Blockchain And Its Applications

Department of Computer Science and Engineering

Indian Institute of Technology, Jodhpur

Presented By:
Dr. Debasis Das
Computer Science and Engineering Department
Indian Institute of Technology, Jodhpur

Attendance Requirements

- A student should have full attendance in each course. Unless the student takes leave of absence for valid reasons, the student has to attend every **lecture, tutorial, or lab session**. The attendance records must be made available to the student after every lecture. Even if the student's attendance falls below **75%,** the student will be allowed to appear for the exams. **Students not meeting attendance criterion of 75% will be required to score C grade to pass a course**. **These students would be awarded F grade if their marks are lower than cut-off for C grade in a course.**

Evaluation Scheme

Components	Weightage	
Minors	20%	
End Sem (Major)	40%	
continuous evaluation(Assignments, Quizes etc)	40%	

Algorithms for Security

confidentiality: only sender, intended receiver should “understand” message contents

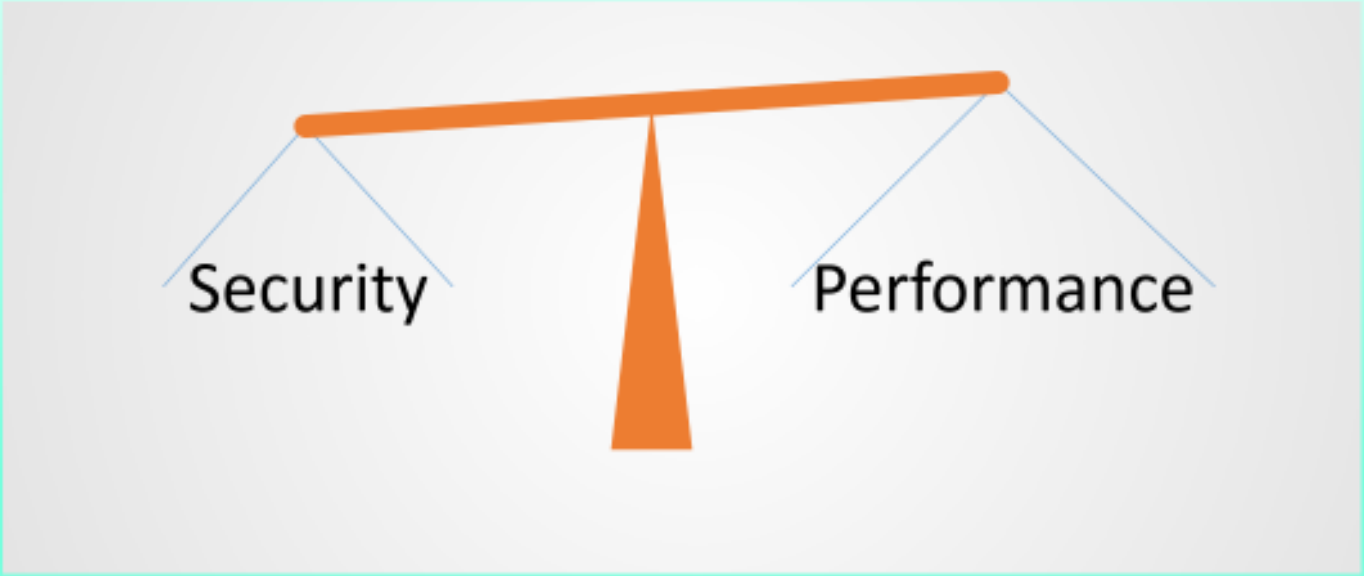
- sender encrypts message
- receiver decrypts message

authentication: sender, receiver want to confirm identity of each other

message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

access and availability: services must be accessible and available to users

Security-Performance Tradeoff



Encryption

Alice

Plaintext
"Attack at Dawn!!"

K

E

encryption

untrusted communication link

#%AR3Xf34^$
(ciphertext)

K

D

decryption

Bob

"Attack at Dawn!!"

