Blockchain: State of the Art, Security Concerns and Future

Group Members:

ABBA GARBA

Dalle nyame Yvonne Patricia

Ange, Herenui BOUMBA

Emahatsion Issac Tekle

Clara RHY Wang

董子宁

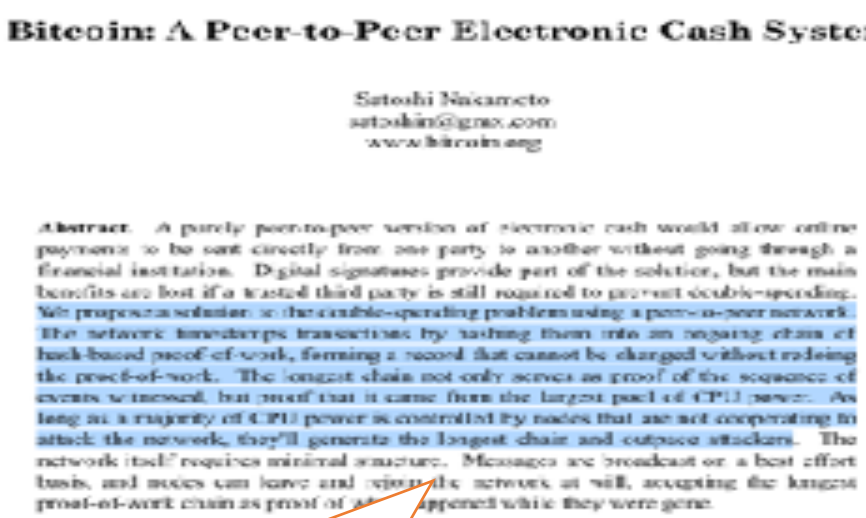
Overview of Blockchain Technology

Introduction

- Technical overview

- Types of Blockchains and their applications
  - Public Blockchains
  - Private Blockchains
  - Consortium Blockchains
- Other form of Blockchains
  - Permissioned
  - Permissionless
- Real world use cases
- Security and Privacy concerns
  - Existing solutions to optimize current Blockchain technologies.
- Conclusion

Introduction of Blockchain Technology



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Satoshi made a Break through by solving long-standing problem of double spending with out the need of a trusted authority.

- Virtual currency system without any **trusted parties.**
- Participants without real **identities**.
- Solve generals problem in a distributed systems (Byzantine).
- Proposed a system which is hard to hack (**Blockchain).**
- Automated contract **(Smart contract)**
- "Bitcoin works in practice, but not in theory" (Bonneau, 2015).

- Security and privacy challenges
- Managing contracts execution

Who invented Blockchain?

Contrary to popular belief, shadowy inventor of Bitcoin, Satoshi Nakamoto, did not invent blockchain. So who did?

Satoshi Nakamoto

Real Satoshi Behind Bitcoin?

Nick Szabo

Craig Steven Wright

Gavin Andresen

Adam Back

Why Blockchain Technology Matters?

- Decentralized, distributed and public digital ledger
- Contains growing list of records called: **Blocks**
- Block contains a transaction data and cryptographic hash of the previous block.
- Managed by a **peer-to-peer network and distributed time-stamping**
- Miners in the Blockchain validate new blocks.
- Data is immutable
- Decentralized consensus (POW/POS/DPOS).

