



6

# Blockchain & DAPP Security

– Pratul Goyal

Assistant Professor, Graphic Era Hill University

 <https://orcid.org/0000-0003-1040-8109>  [pratul.goyal111@gmail.com](mailto:pratul.goyal111@gmail.com)

**B**lockchain is a list of records, called blocks, which are linked using cryptography. Block = Cryptographic hash of previous block + transaction data. Blockchain cannot be modified in any sense. It is an open disseminated ledger that records transactions between parties in a permanent way.

## Keywords

- Blockchain
- Hash
- Cryptography

## ARTICLE HISTORY

**Paper Nomenclature:** View Point (VP)

**Paper Code:** CYBNMV2N9SEP2020VP2

**Submission Online:** 02-Sep-2020

**Manuscript Acknowledged:** 04-Sep-2020

**Originality Check:** 07-Sep-2020

**Originality Test Ratio:** 10% (Drillbit)

**Peer Reviewers Comment:** 12-Sep-2020

**Blind Reviewers Remarks:** 17-Sep-2020

**Author Revert:** 20-Sep-2020

**Camera-Ready-Copy:** 25-Sep-2020

**Editorial Board Citation:** 29-Sep-2020

**Published Online First:** 30-Sep-2020

## Introduction

Blockchain carries no transaction cost even if it costs some infrastructure cost. It is simply a way of passing information from one position to another in an automated way. This transaction creates the block and is verified by millions of computers. Then the verified transaction is adding up to the chain and creating a permanent block in the blockchain process.

The blockchain fixes below issues:

- It simply removed third-party providers like a bank or payment processing applications.
- It simply records each transaction and provides visibility to all users and reduces fraud.
- Transaction does not include personal or PII information.

DApps websites are blockchain-enabled to which Smart Contract is connecting to the blockchain and they are adding the transactions to the block. They are like web applications. The disparity is that they are directly

doing interaction with Smart Contracts where all the calls are done using the API calls and these API calls use the smart contracts to interact with it.

In comparison to conventional, centralized applications, where centralized servers run the backend code, on a decentralized P2P network, with their backend code running. Decentralized software, from the backend to the frontend, consists of the whole package. Just one aspect of the DApps is the smart contract: Frontend (what you can see), and Backend (the business logic).

Let us see the first screenshot for smart contract auditing tools:

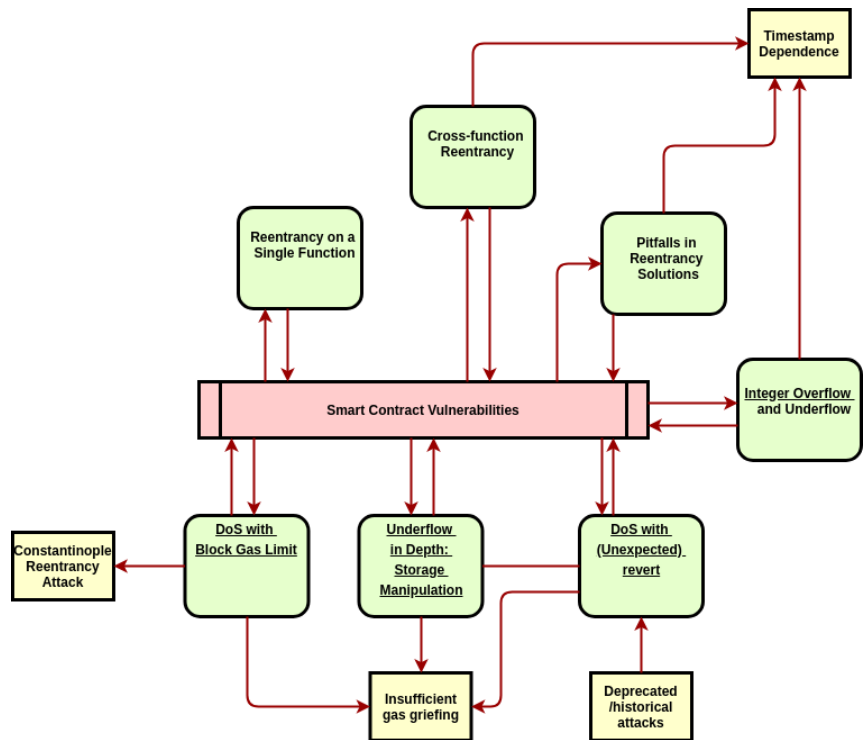
**Smart Contract Audit Tools**

- Echidna**: The only available fuzzer for Ethereum software. Uses property testing to generate malicious inputs that break smart contracts.
- Oyente**: Analyze Ethereum code to find common vulnerabilities.
- MythX**: Professional security analysis tools and extensions for Truffle, Embark and other environments.
- Octopus**: Security Analysis tool for blockchain Smart Contracts with support of EVM and JAVASCRIPT.

Second screenshot for smart contract attacks:



Third screenshot for smart contract vulnerabilities:



**Pratul Goyal**, is an Assistant Professor with Graphic Era Hill University and IIM Postgraduate, He got extensive experience in a vivid domain like data science and cyber security. He is also a consultant and has worked as a corporate trainer for Simplilearn. He also has his blogging website [datasciencejourney.com](https://datasciencejourney.com) and YouTube Channel.

[pratul.goyal111@gmail.com](mailto:pratul.goyal111@gmail.com)

**Annexure I**

Submission Date	Submission Id	Word Count	Character Count
07-Sep-2020	168357	290	5041

**DrillBit** Plagiarism Software

**10** SIMILARITY %    **3** MATCHED SOURCES    **A** GRADE

A-Satisfactory (0-10%)  
B-Upgrade (11-40%)  
C-Fair (41-60%)  
D-Unacceptable (61-100%)

S/N	LOCATION	MATCHED DOMAIN	%	SOURCE TYPE
1.	quizlet.com		6	Internet
2.	www.computerworld.com		1	Internet
3.	Analytical Modeling and Performance Evaluation of Cell Selection Algo, by Olmos, Juan J. Fer- 2013		1	Publication

Note: The Cybernomics had used the DrillBit plagiarism [https://www.drillbitplagiarism.com/] tool to check the originality.



### Reviewers Comment

**Reviewer's Comment 1:** Many sectors like Finance, Manufacturing, Medicine, and Education use Blockchain applications to profit from this technology. Still many are unaware of the blockchain DPP security applications, so this article would be very useful to spread knowledge about this concept.

**Reviewer's Comment 2:** The article gives a handful of knowledge on how blockchain applications fixes many issues. The article depicts how the concept and applications can be used to make the work easy and faster in a smarter way.

**Reviewer's Comment 3:** The article is well structured and the author has made significant usage of facts and figures. It talks about the modification of block chain taking the reference of DApps website, and shows a process of smart contract vulnerabilities.



### Editorial Excerpt

The article has 10% plagiarism which is an acceptable percentage for publication. The comments related to this manuscript are noticeable related to "Blockchain & DAP" both subject-wise and research-wise. The article highlighted about the modification of block chain taking the reference of DApps website, and have shown a process of smart contract vulnerabilities, the authors have also taken the Smart contracts attacks highlighting the different attack in blockchain. After comprehensive review and suggestions by the editorial board the paper has been categorized under the "View Point" category.

### Acknowledgement

The author is highly indebted to Scholastic Seed Inc. a publisher of Cybernomics Magazine and the editorial team including Resident Associate Editors (Ms. Sonakshi Jaiswal, Ms. Jyoti & Ms. Shailza), for making the write-up in the shape of an article.

### Disclaimer

All the views expressed in this paper are my own, of which some of the content is taken from open source websites for knowledge purpose. The content drawn from different sources have been mentioned above in the references section.



### Citation

Pratul Goyal  
"Blockchain & DAPP Security"  
Volume-2, Issue-9, September 2020.  
([www.cybernomics.in](http://www.cybernomics.in))

Frequency: Monthly, Published: 2020  
**Conflict of Interest:** Author of a Paper  
had no conflict neither financially  
nor academically.