Mallory

How do we design ciphers?

Cryptology

("hidden word")

Cryptography

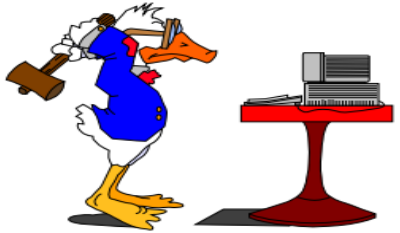
(code making)

The "good guys"

Cryptanalysis

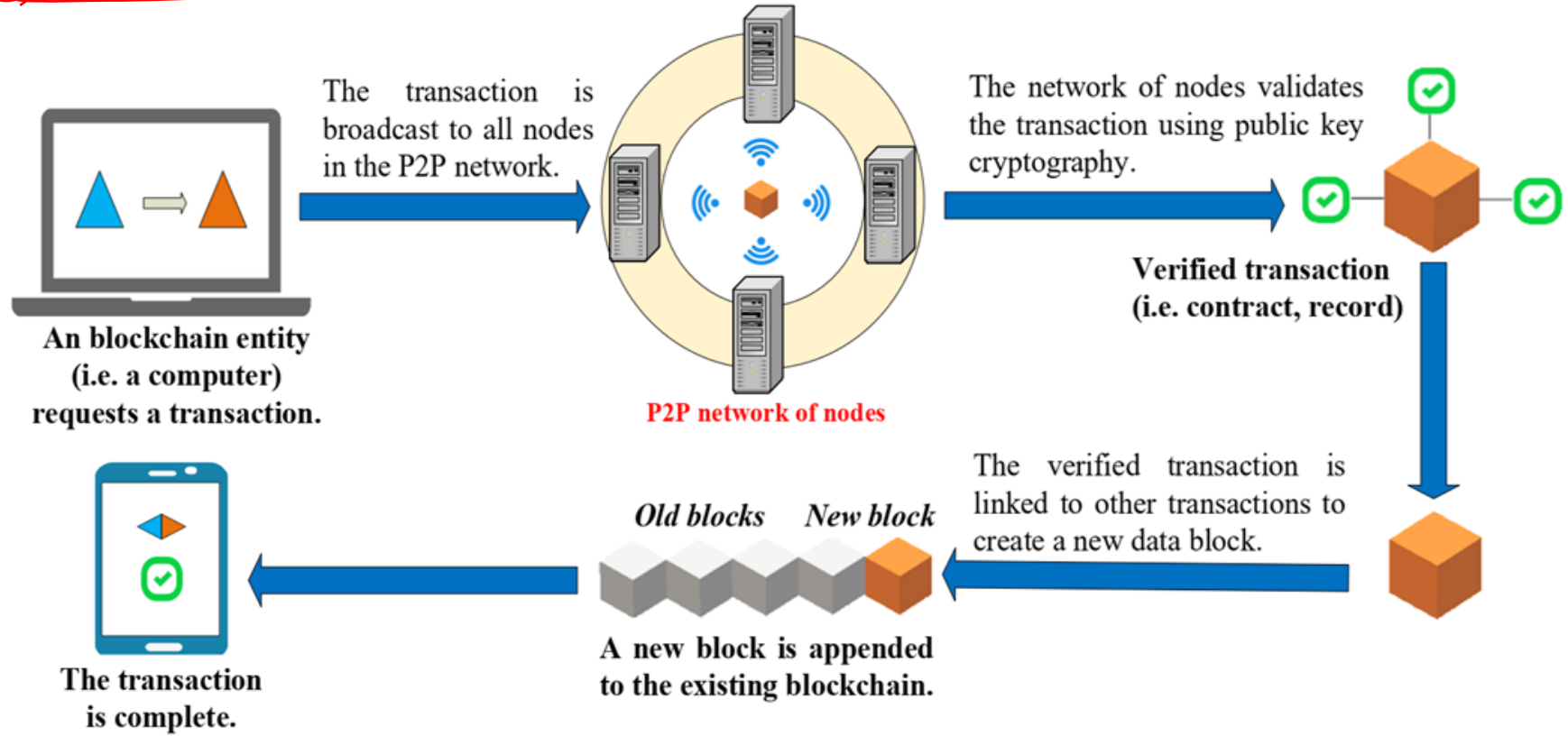
(code breaking)

