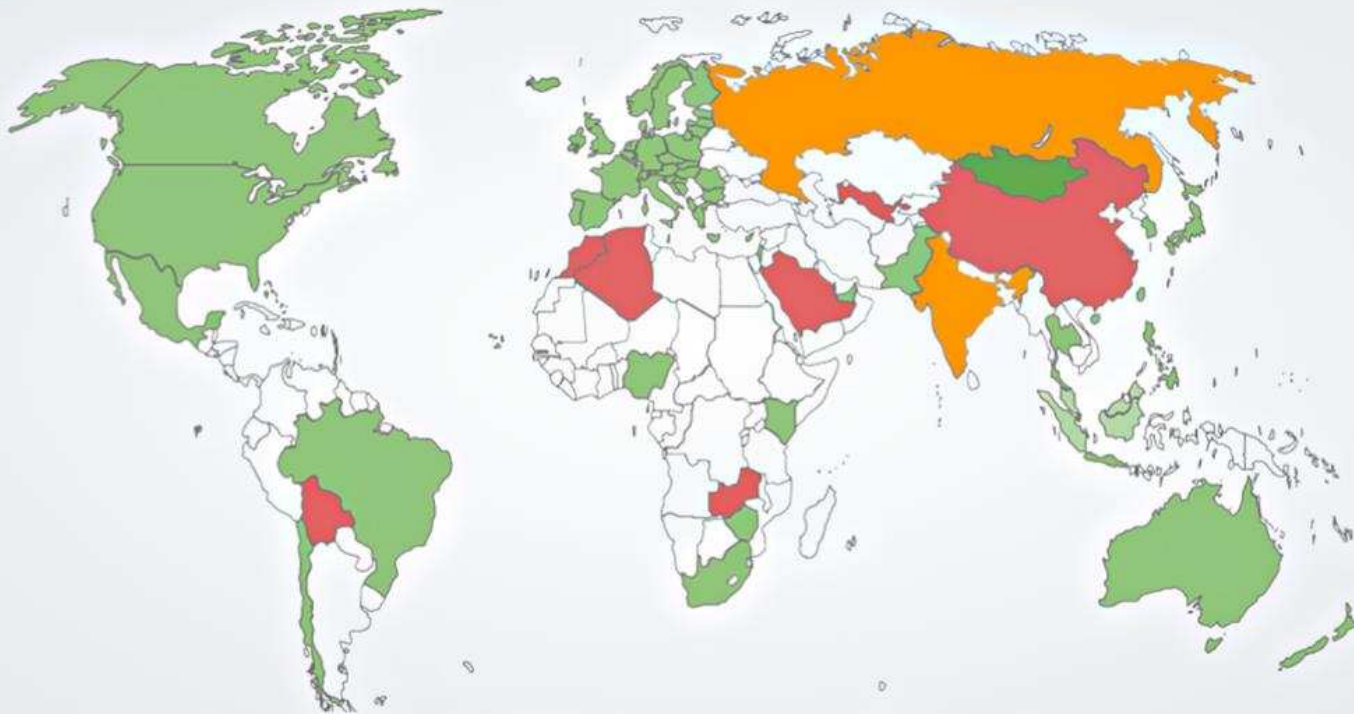

Forensic Accounting: ***Blockchain Technology Promise, Methods, Hurdles & Way Forward***

