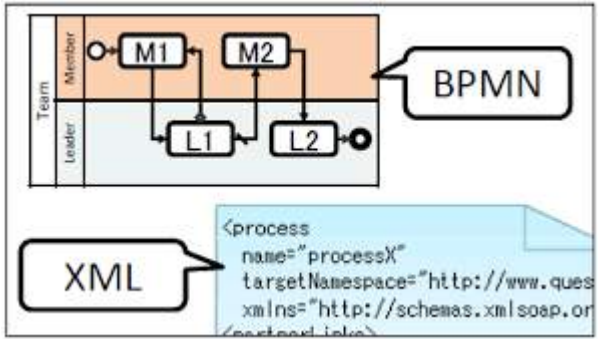


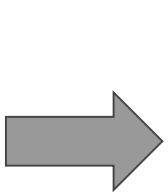
Decentralized
There are many replicas of the blockchain database and no one participant can tamper it. Consensus among majority participants is needed to update the database.

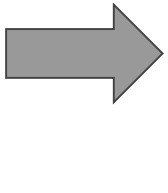
Smart contracts
The Ethereum blockchain can store both data and Smart Contract (“logic”) in the blockchain

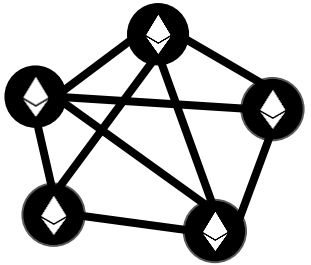
Cryptographically Secure
Uses tried and true public/ private signature technology. Blockchain applies this technology to create transactions that are impervious to fraud and establishes a shared truth.

Automating Ethereum smart contracts generation









Conditions:

- Alice's wants to encrypt values of the products she sales

Result:

- Alice can sell to multiple parties without revealing special pricing for certain customers

```
if (alice.price) => then {
                fhe.balance = fhe.encrypt(price);
}
```

Security, Privacy And Interoperability

Formally specified security and smart contract capabilities

Vendor-neutral

Public – private blockchains compatibility

Private, permissioned blockchains for enterprise and government use cases

Rapidly growing community encompassing 50,000+ developers

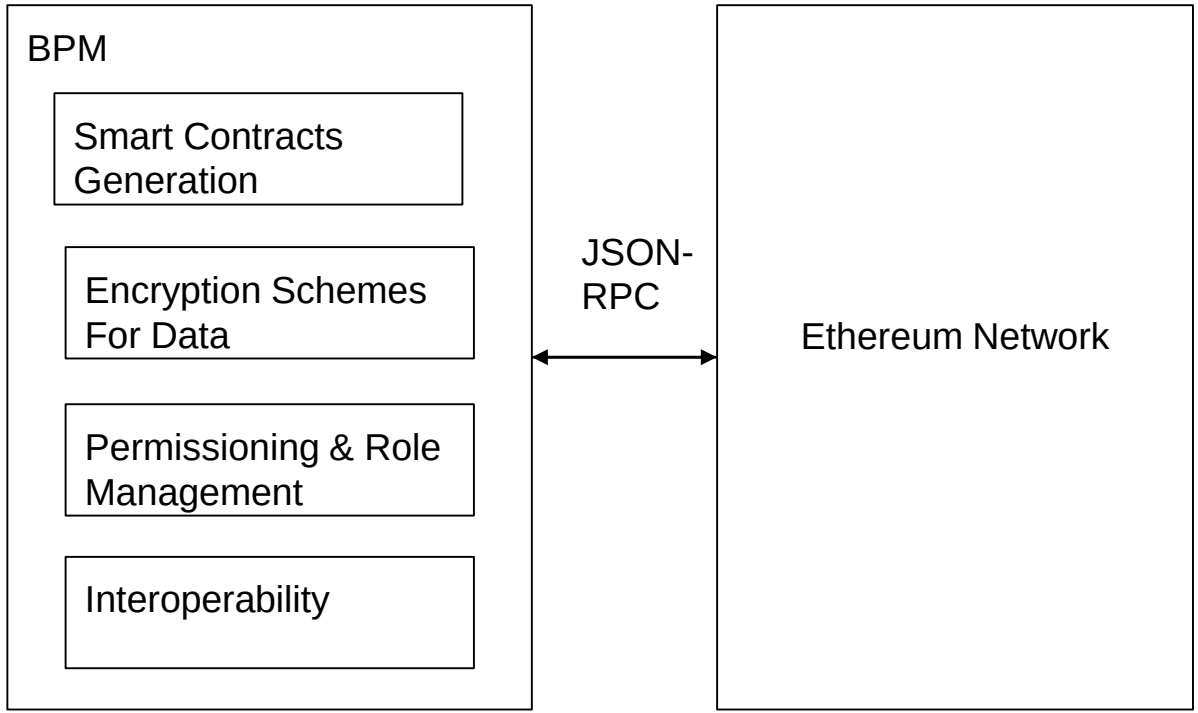
Multi-billion dollars of value protected on the public network