The "bad guys"



Technology : Blockchain

Blockchain is a immutable, distributed, and tamper-proof ledger technology

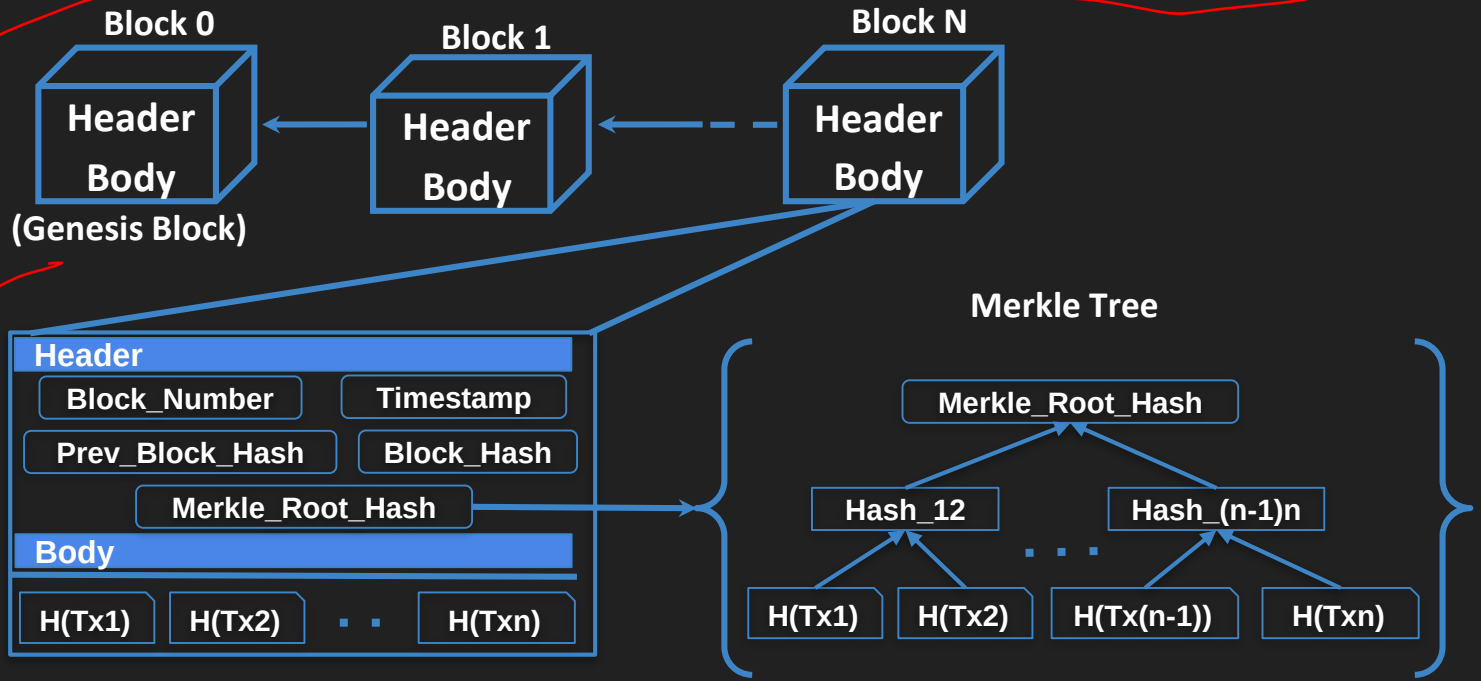


Blockchain

1. The core idea of a blockchain is **decentralization.** This means that blockchain does not store any of its database in a central location.
2. Whenever a new block is added to the blockchain, every computer on the network updates its blockchain to reflect the change.
3. This decentralized architecture **ensures robust and secure operations** on blockchain with the advantages of tamper resistance and no single-point failure vulnerabilities.
4. This is enabled by a mechanism called **consensus** which is a set of rules to ensure the agreement among all participants on the status of the blockchain ledger.