Lakshmi Rao & Gaurav Mehta



Crypto Regulation World Map



Red: Cryptoassets generally prohibited

Green: Cryptoassets are generally allowed

Yellow: Cryptoassets are restricted

White: Regulation pending

Tip of iceberg

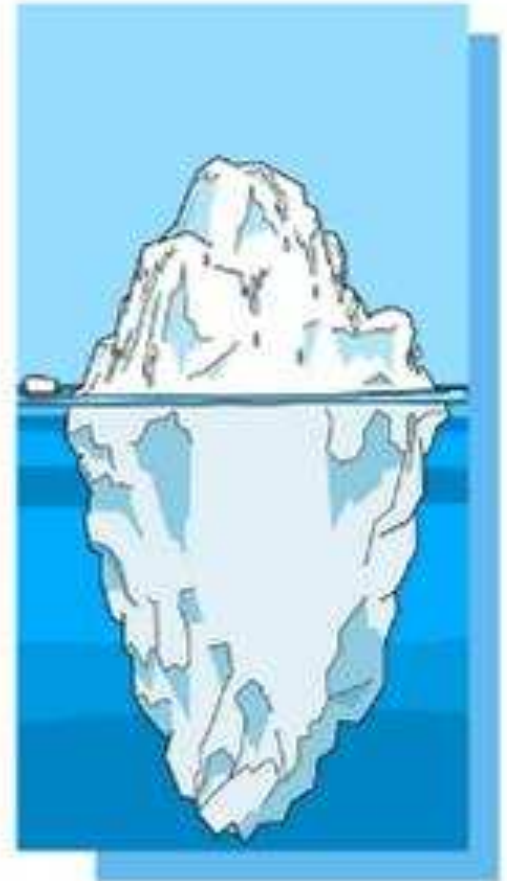
Innovation of Blockchain

Reimagined Bookkeeping, Accounting & Auditing

Advent of Third Party Bookkeeping

Implication beyond Currency & Finance

And... Reliable Source of Truth?



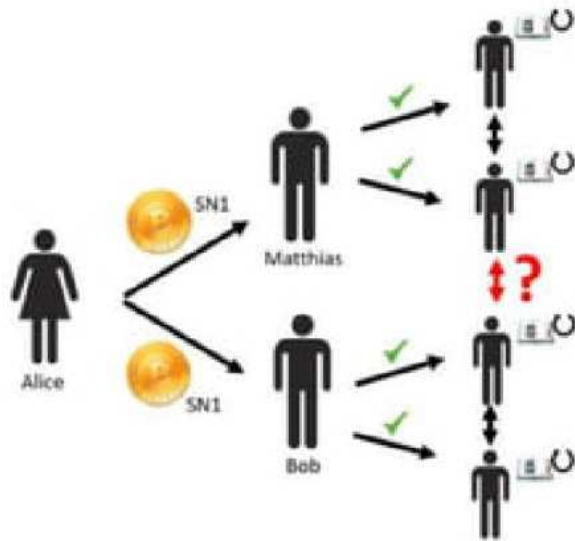
Billion dollar question of digital world:
*How to prove something existed at some point of
time or belongs to someone?*

Technically?

A for Apple, B for Blockchain

- ✓ Too Simplified: A chain of blocks of information – a log or “ledger”
- ✓ Comprehensive, timestamped, updated in real-time, encrypted & immutable
- ✓ Public, Private & Hybrid Blockchains
- ✓ Prominent Use case: Cryptocurrency, Smart Contracts, Data Management, Intellectual Property Protection and evolving

Problem of Double Spending in Digital World



The double spend problem:
Preventing someone making a purchase with digital cash from reusing the same token to purchase again

