WORLDQUANT UNIVERSITY

**Submission Number: 3** **Submission Date: 08/02/2022**

**Group Number: 05**

**Group Members:**

| **Full Legal Name** | **Location (Country)** | **E-Mail Address** | **Non-Contributing Member (X)** |
|---|---|---|---|
| Werner Vermeulen | South Africa | Masters.wqu@gmail.com | |
| Bence Marton | Hungary | bencemartonur@gmail.com | |
| Raghav Duseja | India | raghavduseja@gmail.com | |
| | | | |

**Statement of integrity:** By typing the names of all group members in the text box below, you confirm that the assignment submitted is original work produced by the group (*excluding any non-contributing members identified with an "X" above*).

Werner Vermeulen, Bence Marton, Raghav Duseja

Use the box below to explain any attempts to reach out to a non-contributing member. Type (N/A) if all members contributed.

** Note, you may be required to provide proof of your outreach to non-contributing members upon request.*

1. Describe smart contracts.

Smart contracts in theory was created in the 1990s by Nick Szabo, who described it back then as *"A smart contract objectives are to satisfy common contractual conditions, minimize exceptions both malicious and accidental and minimize the need for trusted intermediaries"*. The first functional smart contact was implemented in Bitcoin in 2009, with a limited function. There are several definitions exist for smart contract, the best we found is *"A smart contract is a secure and unstoppable computer program representing an agreement that is automatically executable and enforceable"*. Basically a smart contract is a computer program, which another computer can understand and in its code it includes agreement between parties, which can be executed automatically when certain conditions are met. Smart contracts do not need any outside enforcements to be executed; they usually use the "code is the law" principle, this also means that they are self-enforcing. Furthermore they are pretty much unstoppable and very safe, even under unfavorable conditions for example if a smart contract running in an environment which differ from the normal or expected state unlike other programs smart contracts are immune to these kind of issues. Although one should not be fooled by the name smart contract, as the contracts are not smart, but they do exactly as they are programmed. This is one of the main features of smart contracts, they provide the same output every time, and consistency is very important in block chain networks.

Summary of the features of a smart contract:

- Automatically executable: It executes without any outside intervention.
- Enforceable: all the conditions of a contract are automatically enforced.
- Secure: Very hard to hack and tamper with the system, it runs with guarantees.
- Deterministic: Same output for a specific output.
- Semantically sound: Can be interpreted both by computers and humans.
- Unstoppable: Unfavorable conditions cannot affect badly the contract.

We should consider the first four features as the minimum for smart contracts, the last two not necessary to deploy smart contracts.

2. Explain how smart contracts function and achieve this functionality (in the Ethereum network)

Once we create and deploy a smart contract, as per its configuration it will listen to any updates from a so called "oracle", this is a streaming data source which is cryptographically secured. Oracles send the right events and messages to smart contracts which execute the code based on the event.

Oracles are necessary as blockchains are closed systems, however time to time updates might be necessary to reach the chain, thus the oracles.

The way oracles work in the Ethereum network:

1. Smart contract requests data from an oracle.
2. The data then is requested from the source. Several methods exists for example data provided by APIs or data requested by another blockchain.
3. Data is forwarded to a notary and there a cryptographic proof is generated in order to validate the request. There are also more than one way to do this one common is TLSNotary.
4. Proof of validity along with the data is forwarded to the oracle.
5. The data and its proof are saved on a decentralized storage system.
6. Proof of validity along with the data is forwarded to the smart contract.

Regarding proof of validity or proof of authenticity, in order to prove that the data is authentic, oracles perform digital signatures and validation of the data. Basically, smart contracts are subscribed to oracles and then they exchange data between each other, by pulling and pushing the data.

In terms of oracles, it is very important that these are not able to manipulate or change anything in the data, and for this porpoise several cryptographic proofing schemes exists, such as TLSNotary or hardware device-assisted proof, ledger proof etc.

## 3. Advantages

- **Clarity:** Smart contracts eliminate ambiguity and increase accuracy by ensuring a clear/equal understanding of the terms of agreement between the two parties, thereby serving as an efficient way of automating plain vanilla contracts.
- **Trust:** Parties to a smart-contract can carry out their legal commitments without the necessity for any interpersonal trust with their counterparties.
- **Costs:** Reduce legal costs. These include system transaction costs (for countries where the legal system is not as developed) and contract transaction costs (where it is expensive to enter and enforce a contract)[i]
- **Intermediaries:** Smart contracts can substantially reduce the number of intermediaries required for business transactions, for eg. an escrow agent/bank is no longer required if the transaction is routed through a smart contract which automatically holds the payment until the payment conditions are met.[ii]
- **Legal validity:** Most smart contracts, like regular contracts, will have legal sanctity as long as they meet the basic requirements of a contract, namely, offer – acceptance – consideration.
- **CBDCs:** In the far-off future, if combined with CBDCs (Central bank digital currencies), smart contracts have the potential to reduce transaction float for Central Banks as well help them in maneuvering monetary policy.[iii]

## 4.Disadvantages

- **Handling Complexity:** Most agreements in the real world are complex and are not amenable to being routed through smart contracts. Smart contracts only work when possibilities are small and narrow.