5. In general, blockchains can be classified as either a **public (permission-less) or a private (permissioned) blockchain.**
6. A **public blockchain** is accessible for everyone and anyone can join and make transactions as well as participate in the consensus process.
7. **Private blockchains** on the other hand are an invitation-only network managed by a central entity. A participant has to be permissioned using a validation mechanism.

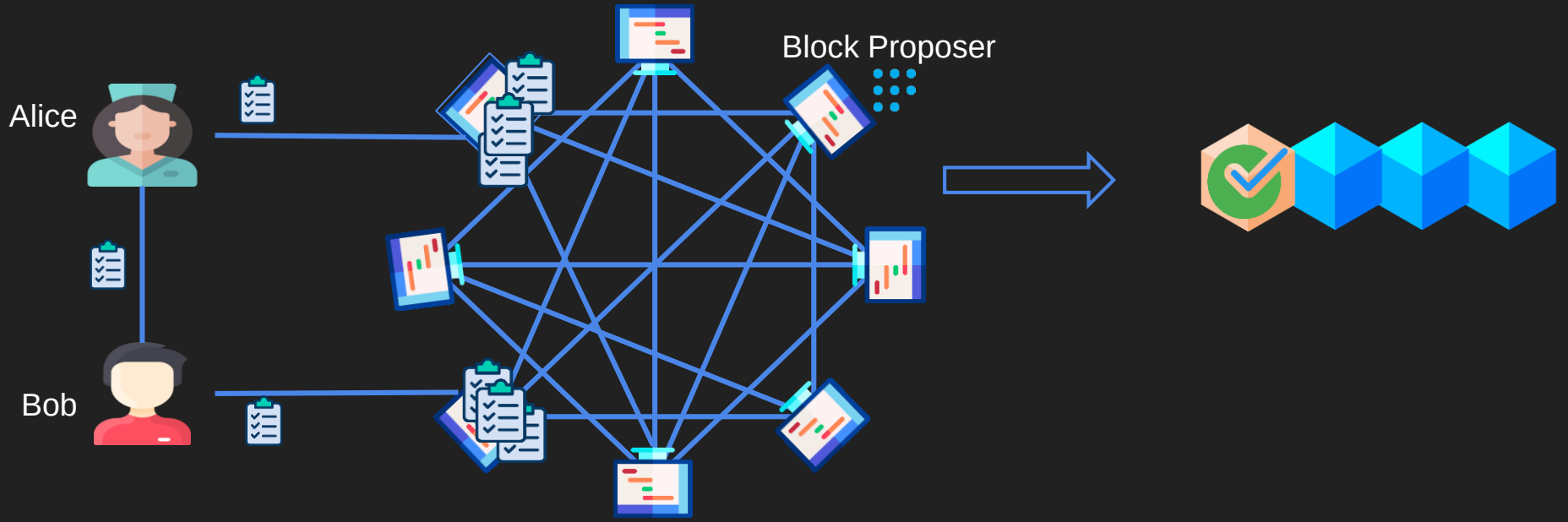
1. Introduction

Blockchain is a immutable, distributed, and tamper-proof ledger technology.



Consensus Algorithm

It is an general agreement between all the participating nodes in the network.



