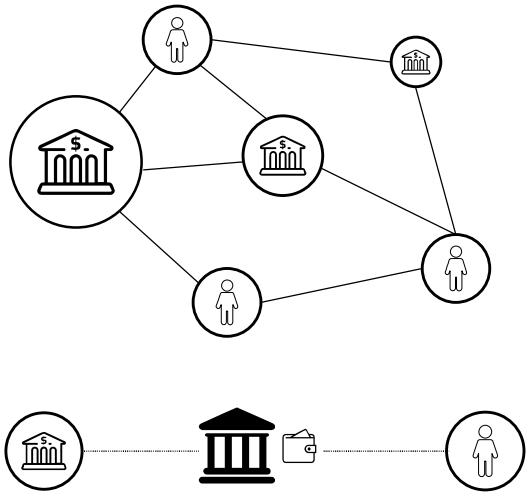
BLOCKCHAIN INTRODUCTION

DARKMATTER

GUARDED BY GENIUS

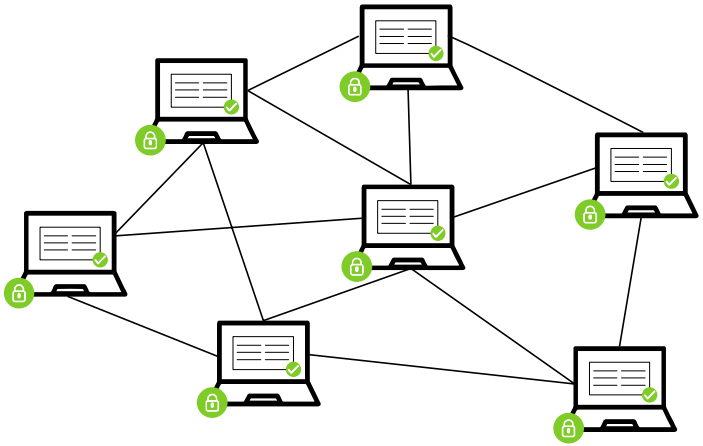
WHAT IS BLOCKCHAIN

Current Financial System



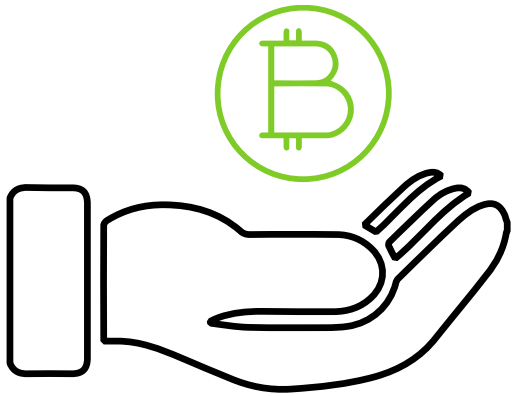
- Central authorities (bank, fed, notary, escrow, etc.) transfer actual value between two parties
- Multiple intermediaries and record-keeping are required to facilitate transfer of assets and create trust

BlockChain System



- Distributed network of computers (nodes) that maintain a shared source of information
- Transaction data is immutable
- Peer to Peer transactions using digital tokens to represent assets and value

BLOCKCHAIN VS BITCOIN



Bitcoin

- A digital currency which was in a lot of ways the first demonstrable use of BlockChain
- A protocol that supports a decentralized, pseudo-anonymous, peer-to-peer digital currency

BlockChain

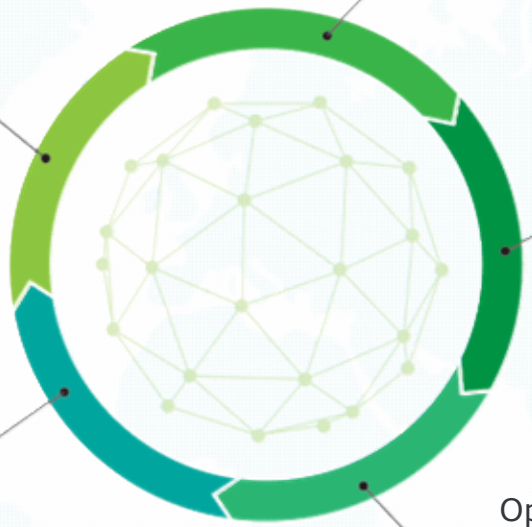
- Distributed
- Secure
- Log file

INTRODUCTION TO BLOCKCHAIN

A **BlockChain** is a distributed secure log file or **shared ledger** with technology to trust transactions without a central authority