Enterprise Ethereum Alliance (EEA) is growing faster than all other blockchain consortia

The dominant platform for the 'token ecosystem'

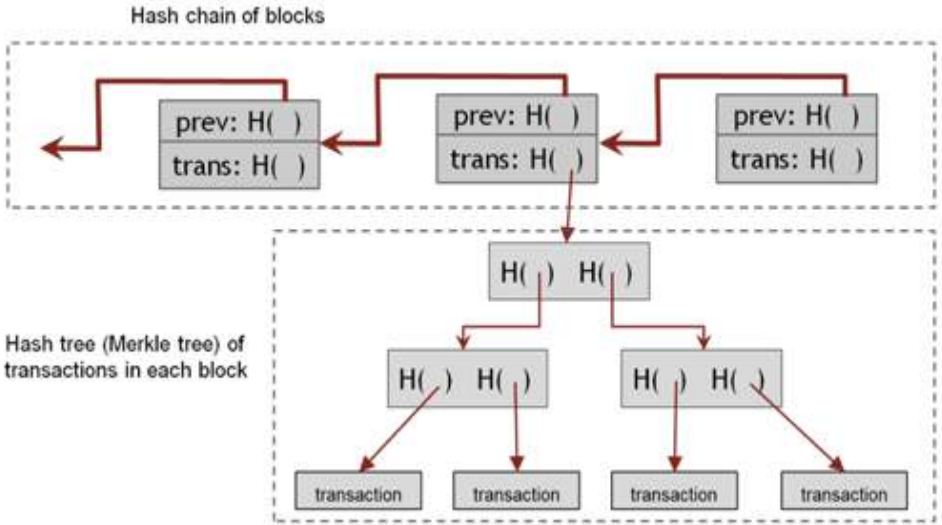
Enterprise Focus

Drive development of ecosystem through alliances and consortia

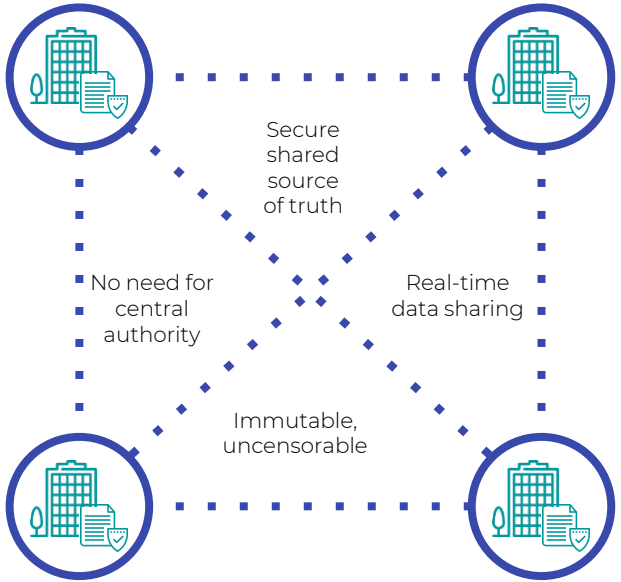


Distributed and disintermediated models

A move toward distribution and disintermediation is a move toward scalability, resilience, efficiency, cost reduction, stability and reliability



Distributed Ledger



Development Process

Create Smart Contract	Create BPMN	Create Unit Test
Create solidity smart contract	Create diagram representing process	Start process
Generate abi and bin files	Define user tasks and script tasks	Create tests for user tasks
Convert to Java class using Web3j	Map functions to process flow	Debug