Key essentials of blockchain technology

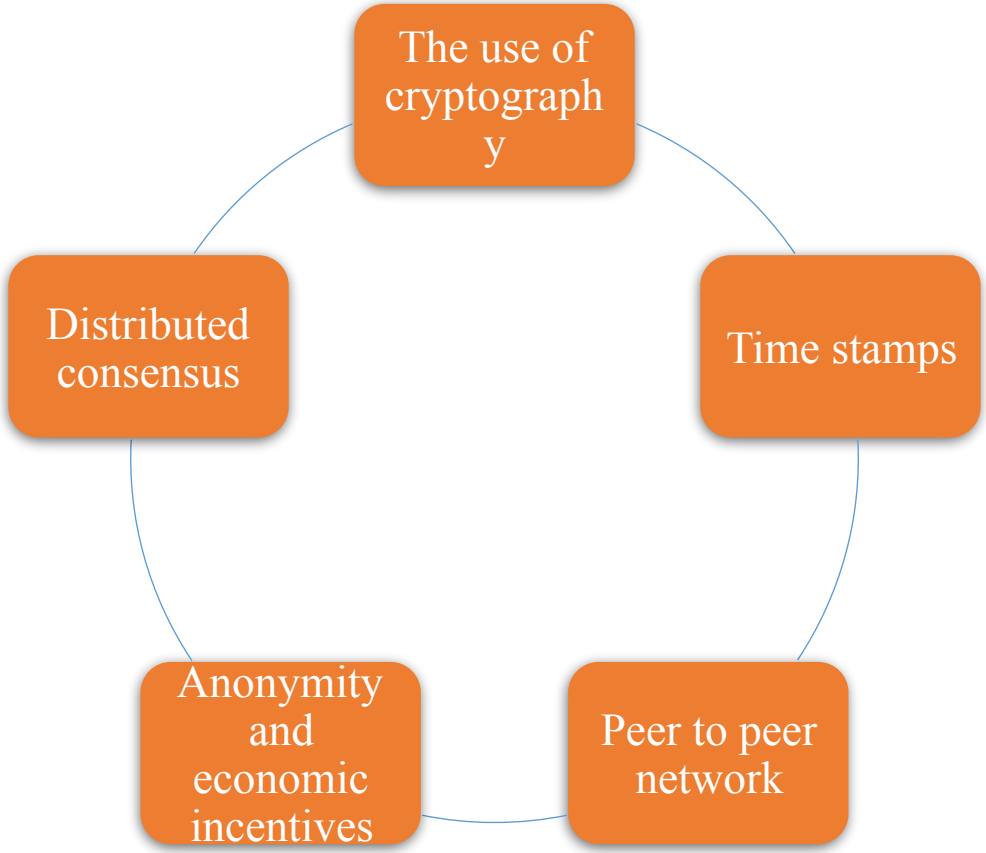


Figure 1: Key essentials of blockchain technology

Transactions, Blocks, Mining, and the Blockchain

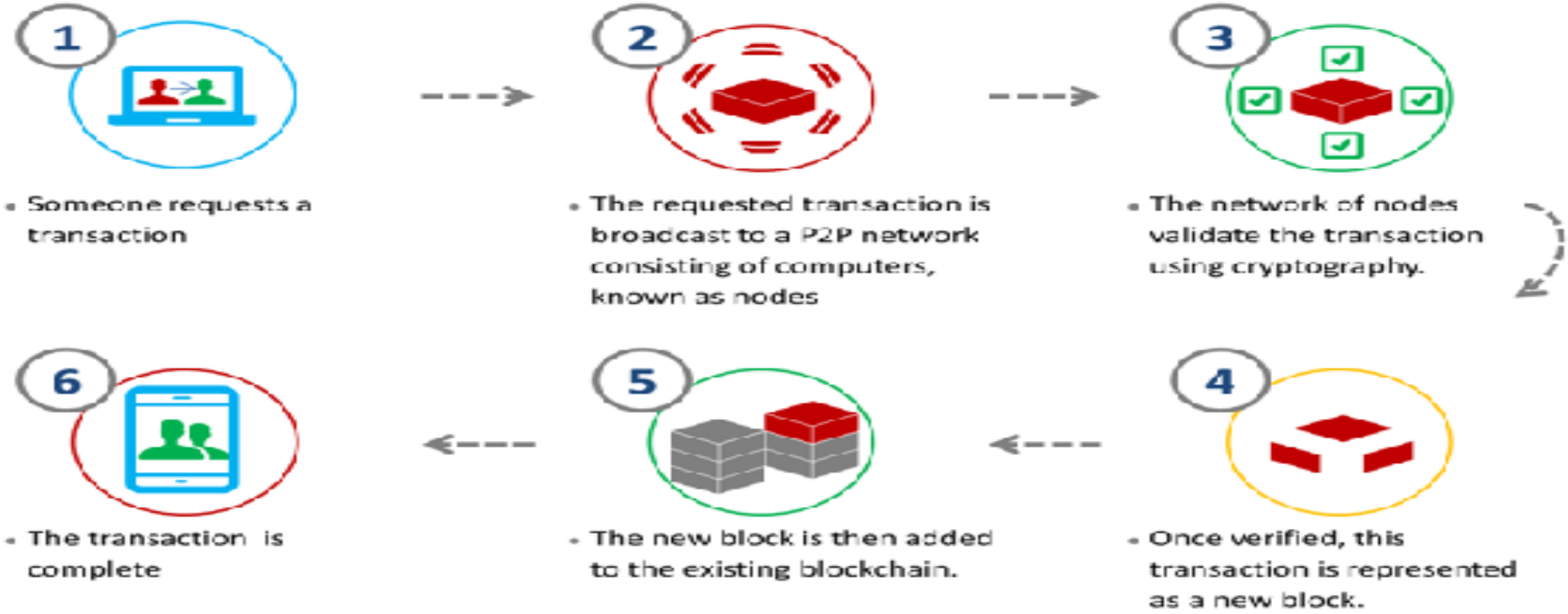


Figure 2: Transaction circle in Blockchain

How Blockchain Works

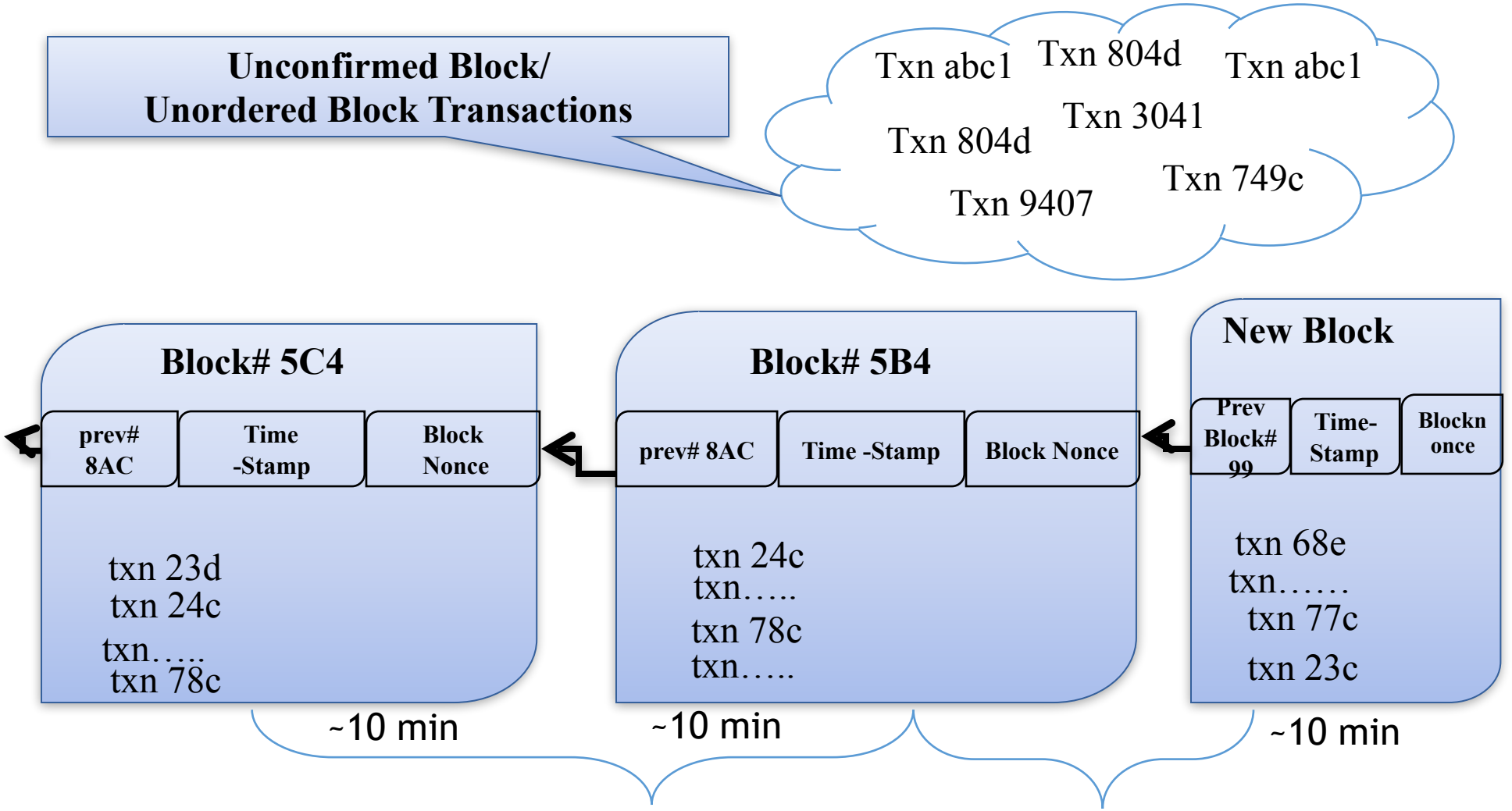