Every **viable transaction** is stored in the **shared public ledger**

A **shared ledger** technology allowing any participant in the business network to see the **established (via distributed consensus) system of record (ledger)**



Transactions are placed in **blocks**, which are linked by **one way hashes**

Each **peer address is anonymous** and **multiple addresses** may map to the same transactor

Operates in a **peer to peer mode** and is mostly based on DNS and **"seed nodes"**

WHAT IS BLOCKCHAIN

A Brief Intro:

- **BlockChains are essentially facilitated on a platform of distributed databases with some inbuilt pre-agreed technical and business logic criteria, kept in sync via peer-to-peer mechanisms and pre-agreed consensus algorithms.** These are the BlockChain Ledgers.

- **Data stored on BlockChains are considered Immutable.** Immutable means that something is unchanging over time or unable to be changed.
  - In a BlockChain context, once data has been written to a BlockChain no one, not even a system administrator, can change it. This provides benefits for audit. As a provider of data you can prove that your data hasn't been altered, and as a recipient of data you can be sure that the data hasn't been altered. These benefits are useful for databases of financial transactions.

- **With respect to immutability, the way the data is structured is significant. There are two key ideas: Hashes and Blocks.**

WHAT IS BLOCKCHAIN

A Brief Intro:

- **Hashes**
  - A hash function is a type of mathematical function which turns data into a fingerprint of that data called a hash. It's like a formula or algorithm which takes the input data (any data, whether it's the entire Encyclopedia Britannica, or just the number '1') and turns it into an output of a fixed length, which represents the fingerprint of the data. There are many types of hash functions e.g. SHA-256

  - When you mash the phrase "Hello from Bits on Blocks!" through this function, you get this fingerprint out:

    389f9ef3822e5c88f4b140db82c459064711a52182a3e438b4ebc7ecda62b9bb (SHA-256 hash of the phrase).

  - Two relevant properties of a good hash function are:
    1. It's hard to back-calculate the original data from the hash
    2. If the input data changes in the slightest, the hash changes in an unpredictable way

WHAT IS BLOCKCHAIN

A Brief Intro:

- **Blocks**
  - An important idea in BlockChain is that transactions are bundled into blocks. Blocks contain a number of transactions (e.g. payments) and also some other data including the previous block's hash. As each block includes the previous block's hash as part of its data, a chain of blocks is formed.

WHAT IS BLOCKCHAIN

A Brief Intro:

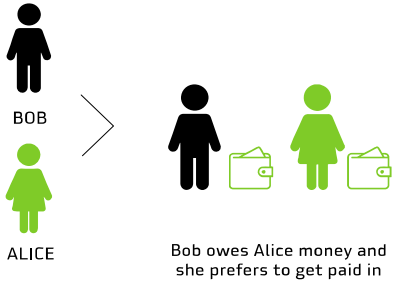
- **Blocks**
  - Creating a ledger of transactions with blocks that refer to previous blocks is a much better idea than numbering pages in a book (in the case of a book ledger).
    - In a book ledger with numbered pages, 1, 2, 3, etc. it would be easy to tear out page 40 and replace it with another page 40 with slightly different transactions.
    - The book's integrity remains intact, with pages 39, 40, 41 becoming 39, 40, 41 – no change. Also there is nothing in the page number '40' that reflects any of the content in that page and the ordering of the pages is implicit from the page numbers.
  - However in a BlockChain, instead of referring to block numbers, blocks are referenced by their hash and each block explicitly specifies which block (hash) it is building on.
    - So, blocks are explicitly ordered by reference to previous block hashes, which reflect content, instead of being ordered implicitly by a numbering system (1, 2, 3) which is content-agnostic.

WHAT IS BLOCKCHAIN

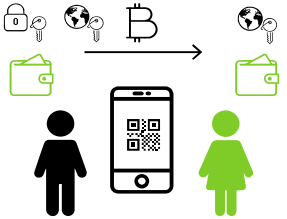
A Brief Intro:

- **Blocks**
  - **Key points**
    - Each block's hash is derived from the contents of the block
    - Each block refers to the previous block's hash, not a sequential number
    - Data in a BlockChain is internally consistent, that is you can run some checks on it, and if the data and hashes don't match up, there has definitely been some tinkering.

