DAYANANDA SAGAR COLLEGE OF ENGINEERING

DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

DSCE

DEPARTMENT OF INFORMATION SCIENCE

BLOCKCHAIN
(19IS7DEBLC)

Faculty in charge:

Bindu Bhargavi S M
Asst. Professor, Dept. of ISE, DSCE

Module 3

- **Smart Contracts:** History, Definition, Ricardian Contracts, - Smart Contract templates, Oracles, Smart Oracles, Deploying smart contracts on a BC. The DAO

SMART CONTRACTS

- Smart contracts are digital contracts stored on a blockchain that are automatically executed when predetermined terms and conditions are met
- They are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary’s involvement or time loss

Working of Smart Contracts

- Works on “if/when…..then” basis
- A network of computers executes the actions when predetermined conditions have been met and verified.
- Ex: releasing funds, sending notifications, issuing a ticket
- Blockchain is updated once the transaction is complete – transactions cannot be changed
- Parties involved in the transaction can only see the results

Benefits of Smart Contracts

- Speed, efficiency and accuracy
  - Once conditions are met, contract is executed immediately
  - Digital and automated
- Trust and Transparency
  - No involvement of third party
  - Sharing encrypted records of transactions
- Security
  - Blockchain transaction records are encrypted
  - Use of distributed ledgers
- Savings
  - They remove the need for intermediaries to handle the transactions

Applications of Smart Contracts

- Safeguarding the efficacy of medications
- Increasing trust in retailer-supplier relationship
- Making international trade faster and more efficient.

- A smart contract is an electronic transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries
- A smart contract is a secure and unstoppable computer program representing an agreement that is automatically executable and enforceable.
- Should be fault tolerant and executable in reasonable amount of time.

- Computer Program – written in language which is understandable by the target machine
- Agreement – business logic
- Automatically executable when certain conditions are met
- Enforceable - all contractual terms are executed as defined and expected
- Secure and unstoppable – designed such that they are fault tolerant and executable in reasonable amount of time.
- Architecture followed for a smart contract – state machine model
- smart contracts ensures that smart contracts produce same output every time they are executed – consistent consensus requirement – more deterministic – thereby ensuring integrity and stability
- Use of Legal Knowledge Interchange Format (LKIF) – XML schema

- **Properties of Smart contracts**
  - Automatically executable
  - Enforceable
    - No need of an arbitrator or a third party to control the execution of the smart contract
  - Semantically sound
  - Secure and unstoppable