Privacy & Security Requirements

- **Users**
  Increase visibility and transparency

  Encourage participation

- **Enterprise**

  Provide a privacy layer

  Increase security

  Automate flow

  Reduce burden on smart contracts

- **Research**

  Contribute to the advancement and implementation of crypto schemes

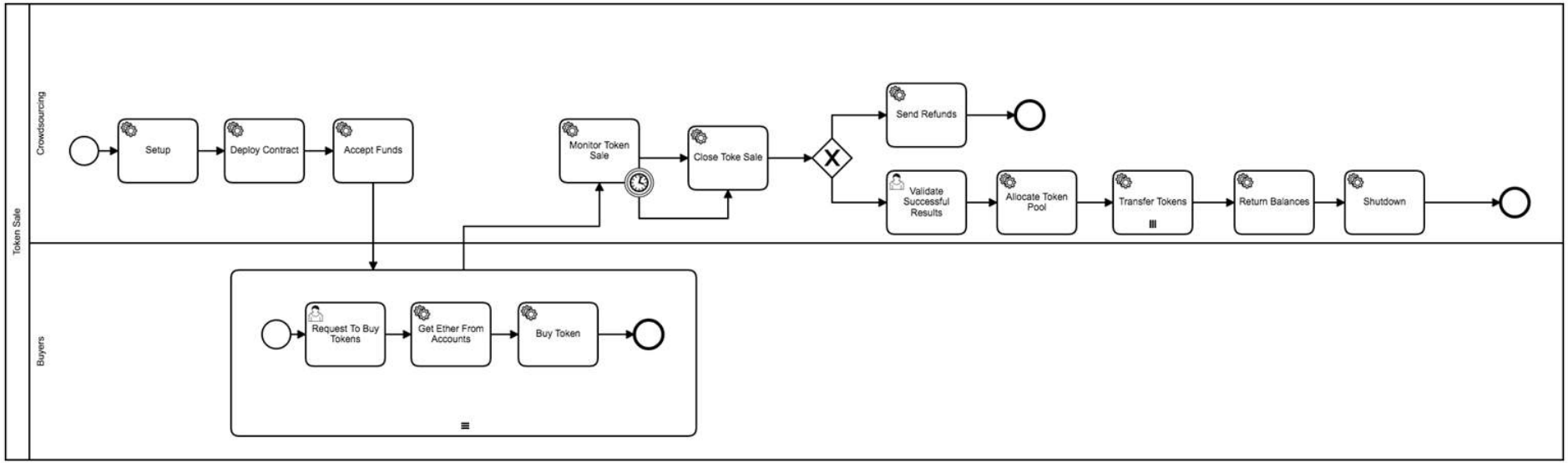
  Create other technologies that facilitate adoption of blockchain in enterprise settings.

Token Sale

A new of Crowdsourcing

A token sale is a transaction between two participants through a smart contract where one party takes money and returns tokens to the buyers.
It’s a mix between and IPO and online crowdfunding.

Token Sale BPMN



Advantages of FHE and other Schemes

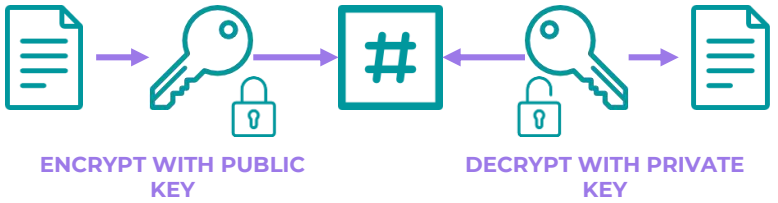
Blockchain technology relies upon well established cryptography

Hashing functions

A one way transform of data into a unique, fixed length digest that cannot be reversed to produce inputs

Public-key cryptography

Enables encryption with a public key that can only be decrypted with a secret, private key and vice versa