  For eg, it will be possible to have a smart contract for the payment and delivery of a product, but it may be difficult to ensure through the smart-contract that the quality of the product is also upto the mark (as gathering evidence about the quality is way more expensive than gathering evidence of delivery).
- **Language:** Converting legal language to code is a cumbersome process and includes the development and maintenance of languages and devices such as CTL (Computation tree logic) and LTL (Linear temporal logic)[iv].
- **Code review and formal verification:** While smart contracts reduce the dependency on lawyers, they now create dependency on professionals such as “smart-contract security auditors” who will verify, review and test the smart contracts for their code and their logic. This has become essential due to the numerous cases of large amounts being stolen through smart-contract hacks.

- **Human judgement:** Often used legal terms like “reasonable” and “fair use” require human judgement and may not flow seamlessly through a coded and automated system which doesn’t understand the broader context.
- **On-chain only:** Only agreements and transactions on the blockchain can be routed through smart-contracts, so use cases are limited unless blockchains in general are widely accepted across sectors and counterparties.
  This problem is partly resolved by usage of Oracles, for eg. when a vanilla smart-contract (on-chain) can form part of a larger more complex set of agreements (off-chain).
- **Enforceability:** A smart contract cannot exist in a vacuum, it does not merely exist between two parties. It has to comply with the law of the land to be legally binding and enforceable. For eg, there may be limits to the interest rate which is allowed to be charged in a country and the smart contract, if it allows for a rate greater than what is allowed, will be considered invalid and unenforceable.
- **Privacy:** As smart-contracts need transparency in payments (through a decentralised ledger), privacy may be a concern in many cases.

5. Identify and describe one appropriate use-case for smart contracts.

**Financial services:**

Financial services can precisely record financial data using smart contracts. Multiple smart contract use cases can be used to manage mortgages, capitalization table management, payments, and settlements, property ownership, insurance and prediction markets.

- For mortgages, smart contracts can automate payment processing and release liens after the loans are paid. Also, smart contracts can enhance the visibility of mortgage records and simplify payment tracking.
- Smart contracts can streamline capitalization table management by circumventing the need for intermediaries in the chain of custody and automating the payment of dividends.

Bank runs can be a complicated issue for various banks. Bank runs usually occur if depositors feel that their bank may be unable to cover their deposits. To tackle this problem, banks can utilize smart contracts to allow depositors and shareholders to view a bank’s lending and reserves within specified parameters. Also, smart contracts can simplify regulatory compliance as necessary documents can be securely stored and shared with the concerned parties effortlessly.

**Property ownership management in financial services.**

Smart contracts can be utilized to transfer the ownership of property. Smart contracts can record ownership rights and verify the identity of every owner. This approach can be especially useful for cross-border purchases, where time-consuming negotiations, tedious documentation, and complicated bureaucratic procedures can be avoided. Smart contracts can also be used for proving intellectual property ownership. Artists can preserve the proof of ownership for their work and protect it from theft and illegal use. Property owners and artists can choose their own terms and conditions for fair use of their work. Also, smart contracts can ensure that artists receive a royalty whenever anyone uses their work. Thus, with smart contracts, artists can reduce the impact of piracy.

**Insurance in financial services.**

Insurance claims processing can be a time-consuming and complex procedure that may require weeks or even months. The entire procedure is manual, adding costs required for resources and increasing chances of human errors. In this scenario, smart contracts can automate certain parts of the claims process. Insurance agencies can write various insurance policies into smart contracts. Smart contracts can include several parameters based on the type of insurance policy. When the requirements of certain parameters are met, insurance claims will be processed automatically. For instance, factors such as the location of a hurricane and wind speed can be recorded into a smart contract and claims process will be initiated if the specified thresholds are crossed. Another use case among multiple smart contract use cases can be auto insurance. Smart contracts can record policy details and driving reports of drivers. By integrating IoT sensors into cars, smart contracts can instantly execute claims processing in case of an accident.

**Prediction markets in financial services.**

Prediction markets enable people to predict the outcome of events such as sports, election campaigns, and auctions. For example, the outcome of a football match or the future election campaigns of a politician. Prediction markets offer valuable insights regarding public opinions about a company or a political campaign. Businesses can also use prediction markets to understand whether they should launch a new product or not. Smart contracts can record the predictions of large groups of participants transparently to obtain more accurate forecasts. Participants can be incentivized for being a part of the prediction market and they can be rewarded after making accurate predictions. Payment of incentives and rewards can become precise and automated with the help of smart contracts.

*References*

i. *Mastering Blockchain, Third Edition, Imran Bashir, ISBN 978-1-83921-319-9, August 2020*

ii. “Smart Contracts and DApps”, MIT OpenCourseWare, https://www.youtube.com/watch?v=JPkgJwJHYSc

iii. https://research.csiro.au/blockchainpatterns/general-patterns/blockchain-payment-patterns/escrow-2/

iv. China's digital currency - Smart contracts for monetary policy?”, https://www.soonparted.co/p/e-cny

v. Smart Legal Contracts and Legal Smart Contracts”, Stanford Law, https://www.youtube.com/watch?v=1Fa_2FXBAjA