Ricardian Contracts

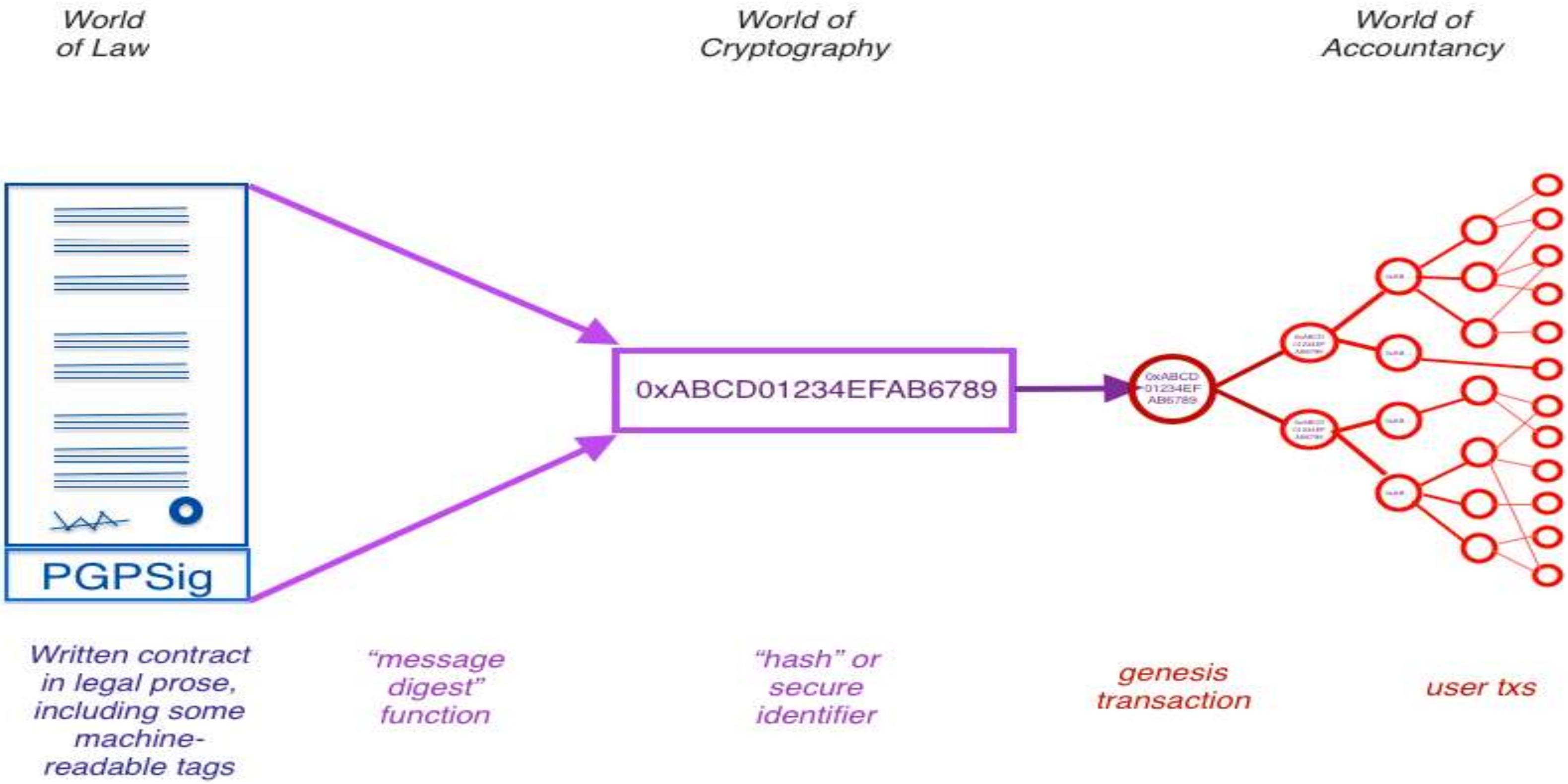
- Used initially in trading and payment system called Ricardo - write a document that is understandable and acceptable by both a court of law and computer software
- Ricardian Contract is a method of recording a document as a contract at law, and linking it securely to other systems - human-readable legal contract between the two parties

- Properties are:
  - A contract offered by an issuer to holders
  - A valuable right held by holders and managed by the issuer
  - Easily readable by people (like a contract on paper)
  - Readable by programs (parsable, like a database)
  - Digitally signed
  - Carries the keys and server information
  - Allied with a unique and secure identifier

- How does a smart contract work
    - Produce a single document containing the terms of contract – legal prose and machine readable tags
    - Digitally signed by the issuer using their private key
    - Hash the document using a message digest function – produce the hash used for identification of the document
    - The same hash is further used and signed by the parties – used to link each transaction