Types of Consensus Algorithm

Baseline Consensus algorithms:

- Proof-of-Work (PoW)
- Proof-of-Stake (PoS)
- Practical Byzantine Fault Tolerance (PBFT)

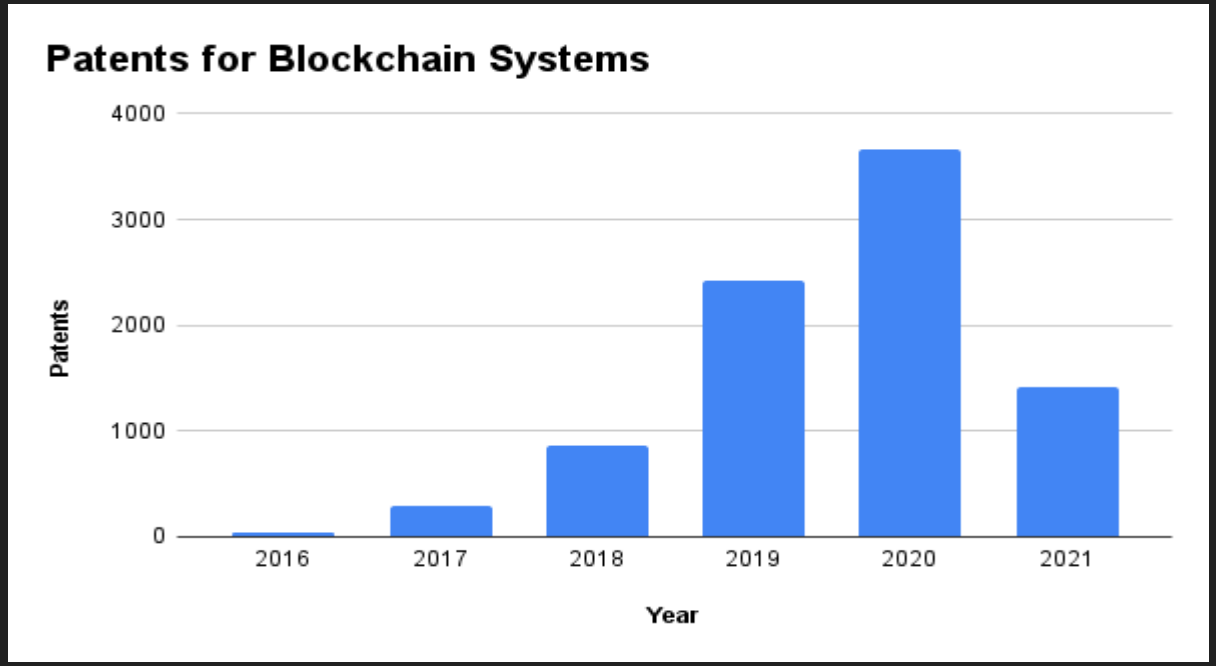
Other variants of Consensus algorithms

- Delegated Proof-of-Stake (DPoS)
- Proof-of-Elapsed Time (PoET)

Blockchain Protocols

Protocol	Year	Consensus	Description	Limitation
Bitcoin [1]	2008	PoW	+ First unanimously accepted cryptocurrency + Uses PoW to agree on the next set of validated transactions	+ High consensus delay + Low throughput upto 4-6 Transaction per second (TPS) + Fork generation
Ethereum [2]	2013	PoW / PoS	+ Second most widely accepted blockchain platform + Uses PoW and smart contracts. + Native cryptocurrency is Ether	+ 51% attack. + Software vulnerabilities due to smart contracts. + Low throughput upto 16 TPS
Bitcoin-NG [3]	2016	PoW, BFT	+ Decouples blockchain operation into Leader selection and transaction serialization + Uses PoW for leader selection and PBFT for block confirmation	+ Unfair leader selection and remuneration policy + Fork generation + Low throughput upto 20 TPS.