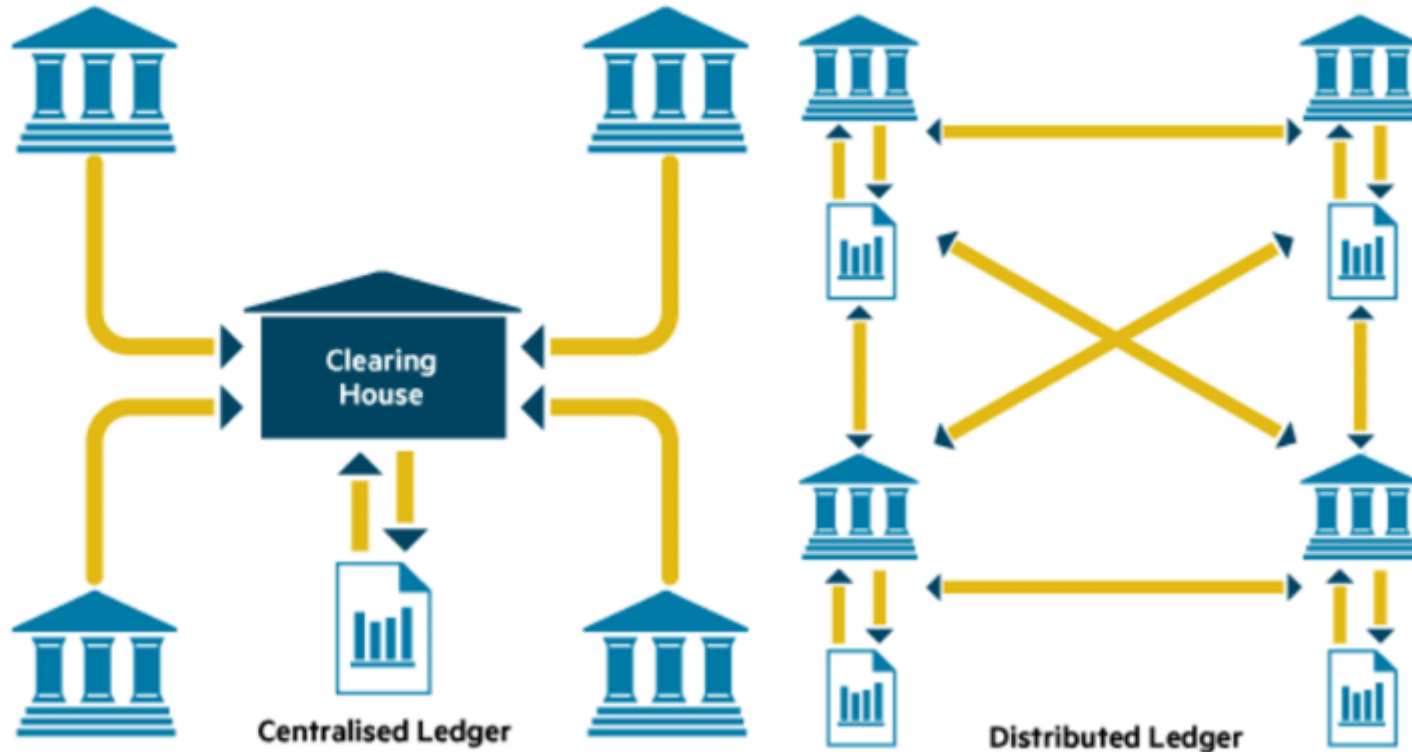
Payment System/Trust System

- Bank transfers; Slow, Expensive
 - Western Union slow and 7% charge
- Paypal: Expensive and not universally available



Embedding distributed ledger technology

A distributed ledger is a network that records ownership through a shared registry

