Kingston University London

Virtual Private Blockchains: Security Overlays for Permissioned Blockchains

[1]Samuel Onalo , [2]Deepak GC & [3]Eckhard Pfluegel

[123]School of Computer Science and Mathematics,

Kingston University London,

United Kingdom.

[1]email: k1450301@kingston.ac.uk

CYBER 2020 Nice, France.

A bit About Myself

Samuel Onalo

Nigerian Born and Bred

First Degree - Applied Physics

Second Degree - Network and Information Security with Business Management.

Currently a Ph.D. student research fellow at Kingston University London.

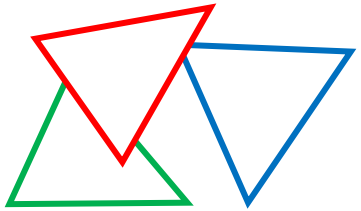
Work experience in Education, IT, Engineering and Business Management.

Area of Research Interest

- Application of Distributed/Decentralised Ledger Architectures for Security in Network and Information Technology Systems.

Content

- Introduction
- Blockchain Security
- Virtual Private Blockchains
- Security Analysis
- System Evaluation
- Application of the VPBC Architecture
- Conclusion

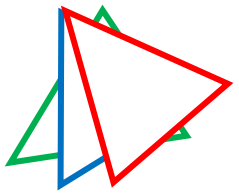


Introduction

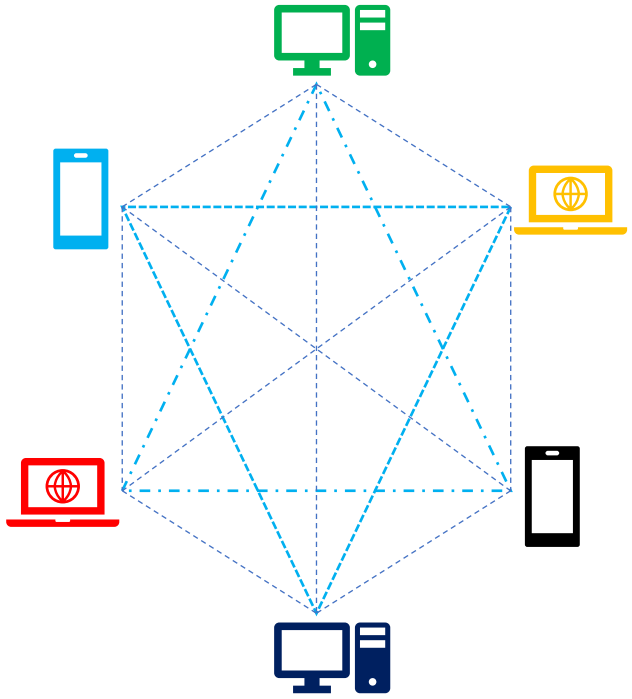
- Blockchain?
- A distributed or decentralized public or private ledger secured by cryptographic protocols with growing adoption across all sectors especially in financial technology.

- Areas of interests for Blockchain use cases for Businesses/Organisations.
- Public verifiability of data, Immutability, Decentralized architectures, Confidential or anonymous transactions.

- Fundamental research question
- Are there alternatives to the Private Blockchain Architecture with robust security infrastructure suitable for generic or specific use cases?
- Are there real-world use cases where such alternatives can be applicable?