Patents for Blockchain Systems

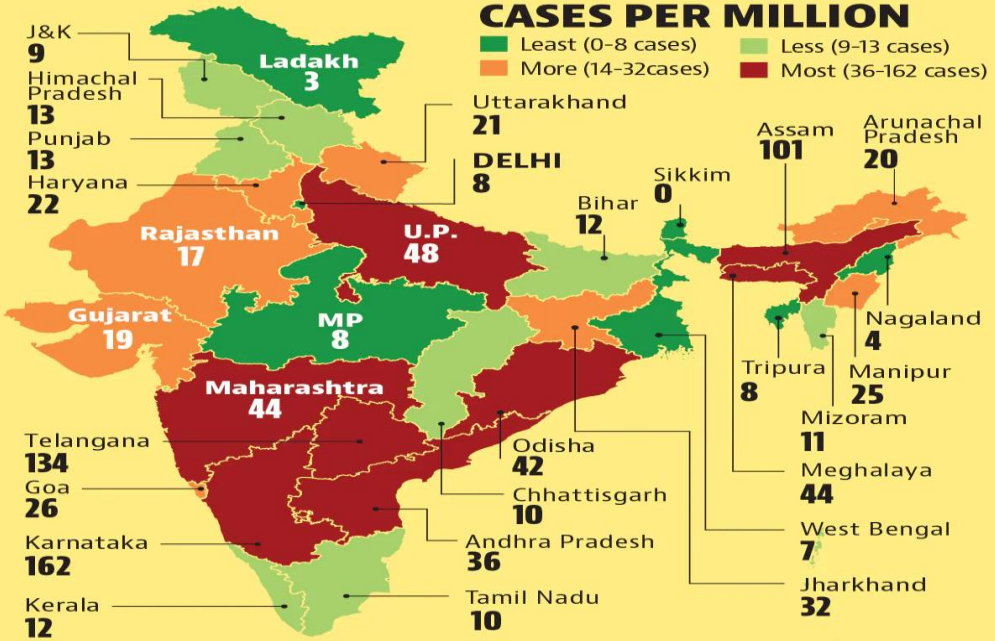


Blockchain for Fintech

Cyber crimes registered 11.8% increase

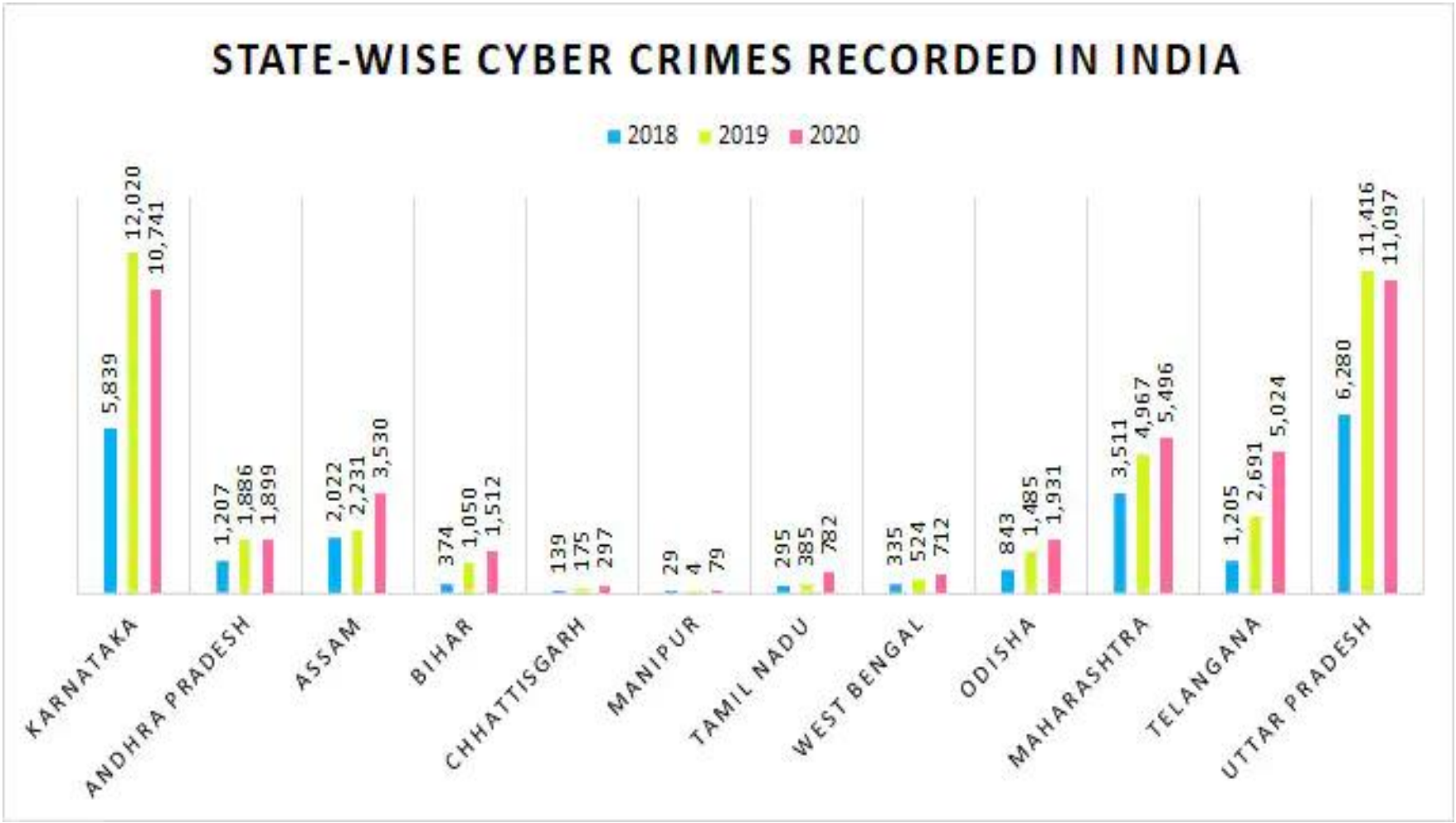
Vulnerable digital space

Number of cases filed last year under sections dealing with cyber crime rose to 50,035 from 44,735 a year before as more people moved to working from home, spending more time with digital tools