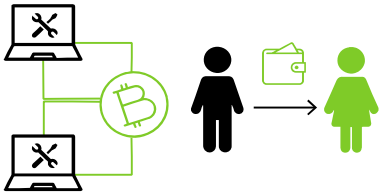
TRANSACTION FLOW FOR BITCOIN (ANONYMOUS BC)



Bob owes Alice money and she prefers to get paid in bitcoin

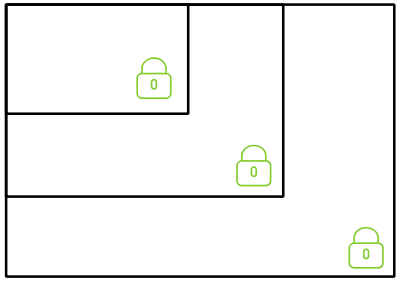


Bob pays Alice in bitcoin using the private key associated with his Bitcoin wallet; Alice is "identified" through her Bitcoin wallet public key

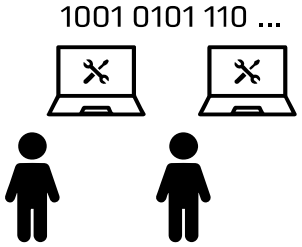


Miners on the public Bitcoin blockchain are alerted and verify that Bob has enough funds to pay Alice

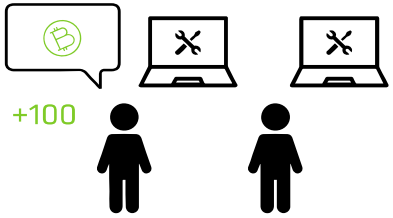
Payment



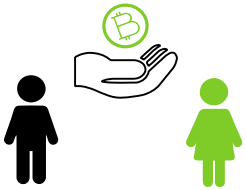
Bob and Alice's transaction is added to the Blockchain. Every subsequent block added further increases the security of the previous blocks



Miners collate all unincorporated transactions into a block, and race to solve a computationally difficult problem



The miner that solves the problem publishes the block, which is then added to the Blockchain; the miner is awarded 100 Bitcoins and transaction fees



Bob and Alice receive confirmation that their transaction has been executed

Verifying Transaction / Mining

Payment

BLOCKCHAIN BENEFITS OVERVIEW

KEEPING SECURE RECORDS	• **Records and validates each and every transaction made in a cryptographic manner**
	  • Multi-Signatures [public key cryptography, specifically ECC due to key-strength and shorter keys]
	  • Encrypted Communication [in particular for generalized B2B transactions]
	  • True Non-Repudiation: Transaction unlinkability while incorporating identity management and auditability

EFFICIENT VALUE TRANSFER	• **BlockChain mining discards the need of any third-party or central authority for P2P transactions needed to transfer value between two parties:** *Process and Cost Efficiency; Reduced internal risks; Mitigate Man in the Middle*
SMART CONTRACTS	• **Decentralization of the technology and distributed Ledger for smart contracts development, exchange and signature** • **Transfer over Internet by anyone with computer or smart phone**