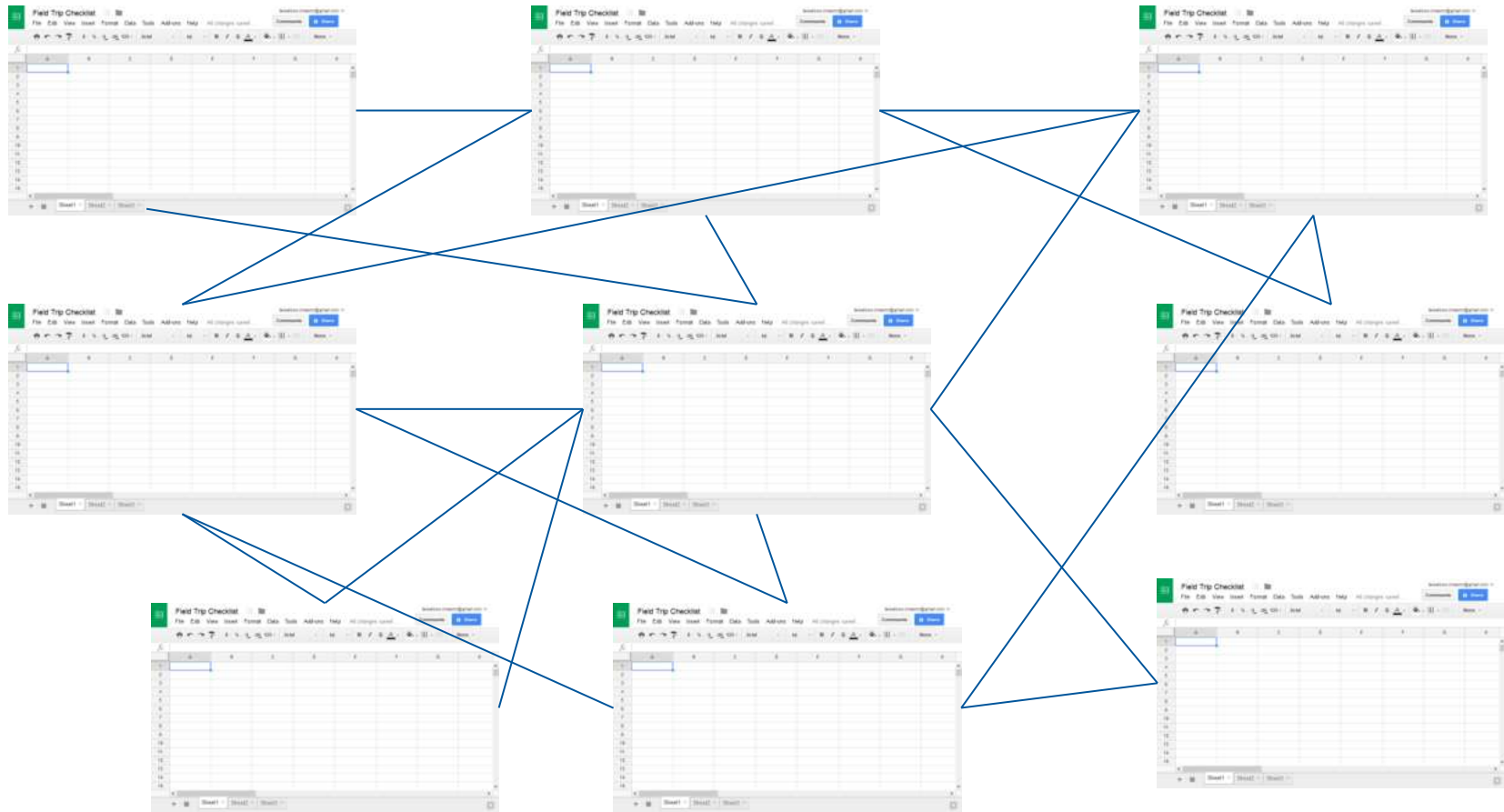


Source: Two examples of ledgers: a centralized and a distributed one. From 10ZTalk.

What is Blockchain?

“The Blockchain is an incorruptible digital ledger of economics transactions that can be programmed to record not just financial transaction but virtually everything of value.”

Don & Alex Tapscott, Blockchain Revolution 2016



How does it work?

1. Picture a google spreadsheet.
2. Duplicated by 1000's of people across world
3. Listening for changes and validating and updating every 10 minutes (Bitcoin Blockchain)
4. If information matches with local copy – Vote yes else no.
5. No single node or centralized version

One party requests a transaction.



Requested transactions are funneled into a P2P network and broadcast to each individual computer (or node).



Individual nodes receive the request and validate the transaction using an algorithm.



Once the block is added to an existing chain, transactions are complete and permanent.



Approved transactions are represented as blocks and added to a public ledger.

**What is incentive for people
copying spreadsheet on computer
and validating transactions?**

Why?

What are reward points?

Definition 1: Hybrid of money, stock and asset class.

Definition 2: Digital Gold or Gold 2.0 which can never be more than 21 million.

Definition 3: Decentralized currency which is based the rule of mathematics.

Definition 4: Technology innovation that reimagines asset class and disruption of money and payment infrastructure across the world with core philosophy of de-monopolizing money printing business of government.



Sweet Conclusion



TECHNOLOGY: A PROTOCOL

pro-to-col: (computer science) a set of rules or procedures for transmitting data between electronic devices, such as computers



INTERNET
Internet Protocol
Suite (TCP/IP)



WEBPAGES
(HTTP)