Figure 3: How Blockchain works

Types of Blockchain

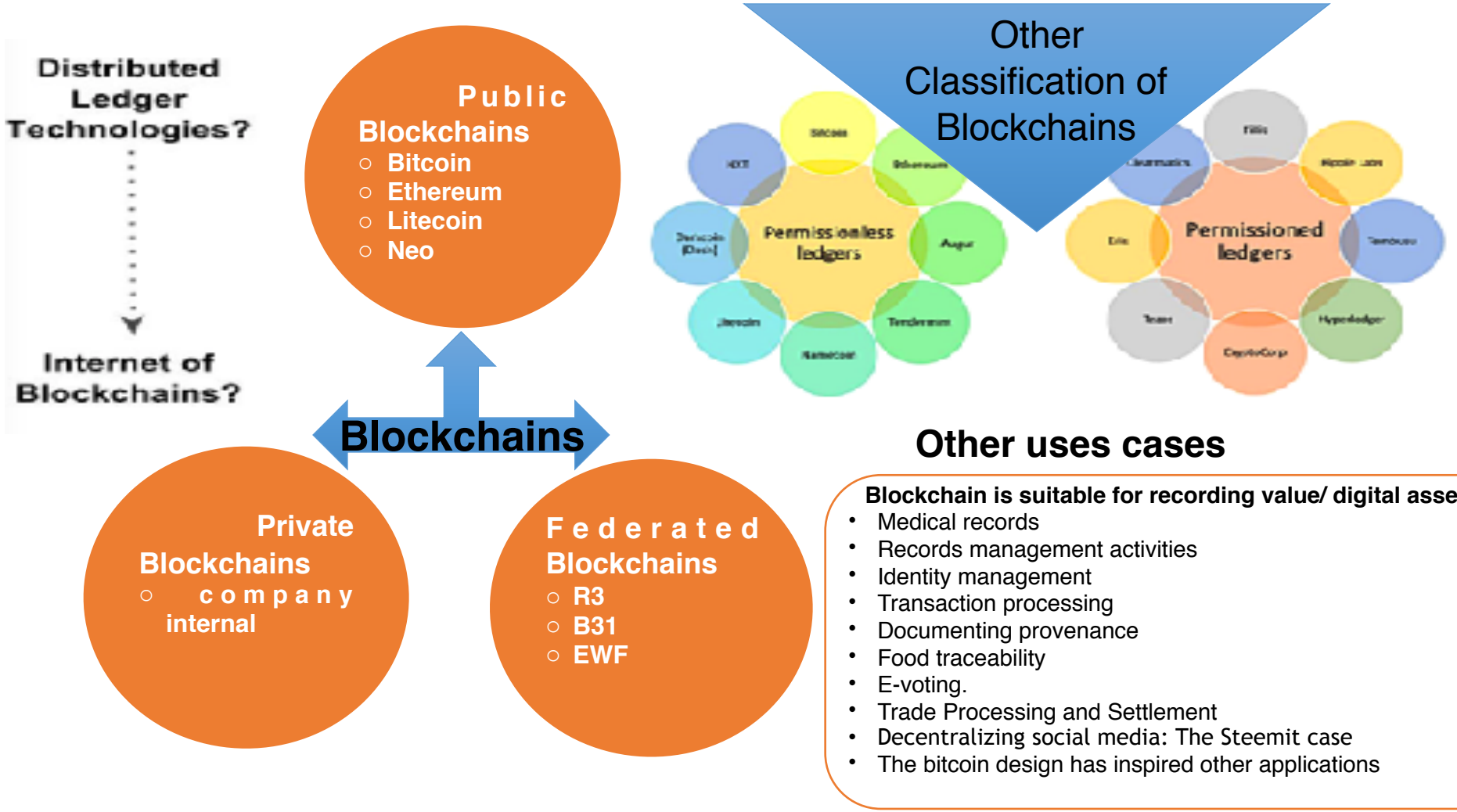


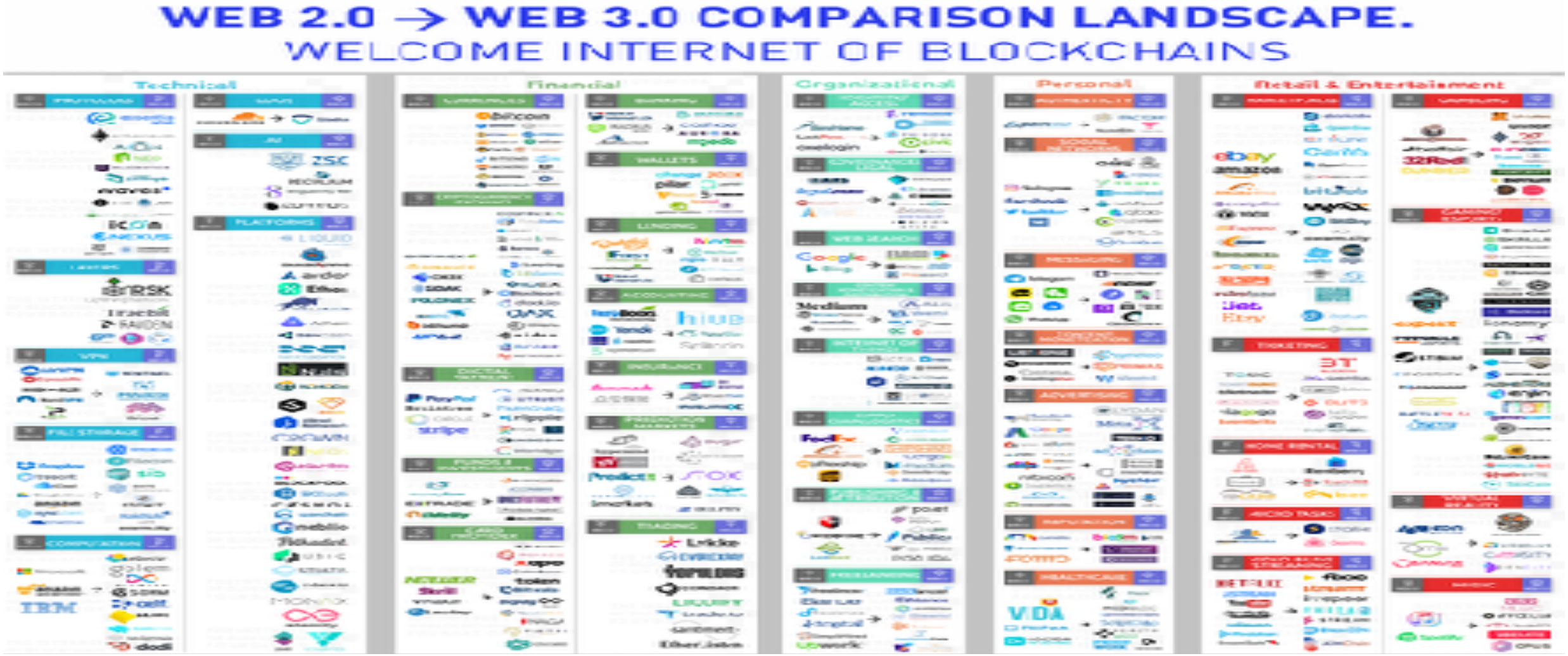
Figure 4: Types of Blockchain

Types of Blockchain

	Public Blockchain	Private Blockchain	Federated/Consortium Blockchain
Access	• Anyone	• Single organization	• Multiple selected organizations
Participants	• Permissionless • Anonymous	• Permissioned • Known identities	• Permissioned • Known identities
Security	• Consensus mechanism • Proof of Work / Proof of Stake	• Pre-approved participants • Voting/multi-party consensus	• Pre-approved participants • Voting/multi-party consensus
Transaction Speed	• Slow	• Lighter and faster	• Lighter and faster