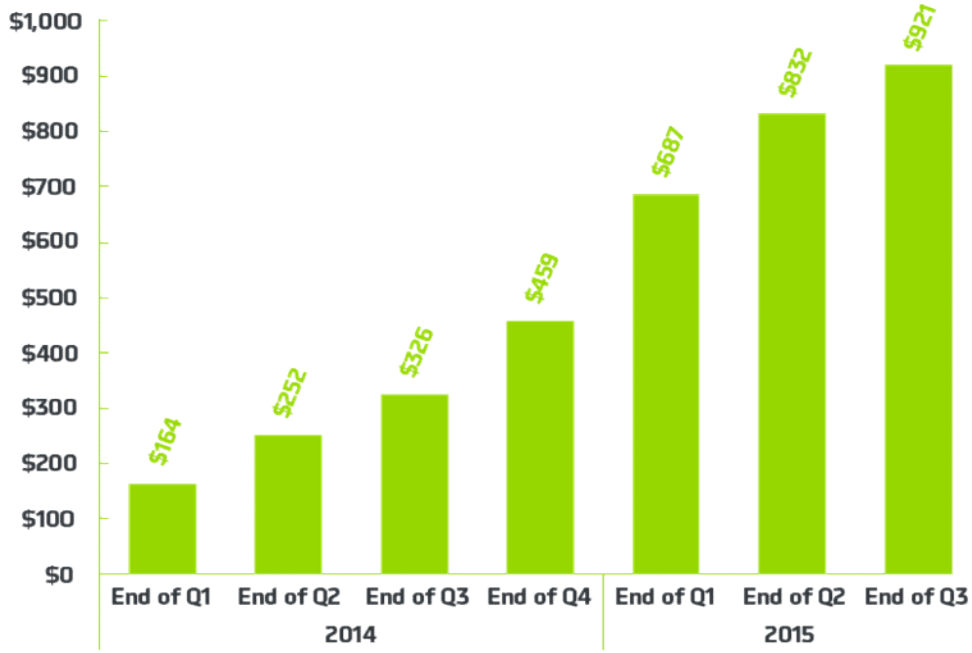
BLOCKCHAIN CHALLENGES

Challenges

- **BlockChain significantly alters the need for trusted third-party authentication through a financial institution**
  - Challenges of legacy infrastructure
- **Challenges in understanding the technology**
  - Complex cryptosystems
  - Decentralized cryptosystems
- **Attacks on Cryptosystems**
- **Government backing and standards are currently in exploratory phase only**
- **Can facilitate money laundering, crime**
- **Currently cannot support a large number of transactions and is not fast enough**

- **Increased Investment**

Cumulative VC Investment in Virtual Currency & BlockChain Tech (USD millions)



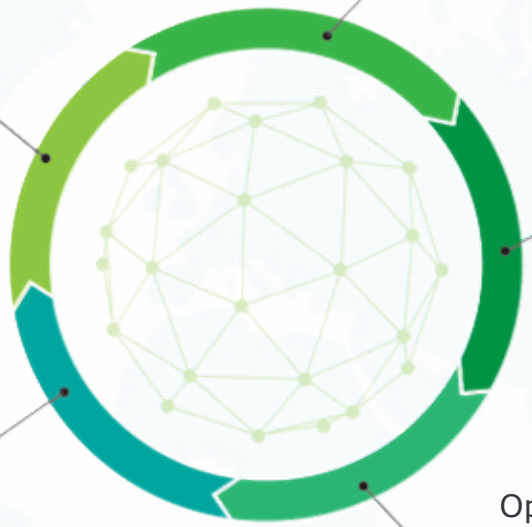
OVER $1 BILLION HAS BEEN INVESTED BY COMPANIES INTO BLOCKCHAIN TECHNOLOGY

PERMISSIONED BLOCKCHAINS

A Permissioned **BlockChain** is a distributed secure log file or **shared ledger** where the ledger is maintained in a private and secure walled garden of participants

Every **viable transaction** is stored in the **shared private ledger**

A **shared ledger** technology allowing any participant in the business network to see the **established (via distributed consensus) system of record (ledger)**