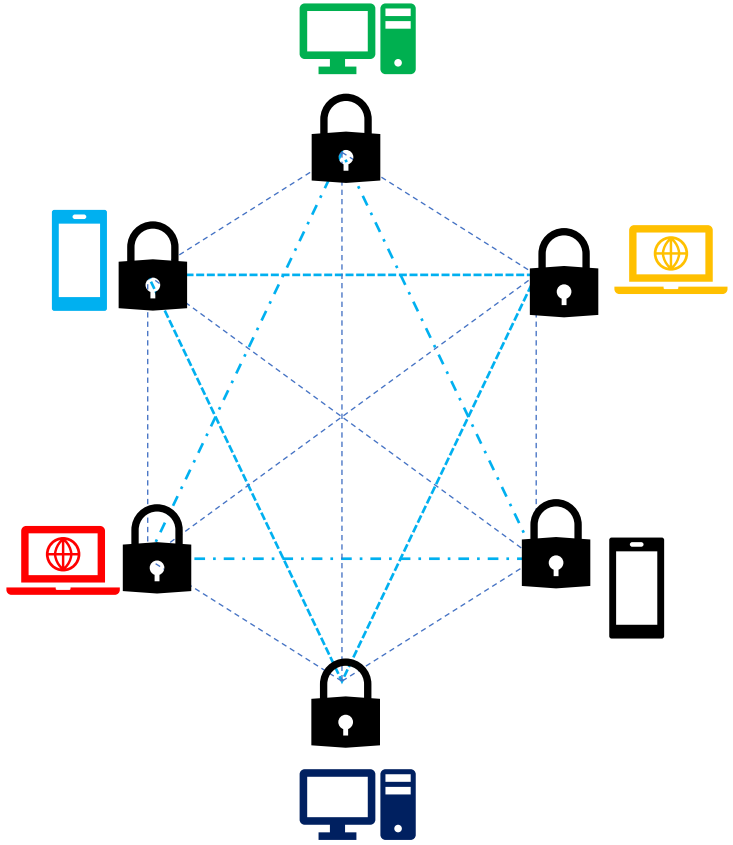


Public vs Private Blockchain Network



Public Blockchain: Permissionless

An open network system where all the nodes can freely access network resources. The ledger is shared and transparent.



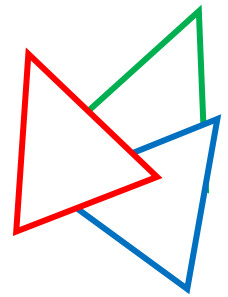
Private Blockchain: Permissioned

A closed network system where all the nodes must be authorised in order to access network resources. User can only join by invitation.

Blockchain Security

- Cryptographic Techniques for Blockchain Security Features
  - Cryptographic hash functions, Consensus mechanisms e.g. Proof of Work (PoW), Digital Signatures.

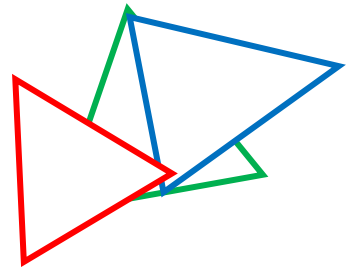
- Advanced Blockchain Dependability and Security
  - Looming issues
    - Scalability
    - No or inefficient confidentiality



Blockchain Security Cont.

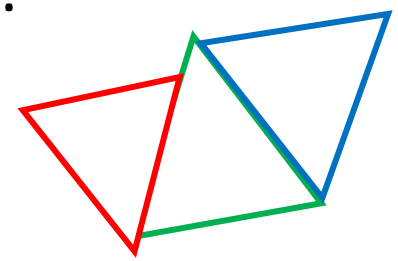
- Establishing Transaction Confidentiality
  - Hyperledger Fabric Channels - implements secure *Channels* between two or more specific network members
  - Multichain Stream Confidentiality – securing data stored on the blockchain *stream* using symmetric and asymmetric cryptography

- Potential solutions in the use of threshold cryptography i.e., Secret Sharing
  - Reduced storage requirements and costs
  - Transaction Integrity



Virtual Private Blockchains

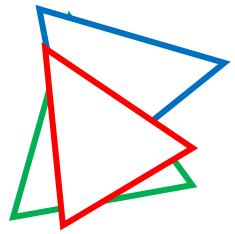
- Definition
  - A mechanism to create a blockchain architecture with properties akin to those of a private blockchain, however leveraging existing public blockchain functionality
- Basic Idea
  - In order to implement a VPBC, one needs to substitute confidential transaction content with pseudo-content or, more specifically, data bits of the originally intended content through information dispersal.