Table 1: Table indicate Blockchain types and their core features

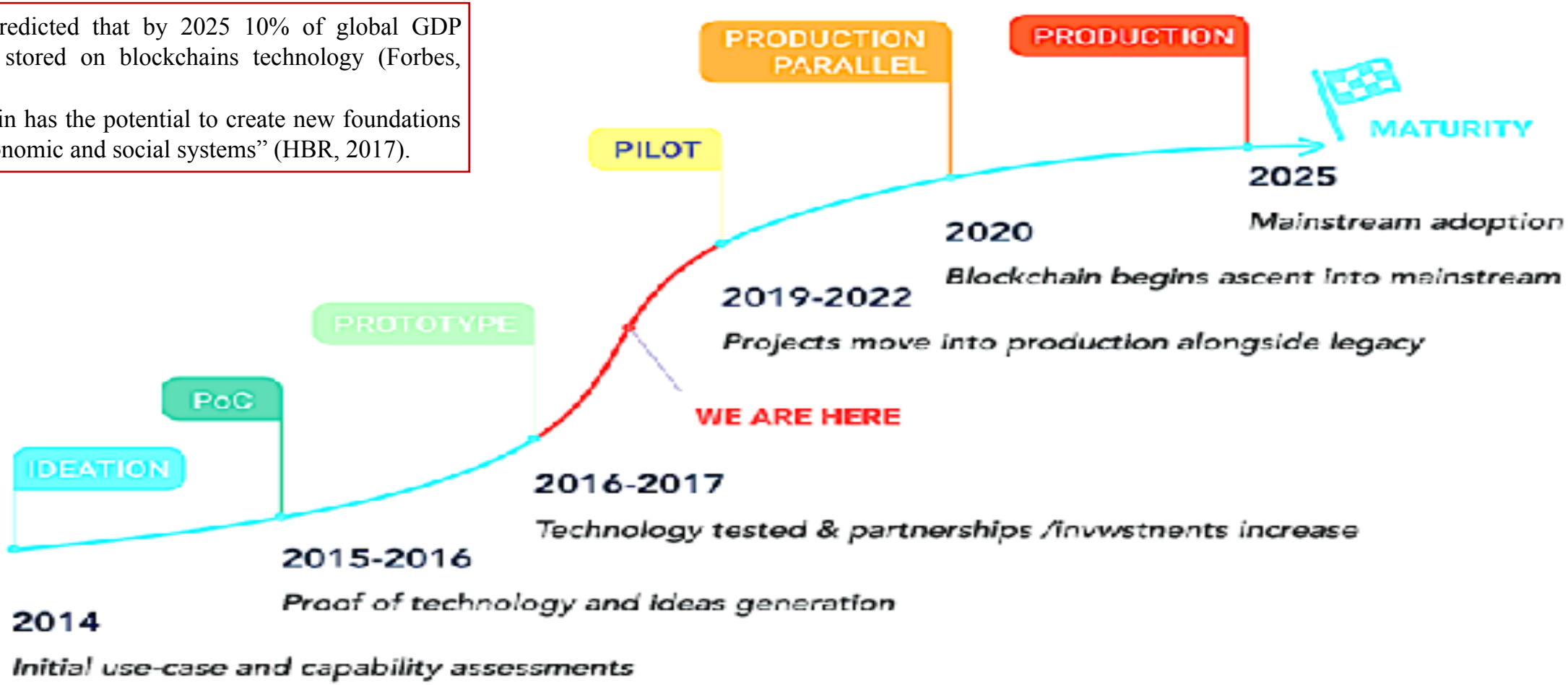
Why the net giants are worried about the Web 3.0



Source: The Internet of Blockchains Foundation (2018).

Blockchain Maturity Model

A WEF predicted that by 2025 10% of global GDP would be stored on blockchains technology (Forbes, 2016).
"Blockchain has the potential to create new foundations for our economic and social systems" (HBR, 2017).



Source: H Wang (2016) Figure 5: Maturity Model of Blockchain

Blockchain Strengths, Weaknesses, Opportunities and Threats (SWOT).