The Ricardian Contract

the BowTie Model



World of Law

World of Cryptography

World of Accountancy

PGPSig

0xABCD01234EFAB6789

Written contract in legal prose, including some machine-readable tags

"message digest" function

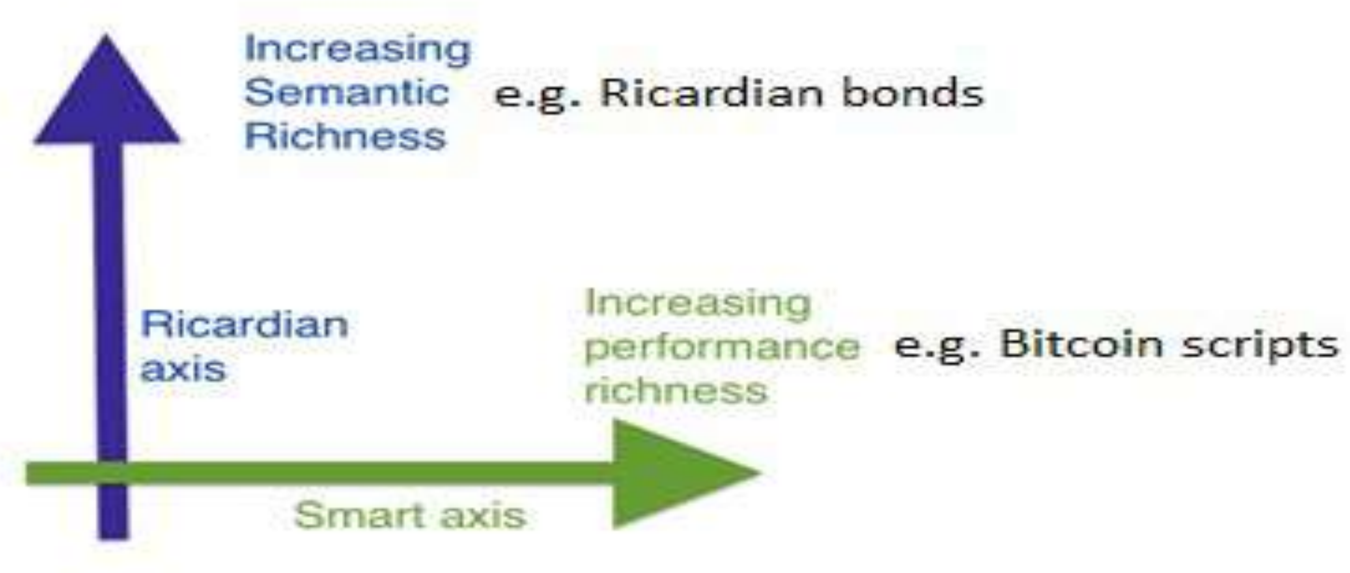
"hash" or secure identifier

genesis transaction

user txs

Ricardian Contracts

- Semantic richness, documents containing contractual legal prose.
- Semantics – operational semantics and denotational sematics
- Operational semantics – actual execution, correctness and safety of the contract
- Denotational semantics - real-world meaning of the full contract.
- Ricardian contract – three tuple object – prose, parameter and code
  - Prose – legal contract in natural language
  - Code – computer understandable representation of legal prose
  - Paramrter – joins the contract to a code