VPBC - Characteristics

- The term “virtual” is justified as a VPBC utilises existing Blockchain functionality and is by nature a Blockchain itself. In particular, a VPBC inherits any built-in, internal Blockchain security mechanisms.

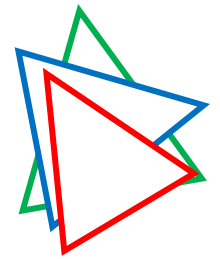
- A VPBC is not visible to other Blockchain users that are not part of it, and it is transparent to its users. This achieves both usability and security, which is a desirable characteristic.



VPBC - Secret Sharing Approach

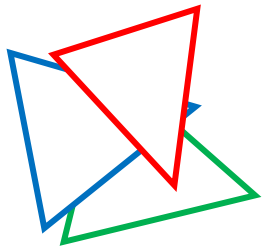
- The idea of secret sharing is to divide given data (the secret ***s***) into ***n*** parts (the shares) in such a way that knowing (at least) ***m*** shares allows for reconstructing ***s***.

- Using the VPBC architecture, consider a Public blockchain where a requested transaction with sensitive transaction information ***t***, requiring protection. Using a suitable ideal (***m, n***)-threshold secret sharing scheme, ***t*** will be shared as ***n*** pieces of information (transaction shares) ***t1***, . . . , ***tn***, and these will be used for the individual transactions, executed on ***n*** independent public blockchains.



VPBC - Secret Sharing Approach Cont.

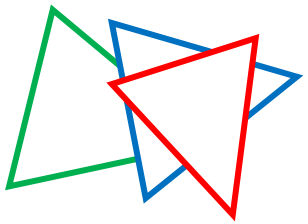
- Resulting shares are random numbers and do not preserve any patterns that might be in the initial secret.
- The recipient, prior to using the scheme, has been informed about the selected blockchains.
- When new transactions occur, a subset of m transactions (which in reality are shares of the real transaction) will be collated and the original secret transaction data can be reconstructed.