Strengths	Weaknesses
○ Distributed resilience and control ○ Decentralized network ○ Open source ○ Security and modern cryptography ○ Native asset creation ○ Asset provenance ○ Dynamic and fluid value exchange	○ Lack of ledger interoperability ○ Customer unfamiliarity and poor user experience ○ Lack of hardened/tested technology limitation ○ Smart contract code of programing model ○ Wallet and key management ○ Poor developer user experience skills scarcity ○ Immature scalability ○ Lack of trust in new technology suppliers
Opportunities	**Threats**
○ Reduced transaction costs ○ Business process acceleration and efficiency ○ Reduced fraud ○ Reduced system risk ○ Monetary democratization ○ New business-model enablement ○ Application rationalization and redundancy	○ Legal jurisdictional barriers ○ Politics and hostile notion state actors ○ Technology failures ○ Institutional adoption barriers ○ Divergent blockchain ○ Ledger conflicts/competition ○ Poor governance

Table 2: Blockchain (SWOT) Source: Niranjanamurthy (2018)

Security challenges of blockchain technology

- Proof-of-work is use to secure public blockchains e.g Bitcoin and Ethereum

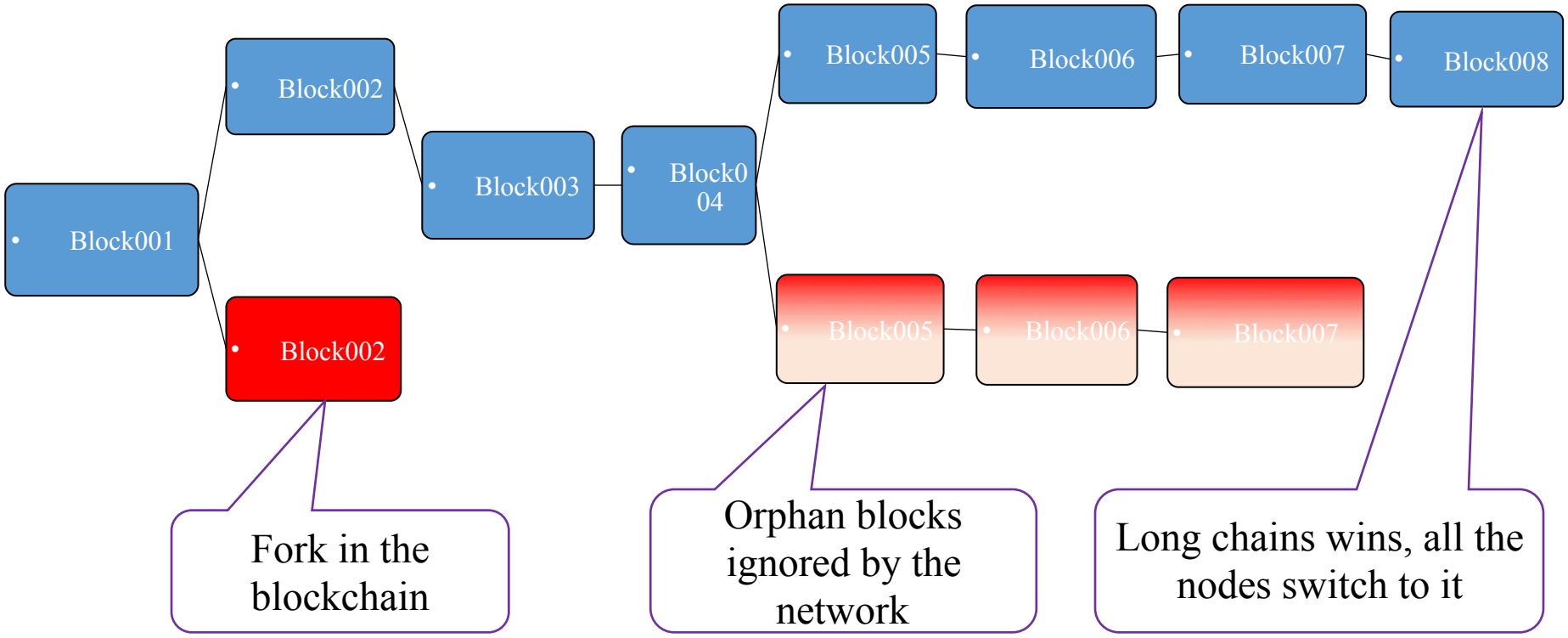


Figure 6: Dynamics of Blockchain

Smart contract Vulnerabilities

What is Smart Contract?

- Smart contracts: are computer programs that can be correctly executed by a network of mutually distrusting nodes, without trusted authority.
- Handle transfer of assets
- Smart contracts are stored on a blockchain **(immutable).**
- Managing the contract execution led to severe security challenges (stealing or tampering the assets)
- Smart Contracts rely on a non-standard software life-cycle (Luu, 2017)
- Handling updates or bugs (Software update)
  - E.g a wallet application freeze (500K Ethers~150M USD), in Nov. 2017.
  - The DAO (~ $150M) June, 2016.
  - An attacker managed to put ~ $60M under her control, until the hard-fork of the blockchain nullified the effects of the transactions involved in the attack (Hamida, 2017).