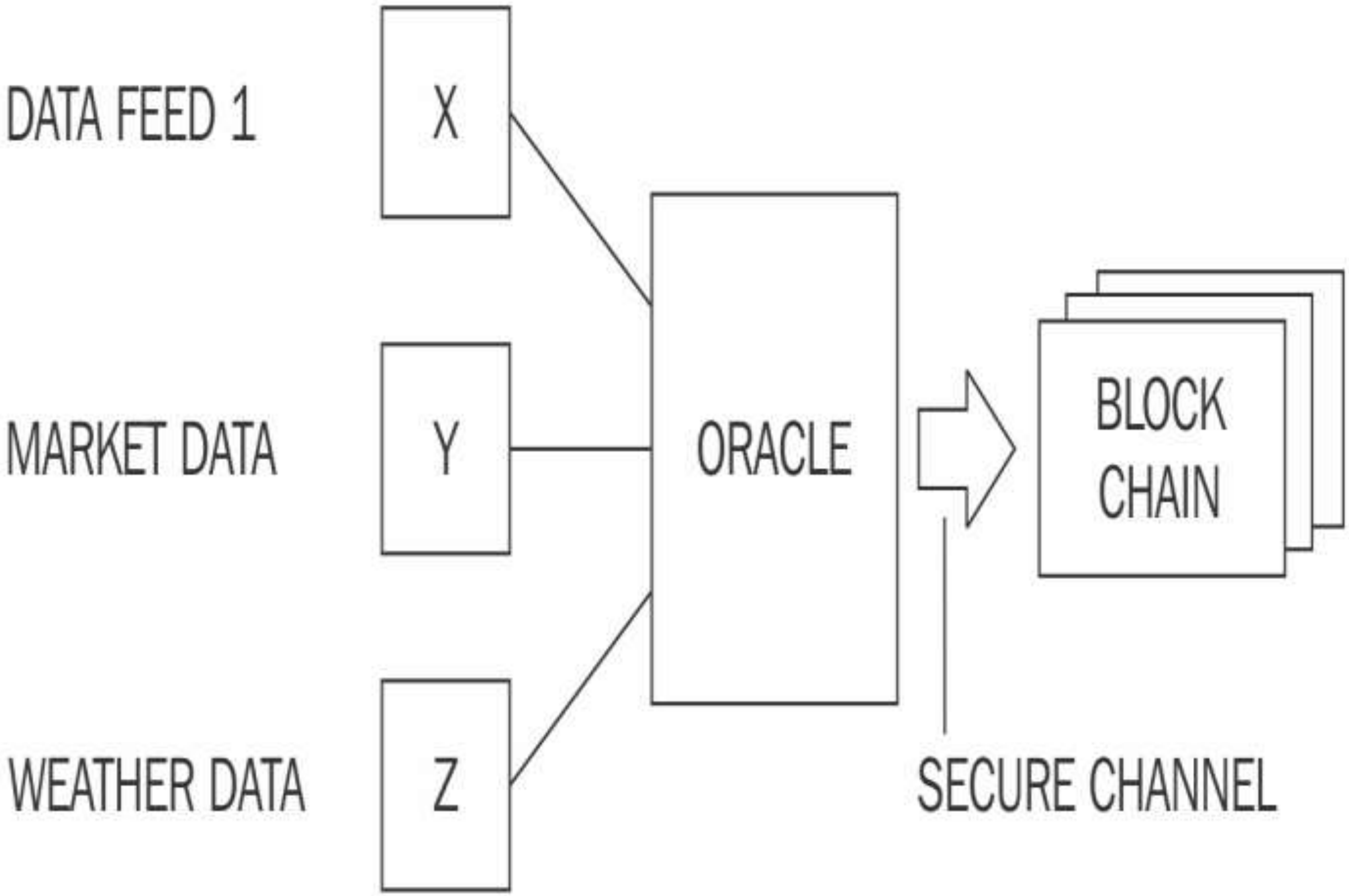


Smart contract templates

- Implemented majorly in financial industries
- Use of Domain specific languages
- CLACK - common language for augmented contract knowledge
  - supporting legal prose
  - executed on multiple platforms and cryptographic functions
- DSL – Solidity, Vyper

Oracles

- An Oracle is an interface that delivers data from an external source to smart contracts
- Oracles are trusted entities that use a secure channel to transfer data to a smart contract
- Oracles are capable of digitally signing the data proving that the source of the data is authentic
- Oracles should not be able to manipulate the data they provide and must be able to provide authentic data
- Decentralized oracles
- Hardware oracles – antitampering mechanism


DATA FEED 1
X
MARKET DATA
Y
WEATHER DATA
Z
ORACLE
BLOCK
CHAIN
SECURE CHANNEL

Deploying Smart Contracts on Blockchain

- Decentralized Autonomous organization (DAO) - A decentralized autonomous organization (DAO) is an entity with no central leadership
- Use of timelocks to enable the transactions to be locked until a specified time/ until a number of blocks
- Timelock used is nLocktime, CHECKLOCKTIMEVERIFY, CHECKSEQUENCEVERIFY

- Requirements of a smart contract:
  - Determinism
  - Bug free
  - Validation and verification
  - Platforms supported – Monax, Lisk, Counterparty, Stellar, Hyperledger fabric, Corda, Axoni core.
  - Language Support – Solidity requires EVM (Ethereum Virtual Machine), Lisk supports JavaScript, Hyperledger fabric supports Golang, Java, JavaScript.

Working of DAO

- A DAO, or “Decentralized Autonomous Organization,” is a community-led entity with no central authority.
- It is fully autonomous and transparent: smart **contracts lay the foundational rules, execute the agreed upon decisions**, and at any point, proposals, voting, and even the very code itself can be publicly audited.

DAO	A traditional organisation
Usually flat, and fully democratized.	Usually hierarchical.
Voting required by members for any changes to be implemented.	Depending on structure, changes can be demanded from a sole party, or voting may be offered.
Votes tallied, and outcome implemented automatically without trusted intermediary.	If voting allowed, votes are tallied internally, and outcome of voting must be handled manually.
Services offered are handled automatically in a decentralized manner (for example distribution of philanthropic funds).	Requires human handling, or centrally controlled automation, prone to manipulation.
All activity is transparent and fully public.	Activity is typically private, and limited to the public.

- **Ethereum and DAOs**
  - Ethereum’s own consensus is distributed and established enough for organizations to trust the network.
  - Smart contract code can’t be modified once live, even by its owners. This allows the DAO to run by the rules it was programmed with.
  - Smart contracts can send/receive funds. Without this you'd need a trusted intermediary to manage group funds.
  - The Ethereum community has proven to be more collaborative than competitive, allowing for best practices and support systems to emerge quickly.

The DAO

- The DAO was an organization created by developers to automate decisions and facilitate cryptocurrency transactions.
- Automated and decentralized in nature, based on a open source code, without a typical management structure or board of directors
- Main aim was to eliminate the human error or manipulation of the investor funds – decision making by automated systems and a crowdsourced process

The DAO Controversy: The Case for a New Species of Corporate Governance?

- There are no trusted human executives since the organization is governed and operated by smart contracts, hence trust is “alienated” from the organization
- The smart contracts which form their governance are written and executed as computer code
- Monitoring and enforcement of smart contracts are likewise by computer algorithms
- There are weak or non-existent mechanisms for dispute resolution, since the “code is law,” and all participants have agreed in advance to abide by the code of the smart contract(s)

- Link: https://www.frontiersin.org/articles/10.3389/fbloc.2020.00025/full