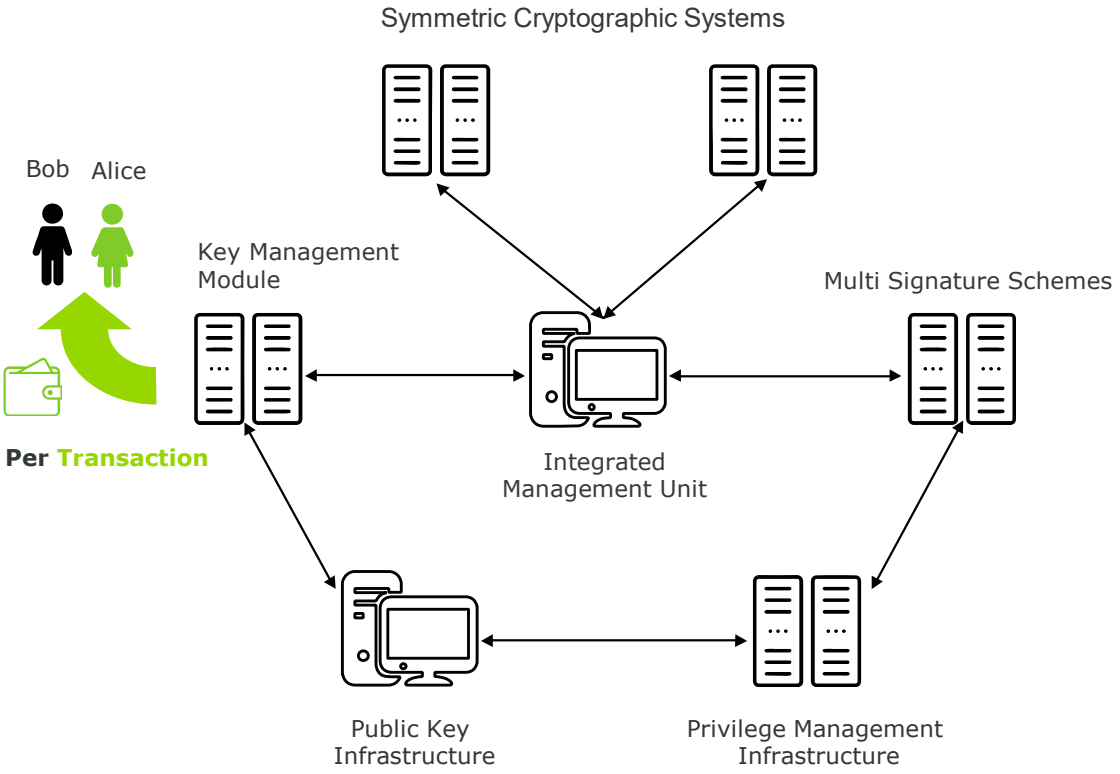


Transactions are placed in **blocks**, which are linked by **one way hashes**

Each **peer address is discrete and known** and **access** is controlled by a common trust infrastructure of PKI based trust anchors

Operates in a **peer to peer mode** but among a known community of private databases or ledgers

PKI-ENABLED PERMISSIONED BLOCKCHAIN



Transaction Level 2:
Crypto Infrastructure: Threshold Crypto Custom variants utilized and security levels to meet / exceed what is openly available

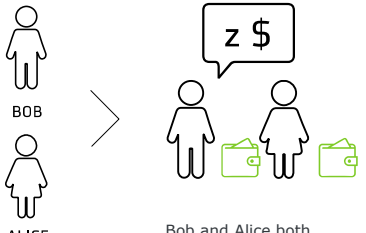
Transaction Level 1:
Key Management and Multi-Signatures Structure: Introduces non-circumventable hierarchical auditability and unlinkable certificates

Block Chain Infrastructure Enablement Level:
Public Key Infrastructure (PKI): Vetted and load-balanced means to bridge external- and on-chain- services

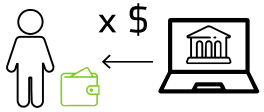
Privilege Management Infrastructure (PMI): Leverages existing Identity Providers and Attribute Authorities through interoperable import

E.g.: **DarkMatter Seamless SDK** that integrates into **your application;** standardizes **BLOCKCHAIN** Security Schemes and Crypto Algorithms based on ***Extended Functionality Version of Hyperledger Fabric***

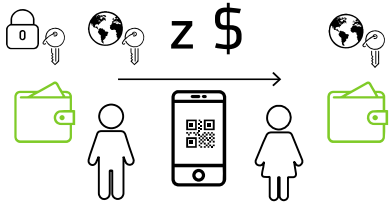
TRANSACTION FLOW EXAMPLE FOR PERMISSIONED BLOCKCHAIN



Bob and Alice both have BlockChain wallets on their mobile devices. Bob owes Alice z dollars

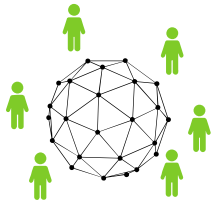


Bob's bank has deposited x dollars into Bob's BlockChain accountID_B from an off-chain bank account



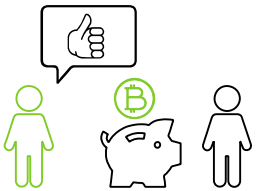
Bob gets a key agreement transaction certificate for Alice's accountID_A, and extracts a transaction certificate and corresponding private key from his wallet in order to sign a transaction that transfers z dollars from accountID_B to accountID_A

[secured using the public key from Alice's key agreement transaction certificate and public key for Validator group]

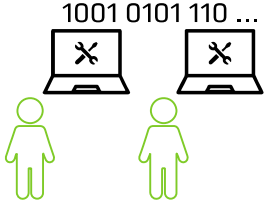


Bob sends the transaction to a trusted Validating Peer (VP) that broadcasts the transaction to all other VPs

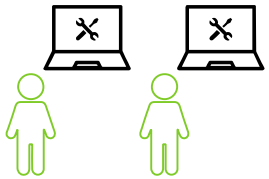
Payment



Each VP checks in state table That z ≤ accountID_B balance

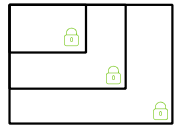


All VPs reach consensus (using PBFT algorithm) on the order to follow to execute the transactions



Each VP independently executes the transactions and incorporates them (as well as the state values that result from execution) into a new block – and the state table is updated

Bob and Alice receive confirmation that their transaction has been executed



Bob and Alice's transaction is added to the BlockChain. Every subsequent block added further increases the security of the previous blocks

Verifying Transaction / Consensus

Payment

DOES IGTF NEED BLOCKCHAINS?