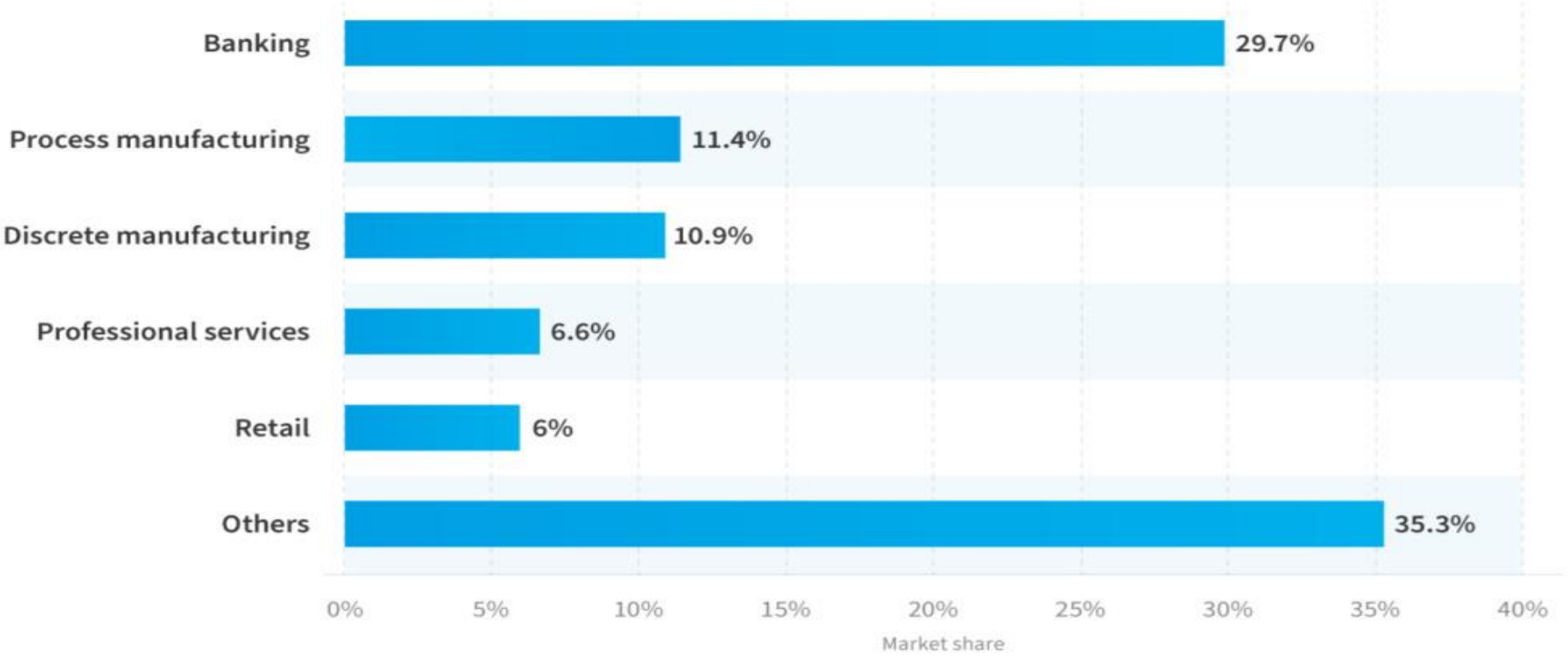


RATE OF CRIME

State	Cases filled in 2020	Change from 2019
Uttar Pradesh	11,097	-2.8%
Karnataka	10,741	-10.6
Maharashtra	5,496	10.7
Telangana	5,024	86.7
Assam	3,530	58.2
Odisha	1,931	30.0
Andhra Pradesh	1,899	0.7
Bihar	1,512	44.0
Rajasthan	1,354	-23.2
Gujarat	1,283	63.6
Jharkhand	1,204	10.0
Tamil Nadu	782	103.1
West Bengal	712	35.9
Madhya Pradesh	699	16.1
Haryana	656	16.3
Kerala	426	38.8
Punjab	378	55.6
Chhattisgarh	297	69.7
Uttarakhand	243	143.0
Delhi	168	46.1


STATE-WISE CYBER CRIMES RECORDED IN INDIA
2018
2019
2020
KARNATAKA
5,839
12,020
10,741
ANDHRA PRADESH
1,207
1,886
1,899
ASSAM
2,022
2,231
3,530
BIHAR
374
1,050
1,512
CHHATTISGARH
139
175
297
MANIPUR
29
4
79
TAMIL NADU
295
385
782
WEST BENGAL
335
524
712
ODISHA
843
1,485
1,931
MAHARASHTRA
3,511
4,967
5,496
TELANGANA
1,205
2,691
5,024
UTTAR PRADESH
6,280
11,416
11,097

Distribution of blockchain market value worldwide in 2020, by vertical



Source: Statista 2020

Challenges of Blockchain for Fintech

1. How to design a consensus protocol that is suitable for banking and Finance Industry transaction processing ?

1. How to improve the scalability issue in consensus protocol?

1. How to avoid a single point of failure, meaning, making the network as decentralised as possible?

1. How to design a consensus protocol that is secure even in the presence of a malicious node?

1. How to design a consensus protocol that respects the balance between decentralisation, security, and scalability?

An Ideal Blockchain System

- **Robustness**
  - *Safety* against double spending attacks
  - *Liveness* against denial of service attacks

- **Performance**
  - High *throughput*
  - Fast *confirmation*

- **Decentralization**
  - *Scale* to large amount of participants
  - *Permissionless* to join and leave

Blockchain Performance Problem

Transactions per Second:	~7	~30	~200	~3000
Confirmation Latency:	1 hour	7~10 minutes	Few seconds	Few seconds


THANK YOU