Attacks and Counter Measures

Attack	Description	Primary targets	Adverse effects	Possible countermeasures
Double spending attacks	coins in multiple transactions, send two conflicting transactions in rapid succession	sellers or merchants	sellers lose their products, drive away the honest users from network, creates blockchain forks	inserting observers in the network, communicating double spending alerts among peers , nearby peers should notify the merchant about an ongoing double spend as soon as possible, merchants should disable the incoming connections.
> 50% hashpower or Goldfinger	adversary controls more than > 50% of computational power in the Bitcoin network	Bitcoin miners, exchange and users network, Bitcoin centers,	drive away the miners working alone or within small mining pools, weakens the effectiveness of consensus protocol, DoS	inserting observers in the network, communicating double spending alerts among peers, disincentivize large mining pools.
Eclipse or net-split	adversary monopolizes all of the victim's incoming and outgoing connections	miners and users	inconsistent view of the network/ block chain at the attacked node, enable double spends with more than one confirmation	use whitelists, disabling incoming connections.
Smart contract Vulnerabilities	Course a wallet application freeze, adversary can manipulate smart contract execution to gain profit. Improper execution of contracts.	Participants in the contract.	Causing the freezing huge amount of Eth	Formal verification tools such as: Oyente to find potential security bugs.

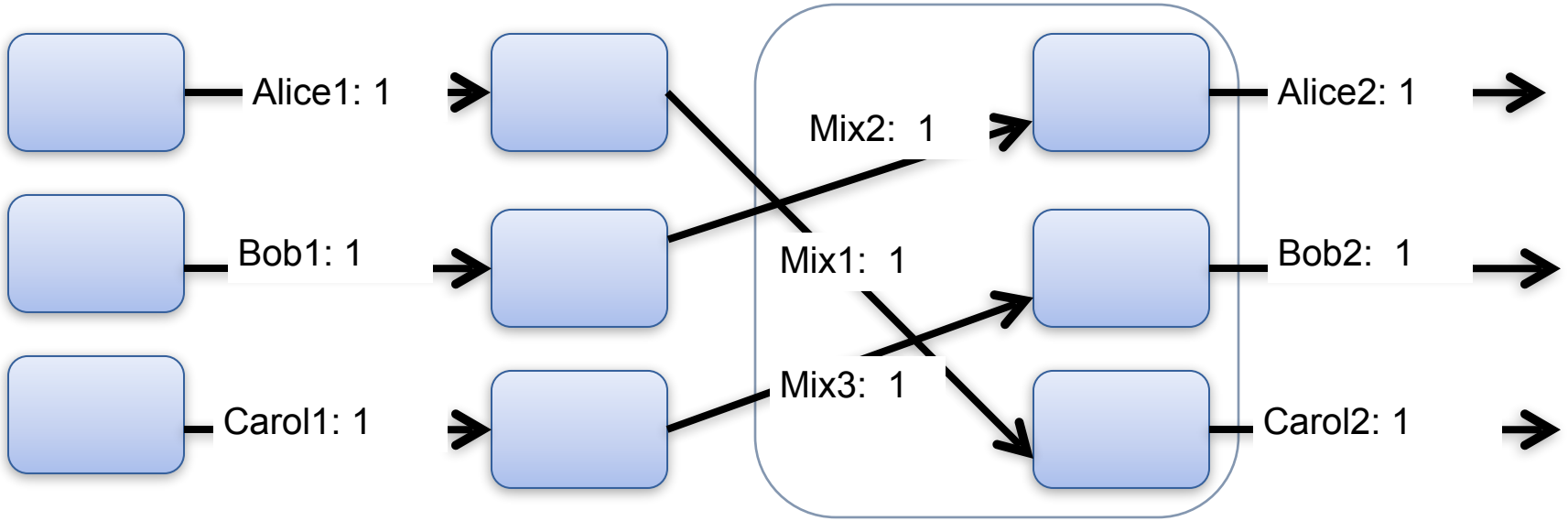
Table 3: Attacks and Counter Measures Source: Mauro Conti (2017)

Privacy and Anonymity

"Bitcoin is a secure and anonymous digital currency" (Wikileaks).
"Bitcoin won't hide you from the NASA's prying eyes" (Wired, UK).

- In Bitcoin and smart contracts entire transactions are stored in public ledger (Data privacy)
  - –Users privacy hidden behind pseudonymous (i.e., public keys)
  - –Smart contract transaction (Data flow in a contracts)
- Meta data in the Private Blockchain is crucial (Competitors)
- The public verifiability of pseudonymous transactions in Blockchain is vulnerable :
  - –De-anonymization Attack
  - –Traceability
  - –Linkability
  - –IP address monitoring nodes
  - –web-spidering
- Balances held by each address can be exposed and readily available (UTXO).
- There is possibility of transaction graph analysis

Mixing Technique



✓ Users to send their funds to a central pool and later retrieve the funds to a different Bitcoin address.
✓ These services combine the inputs of many users so that the outputs are difficult to trace back to the inputs.