A brief look at BlockChain applications in various industries…

ELECTRONIC MEDICAL RECORDS AND HEALTH INSURANCE: MAKING SYSTEMS INTEROPERABILITY A REALITY

PROBLEMS WITH HANDLING MEDICAL RECORDS TODAY

Lack of interoperability:

- Current systems generally disconnected from one another – resulting in significant cost and delay (e.g., due to inefficient manual processes) when patients change healthcare providers
- Payer and provider systems are disconnected from one another as well

Attack Surface:

- Centralized healthcare data (maintained in on-site repositories powered by physical servers or on an IT cloud) and heightened vulnerability to security breaches (theft as well as potentially undetected modification/falsification)

ROLE OF BLOCK CHAIN

Enablers

- Hospital and Med. Centers Visit-Management
- Peer to Peer Insurance System Mgmt.
- Medical Data Collection and Quantification
- Peer-based Mediation and Legal System
- Paying Ransom when Access is denied

Linkages

SMART SOVEREIGNTY AND PROVENANCE

Counterfeit Product Detection

=

```
79054025
255fb1a2
6e4bc422
aef54eb4
```

- Decentralized detection and control of the counterfeit drugs problem
- Smart tracking of quality of product and manufacturing
- Tagging enables physical objects to be represented virtually; tags (e.g., QR codes) can be securely hashed onto a BlockChain
- Tags/codes used for counterfeit product detection today
- BlockChain as: world-wide tracking with auditability and without undue infringement of privacy

Reduced Criminal Activity

- Code hidden at point of sale
- Revealed code checked for legitimacy & "freshness*"
- Alteration of code destroys value
- Protect against code reuse

SMART CONTRACTS

Sign lease and insurance contracts: DocuSign → **Pay:** VISA **With:** Bitcoin

Blockchain ✓

Cryptocurrency ✗

HEALTHCARE BARRIERS: MANAGING CONTRACTUAL CORRECTIONS

HEALTHCARE BARRIERS	
Barrier Root Cause	“Many hospitals are unwilling to digitally sign some documents because the codes that HIPAA mandates may need to be manually corrected, and those corrections will break a digital signature.”
Surmounting the Barrier	Instead, such modifications can (and should) be captured in additional digital signatures/follow-on transactions

HEALTHCARE BARRIERS-2: PATIENT MANAGEMENT OF OWN DATA

HEALTHCARE BARRIERS	
Barrier Root Cause	"How to achieve the HealthCare Industry objective of Patients and Consumers 'owning' and controlling their own Health related data?"
Surmounting the Barrier	Permissioned BlockChains with strong PKI based authentication of Identity would enable the Patient/Consumer to reliably control and manage their own HealthCare records

JURIDICAL BARRIERS: MANAGING JURISDICTION-SPECIFIC PRIVACY LAWS

BARRIERS	
Barrier Root Cause	Recording certain types of transactions in a public ledger may be disallowed in a given country because of privacy laws
Surmounting the Barrier	▪ Access to confidential data may be restricted within a permissioned BlockChain ▪ A public BlockChain may include one-way hashes of confidential data, where access to that data is controlled; the database(s) containing such data can be (partially or totally) purged, if necessary **Also to think about: What about "Right to be Forgotten" ?** ▪ *Does purging the data from the associated off-chain database meet this requirement?: If someone re-presents such data, they can prove that it matches the corresponding immutable transactions on the BlockChain*

FINANCIAL TRANSACTION BARRIERS: MANAGING TRANSACTIONAL RECOURSE

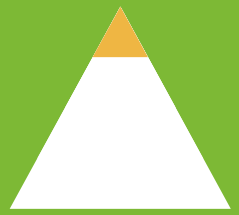
BARRIERS	
Barrier Root Cause	"It's possible to undo lots of transactions in our current legal environment. Reversing charges on credit cards is possible, for example, and is a desirable feature of our current system."
Surmounting the Barrier	▪ Immutability does not imply inability to reverse a transaction via a follow-on linked transaction ▪ BlockChains can be made interoperable with legacy systems such as credit card processing

PERMISSIONED BLOCKCHAINS FOR IGTF?