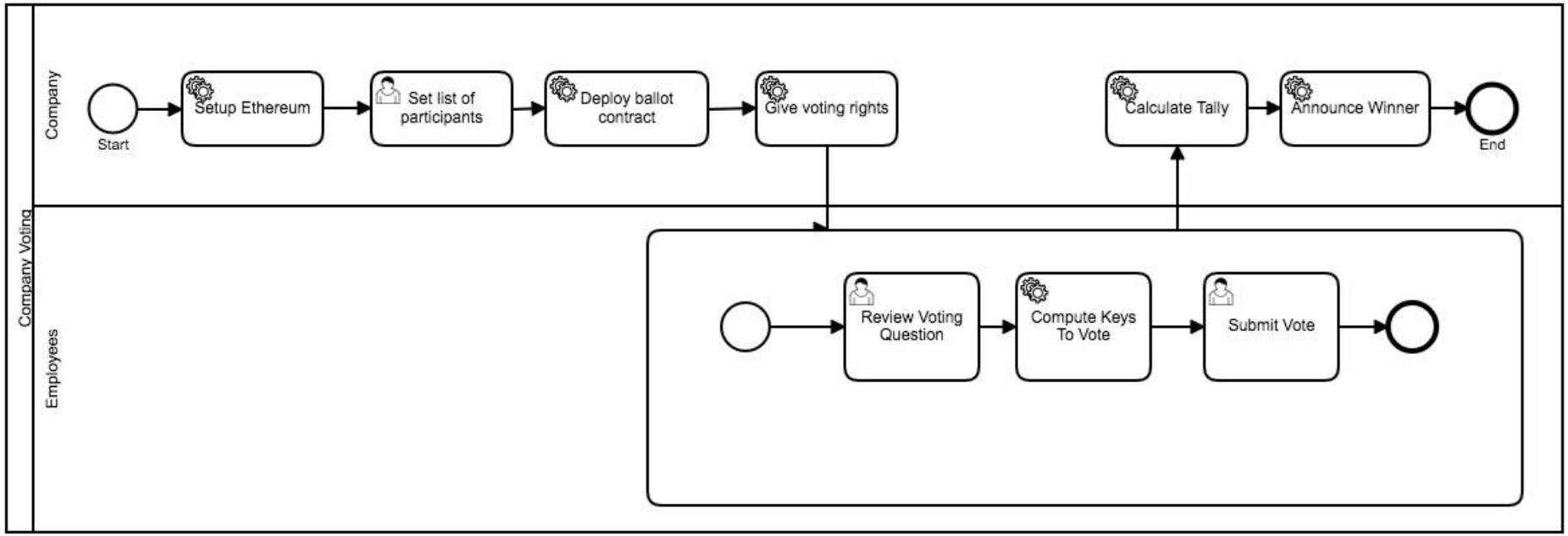
Digital signatures

A mathematical technique used to validate the authenticity, integrity and originator of a message

Homomorphic Encryption

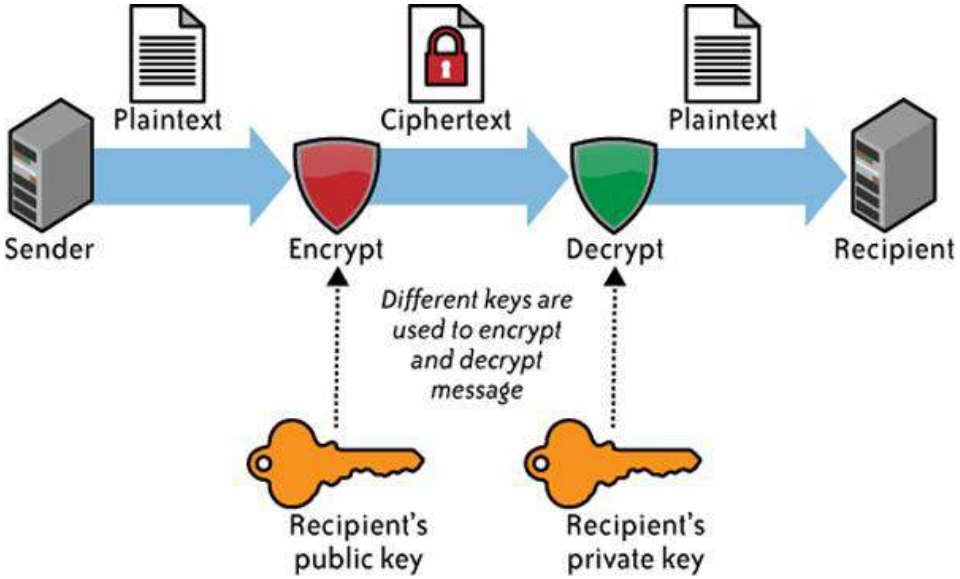
Is a form of **encryption** that allows computation on ciphertexts, generating an **encrypted** result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext.