- **Drawback**
  - Delay between the deposit and the withdrawal.
  - vulnerable to Sybil attacks
  - Lack of trust from the operator

Comparison of different Privacy enhancing Schemes

Proposals	Type/Class	Distinct features and properties	Advantages	Disadvantages
ConJoin	P2P	uses multi-signature transactions to enhance privacy	Prevent thefts, lower transaction fee	anonymity level depends on the number of participants, vulnerable to DoS, Sybil and intersection attacks, prevents plausible deniability
CoinShuffle	P2P	decentralized protocol for coordinating CoinJoin transactions through a cryptographic mixing protocol	internal unlinkability, robust to DoS attacks, theft resistance	lower anonymity level and deniability, prone to intersection and sybil attacks
Xim	P2P	anonymously partnering and multi- round mixing	distributed pairing, internal unlink- ability, thwarts Sybil and DoS at- tacks	higher mixing time
Dandelion	P2P	networking policy to prevent network-facilitated deanonymization of Bitcoin users	provides strong anonymity even in the presence of multiple adversaries	vulnerable to DoS and sybil attacks
SecureCoin	P2P	based on CoinParty concept, an efficient and secure protocol for anonymous and unlinkable Bitcoin transactions	protect against sabotage attacks, at- tempted by any number of participating saboteurs, low mixing fee, deniability	vulnerable to DoS attacks, limited scalability

Table 4: Privacy Enhancing Schemes 1 Source: Mauro Conti (2017).

Comparison of different Privacy enhancing Schemes

Proposals	Type/Class	Distinct features and properties	Advantages	Disadvantages
BlindCoin	Distributed	based on MixCoin concept, uses blind signature scheme to ensure anonymity	internal unlinkability, DoS and Sybil resistance	partial theft resistance, additional costs and delays in mixing process
TumbleBit	Distributed	unidirectional unlinkable payment hub that uses an untrusted intermediary	prevents theft, anonymous, resists intersection, Sybil and DoS, scalable (implemented with 800 users)	normal payment using TumbleBit needs at least two sequential trans- actions
ZeroCoin / Zero-Cash	Altcoin	a cryptographic extension to Bit- coin , unlinkable and untraceable transactions by using zero knowledge proofs	provides internal unlinkability, theft and DoS resistance	relies on a trusted setup and non- falsifiable cryptographic assumptions, blockchain pruning is not possible
CryptoNote	Altcoin	relies on ring signatures to provide anonymity	provides strong privacy and anonymity guarantees	higher computational complexity, not compatible with pruning
MimbleWimble	Altcoin	a design for a cryptocurrency with confidential transactions	CT compatibility, improve privacy, fungibility and scalability	vulnerable to DoS attacks, not compatible with smart contracts
ByzCoin	Altcoin	Bitcoin-like cryptocurrency with strong consistency via collective signing	lower consensus latency and high transaction throughput, resistance to selfish and stubborn mining , eclipse and delivery- tampering and double-spending attacks	vulnerable to slow down or DoS attack and 51% attack.

Table 5: Privacy Enhancing Schemes 2 Source: Mauro Conti (2017).

Innovation and Future Blockchain Applications

- Blockchain in IOT and AI
- Asset management
- Insurance
- Supply chain management
- Health care
- Cloud storage
- Food and provenance
- Identity Management
- Entertainment, Music, IP, Energy etc.

Thanks for your time!

References

- Eyal, I. and Sirer, E.G., 2014, March. Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security* (pp. 436-454). Springer, Berlin, Heidelberg.
- Satoshi Nakamoto (2009)Bitcoin: A Peer-to-Peer Electronic Cash System
- Conti, M., Kumar, S., Lal, C. and Ruj, S., 2018. A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials*.
- Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A. and Felten, E.W., 2015, May. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In *Security and Privacy (SP), 2015 IEEE Symposium on* (pp. 104-121). IEEE.
- Marr, B., 2016. How Blockchain Technology Could Change The World. *Forbes, May*, *27*.
- Harvard Business Review (2017)
- Niranjanamurthy, M., Nithya, B.N. and Jagannatha, S., Analysis of Blockchain technology: pros, cons and SWOT. *Cluster Computing*, pp.1-15.
- Wang, H., Chen, K. and Xu, D., 2016. A maturity model for blockchain adoption. *Financial Innovation*, *2*(1), p.12.
- Hamida, E.B., Brousmiche, K.L., Levard, H. and Thea, E., 2017, July. Blockchain for Enterprise: Overview, Opportunities and Challenges. In *The Thirteenth International Conference on Wireless and Mobile Communications (ICWMC 2017)*.
- Luu, L., Chu, D.H., Olickel, H., Saxena, P. and Hobor, A., 2016, October. Making smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 254-269). ACM.
- Li, X., Jiang, P., Chen, T., Luo, X. and Wen, Q., 2017. A survey on the security of blockchain systems. *Future Generation Computer Systems*.
- Atzei, N., Bartoletti, M. and Cimoli, T., 2017, April. A survey of attacks on Ethereum smart contracts (SoK). In *International Conference on Principles of Security and Trust* (pp. 164-186). Springer, Berlin, Heidelberg.
- Karame, G.O., Androulaki, E. and Capkun, S., 2012, October. Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM conference on Computer and communications security* (pp. 906-917). ACM.
- Bravecoin (2018) https://bravenewcoin.com/news/more-51-blockchain-attacks-expected/
- Wired UK, (2017)
- Weakileaks, (2018)