CHOOSING THE RIGHT BLOCKCHAIN SCHEMES: *ARCHITECTURE IS KEY*

Why IGTF might consider adopting *permissioned* BlockChains - *instead of permission-less BlockChain that does not address abuse prevention or suitable recourse*

Universality



- Collects transaction records from diverse set of systems

Immutability and Non Repudiation

- Append-only and tamperproof qualities create high-confidence audit trail
- Rigorous incorporation of identity management in order to meaningfully enable transaction non-repudiation

Privacy/Confidentiality

- Ensure authorized user access and selective disclosure

Authentication and Authorization

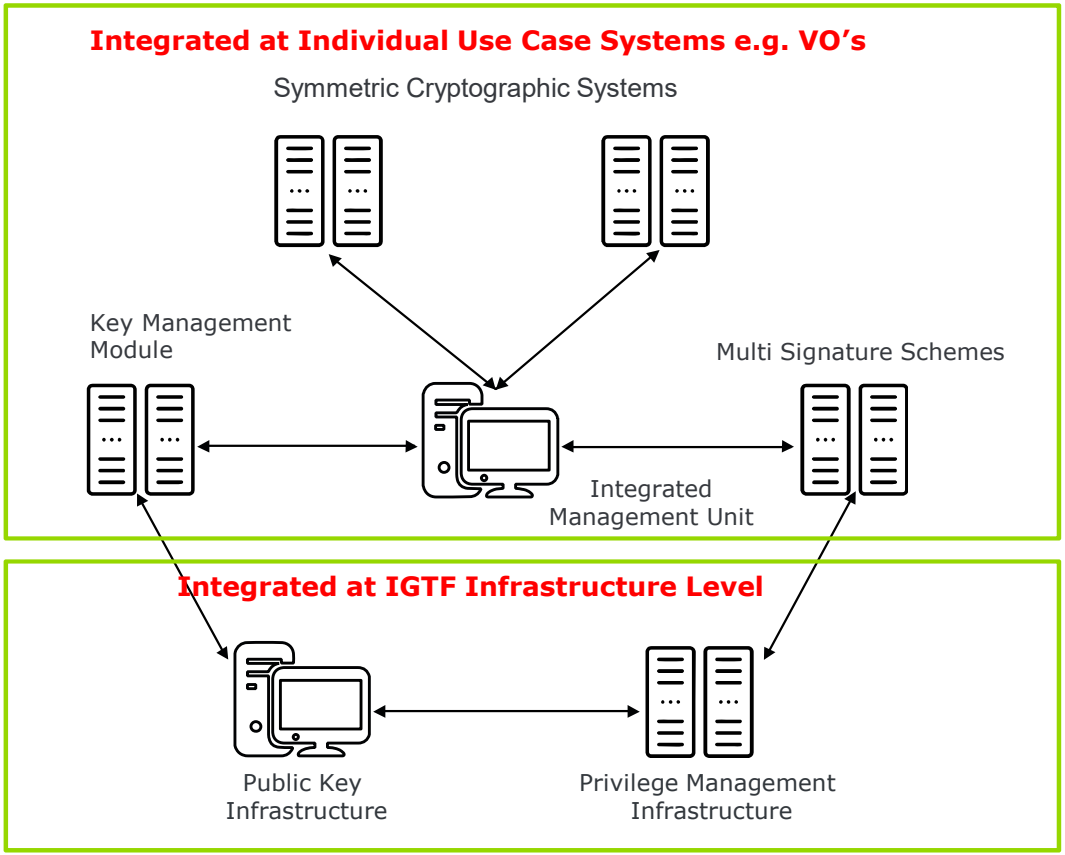
- Derived from PKI standards-based ID management

NATURAL BLOCKCHAIN + IGTF INTERSECTIONS

Permissioned BC potentially has a place in IGTF:

- **What are the natural intersections for Permissioned BC and IGTF?**
  - Permissioned BC is dependent on strongest authentication of actors within the system, to ensure non-repudiation on transactions, just the same as Grid/Supercomputing
  - Digital Signing of transactions for confidentiality and integrity purposes (in addition to Identity/Access controls identified above) makes PKI the natural (the BEST) solution for permissioned BC, same as is used for IGTF
  - BC Nodes should be run on strongly audited and securely operated infrastructure, which is what IGTF requires of Authentication Providers, and potentially to a lesser degree the Attribute Authority providers (I can be convinced of the latter perhaps)
  - Global trust infrastructure at known levels of assurance is already in place for IGTF, this could potentially allow easy deployment of global BC
    - But do we need a new level of hardware based certificates for BC operations?
  - What are the natural items that an IGTF BC infrastructure would be need for?
    - Global Identities? (Individuals, nodes, services, LRAs?)
    - Global Virtual Organizations with added benefit of transparency?
    - Distribution of anchors and CRLs via BC?