Anonymous Voting



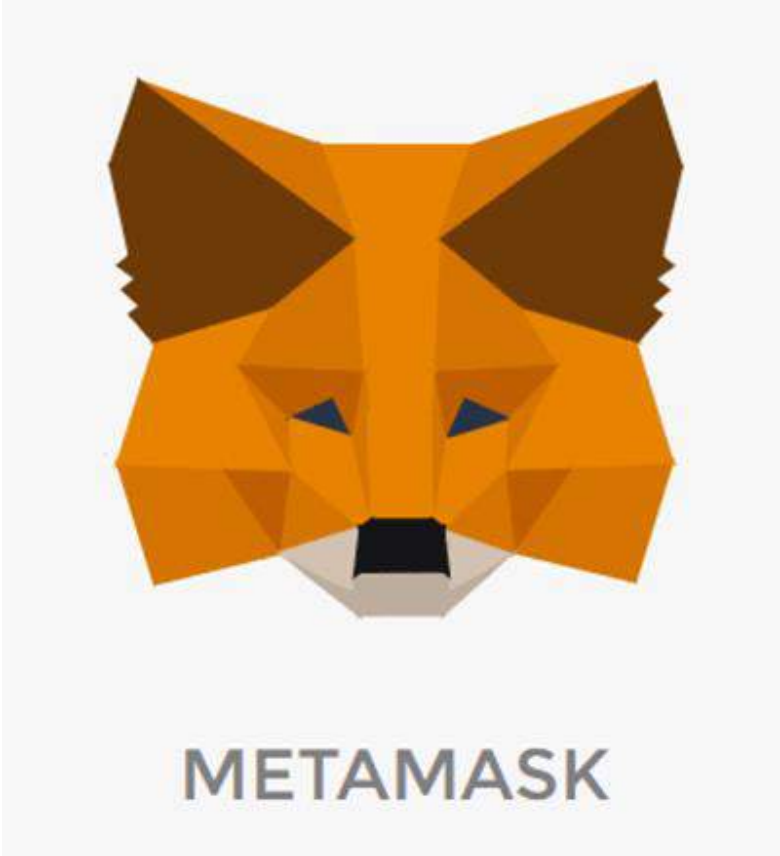
ZKP or Zero Knowledge Proof

- is a way of doing authentication where no passwords are exchanged.
- No information is revealed but rather proofs that the information is correct are used to verify results.



Roles and Permissions

- Users will be able to login through Metamask a Consensys project that allows you to visit the distributed web of tomorrow in your browser today.
- Their roles and permissions would then be verified through contracts for authorization and authentication.



Blockchain & BPMN

Advantages of the Blockchain

- Peer to peer payment system
- Programmable logic through smart contracts
- Increase visibility
- User empowerment

Advantages of BPMN

- Visual tool
- Automated Process
- Timers
- Currently used by many businesses

Limitations With Current Contracts

The cost and size of contracts can increase as more complex uses arise.

- Our goal is to automate this as much as possible by using BPM tooling.

Contracts get bulky and unnecessarily large when dealing with things as time management.

```
// Election Authority dictates that the sign up period has begun.
function beginSignUp(bool commitment, uint finishSignup, uint endSignup, uint endComputation,
    uint endCommitment, uint endVoting, uint endRefund, uint deposit) {
    string memory question = "Should Satoshi Nakamoto reveal his real identity?";

    setEligible();
    con.beginSignUp(question, commitment, finishSignup, endSignup, endComputation,
        endCommitment, endVoting, endRefund, deposit);
}

// Easy function to begin election without commitment
function beginSignupWithoutCommitment() {
    uint gap = con.gap();
    uint multiplier = con.refundgapmultiplier();
    uint finishSignup = 2;
    uint endSignup = finishSignup + gap;
    uint endComputation = endSignup + gap;
    uint endVoting = endComputation + gap;
    uint endRefund = endVoting + (gap*multiplier);
    string memory question = "Should Satoshi Nakamoto reveal his real identity?";
    con.beginSignUp(question, false, finishSignup, endSignup,
        endComputation, 0, endVoting, endRefund, 0);
}

// Easy function to begin election with commitment
function beginSignupWithCommitment() {
    uint gap = con.gap();
    uint multiplier = con.refundgapmultiplier();
    uint finishSignup = 2;
    uint endSignup = finishSignup + gap;
    uint endComputation = endSignup + gap;
    uint endCommitment = endComputation + gap;
    uint endVoting = endCommitment + gap;
    uint endRefund = endVoting + (gap*multiplier);
    string memory question = "Should Satoshi Nakamoto reveal his real identity?";
    con.beginSignUp(question, true, finishSignup, endSignup,
        endComputation, endCommitment, endVoting, endRefund, 0);
}
```

Complimenting with BPMN

As with any emerging technology, limitations to the adoption of blockchain still exist but a talented and enthusiastic community is actively working to overcome such obstacles

Integration

There is limited interoperability and integration between different protocols and legacy systems.
By incorporating BPMN new systems as well as legacy systems can be connected.

Latency

Current transaction speed and latency represent a limit to adoption for some use cases.
By removing complexity from smart contracts into business processes user adoption can be increased.

Privacy

Pseudonymity doesn't satisfy the privacy requirements for many use cases.
There is a need to increase control over data, and access in the blockchain which can be achieve through different layers.

New Projects

Stronger cooperative economy

Disintermediate non value added activities to strengthen the participant's participation in the economy and their ability to capture value.

Social enterprise

The ability to trace transactions and set up organizations and voting mechanisms linked to reputation and identity will provide for the ability to recognize and report corruption. Immutable reputation will also incentivize best behavior.

New governance models

Ability for blockchain to organize and help in the delivery of projects through real time voting, which will have greater consequences when applied to liquid democracies, and prediction markets.

Accessible financial services

Bringing financial services to the billions of unbanked through near zero transaction fees and east of micropayments.

Future Uses