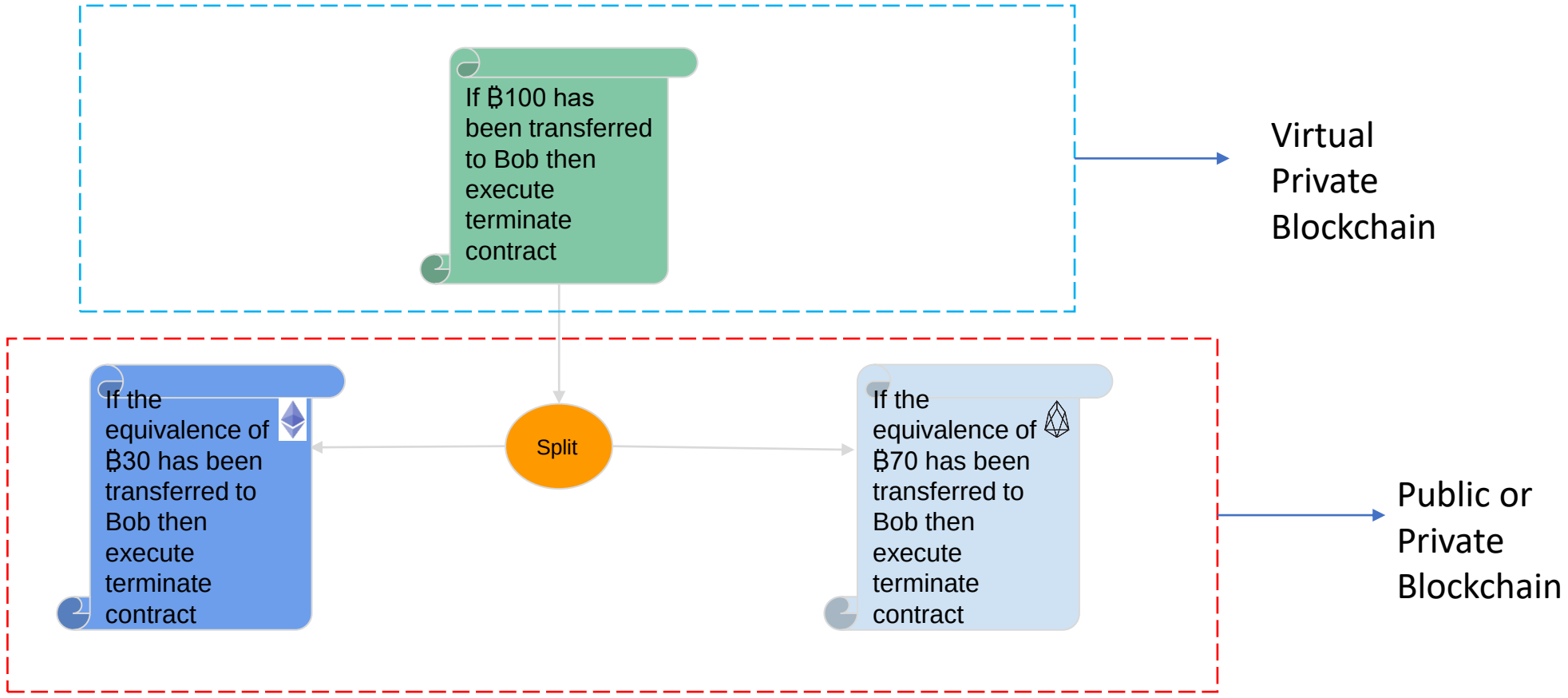
Security Analysis

- Security principles implemented include:
  - Inheritance of Native security infrastructure
  - Security by obscurity
  - Steganography by cover synthesis or modification

- Possible Attacks on the scheme:
  - Brute-force attack
  - Deanonymisation Attack

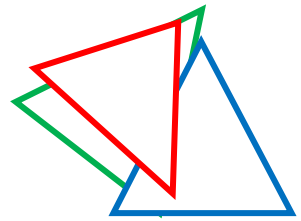


Basic Idea Demo



System Evaluation

- Initial implementation simulations have been done on the Multichain blockchain Platform
  - Two private Multichain blockchain systems (A and B) were set up on different instances of Ubuntu 12.04 LTS servers
  - The Multichain API was used by a separate process, running on a separate node (virtual node C) implementing our Virtual Private Blockchain, where the desired transaction is generated and executed via a smart contract.
  - The transactions on node A and node B are verified by the blockchain, and upon successful execution of both transactions, our system will report a successful conclusion/execution of the virtual transaction.

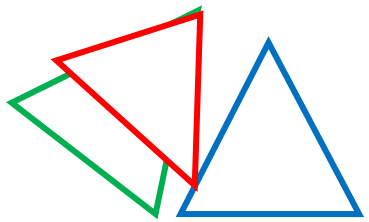


Application of the VPBC Architecture

- Confidential Cryptocurrency transactions
  - Virtual smart contracts for digital Real Estates (Tokenised Physical Assets)
  - Prevention of potential violations of data protection (such as GDPR)

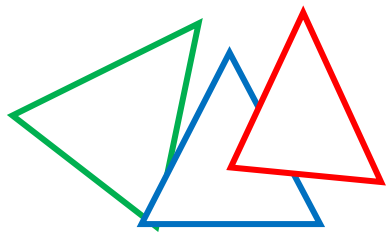
- Higher Education Systems Architectures can be made robust through the adoption of Secure Overlay Blockchain Technologies.

- Introduction of a new Distributed/Decentralised Ledger Technology Taxonomy
  - Vertical and Horizontal Distribution of Permissioned or Permissionless Blockchain Systems.



Conclusion

- A novel Blockchain architecture is introduced by designing a security overlay, spanning across multiple Blockchain implementations.
- The resulting system is referred to as a Virtual Private Blockchain (VPBC) and can be interpreted as a Permissioned Blockchain with vertical (rather than horizontal) distribution of the public ledger.
- Initial security analysis shows scheme is robust against possible known attacks
- Potential real-world applications have been identified and documented



Thank you.