ACHIEVABLE PERMISSIONED BLOCKCHAINS



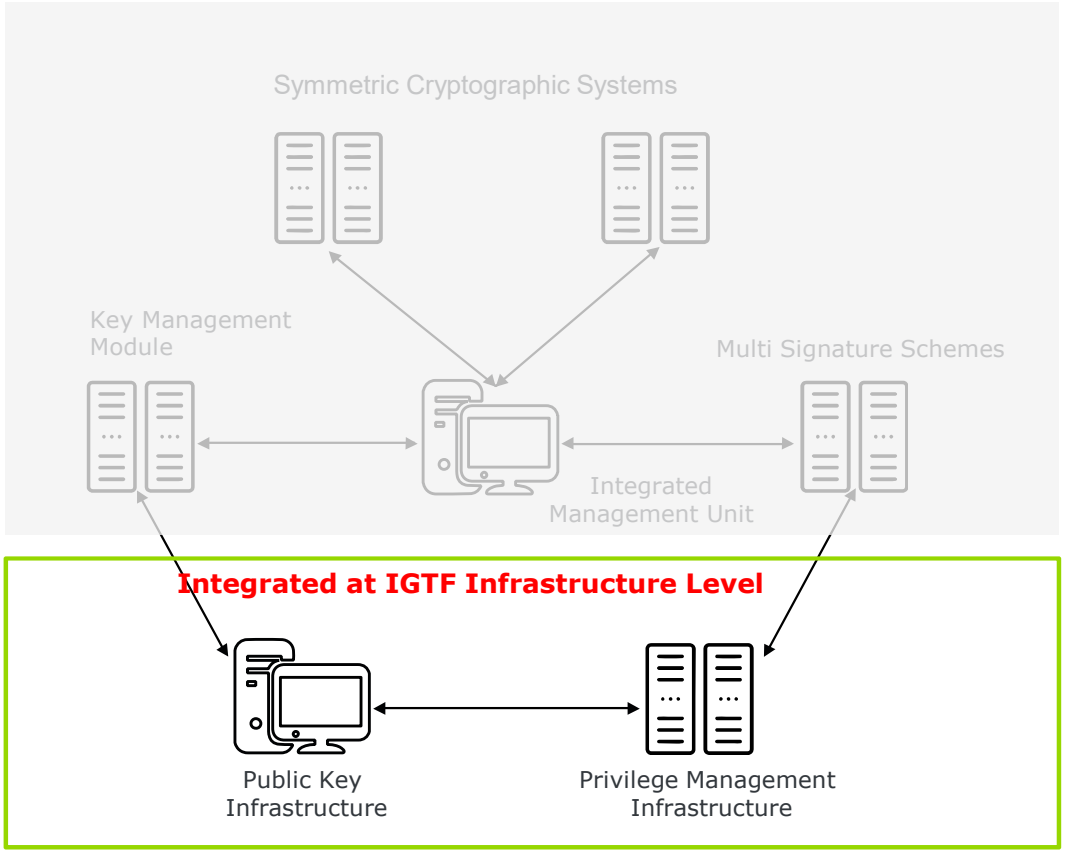
Transaction Level 2:
Crypto Infrastructure: Underlying crypto algorithms (state-of-art and customized) are key Crypto Schemes should ensure interoperability and a multi-faceted audit capability within a distributed trust framework while maintaining resistance against traffic analysis

Transaction Level 1:
Key Management and Multi-Signatures Structure: are critical

Block Chain Infrastructure Enablement Level [Based on Hyperledger-Provided Framework]:
Public Key Infrastructure (PKI): Achieved through a hybrid PKI- and BlockChain- model

Privilege Management Infrastructure (PMI): Proper Node (Client) and Membership Services (Privilege Management Servers) to be designed

INFRASTRUCTURE SCALABILITY IS KEY



IGTF adopted infrastructure architecture could provide the distributed ledgers where BlockChains are kept, with a number of potential use cases.

Any adopted PKI trust infrastructure architecture should support **multiple Certificate Authorities** audited to common Trust policies either as a hierarchy of scalable servers/services or by splitting the responsibility (partitioning) into a set of (relatively) disjoint (distributed) sets

Goals achievable via potential expansion of existing IGTF framework and DarkMatter-enabled Permissioned BlockChain SDK's integrated in existing architectures

DARKMATTER + IGTF + BLOCKCHAIN

Questions?

Scott.Rea@DarkMatter.ae

THANK YOU

DARKMATTER

GUARDED BY GENIUS