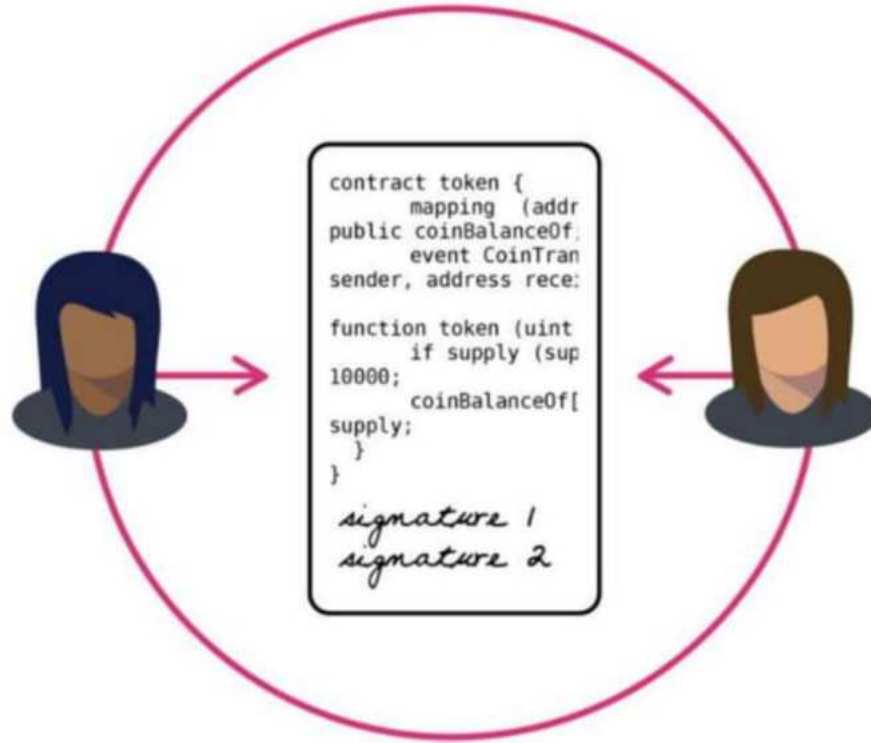
EMAIL
(SMTP/IMAP)



VOICE
(VoIP)



BITCOIN
(BtcP)



Contract Deployed on Blockchain?

How does a **SMART CONTRACT WORK?**



Pre-Defined Contract

Terms and conditions are agreed by all the parties involved.



Events

Execution of the contract is triggered by an event.



Execution

The smart contract is executed automatically.



Settlement

All the settlements are executed quickly and efficiently.

Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets*, 1996:

"a set of promises, specified in digital form, including protocols within which the parties perform on these promises"

To Question:

- Do lawyers, industry stakeholders and technologists understand each other when they use this term?
- What are the key constituents of a smart contract?
- Can traditional (natural language) contracts be adequately translated into computer code, and can computer programs themselves represent a legally binding contract?

And of course:

"Is there any reason to think that smart contract means less work for in-house counsels thereby leading companies to rely less on lawyers? Or does it present more opportunities?"

WHAT ARE SMART CONTRACTS

- A computer protocol that can self-execute, self-enforce, self-verify and self-constrain the performance of its instructions.
- Usually part of a decentralized (blockchain) application.
- Popular examples – Bitcoin, Ethereum (Solidity), Ripple.

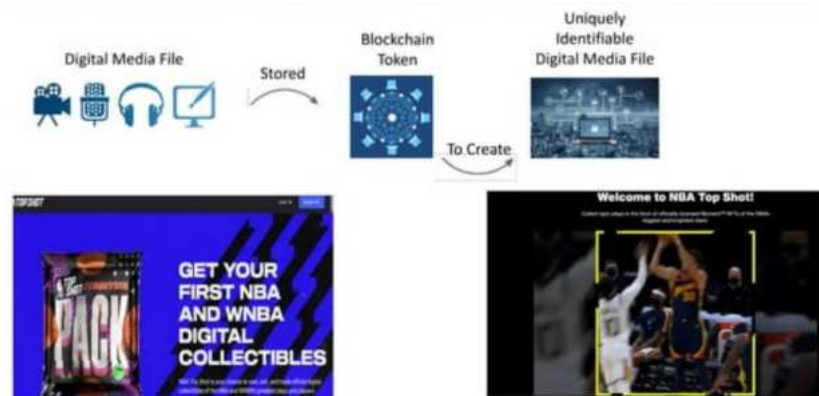
EVALUATING EXISTING REGULATORY REGIMES

- Global regulatory regime – Recognised and defined in certain jurisdictions – State of Arizona, USA.
- Indian statutes – Contract Act, Evidence Act, Competition Act, Information Technology Act – now the Data Protection Bill.

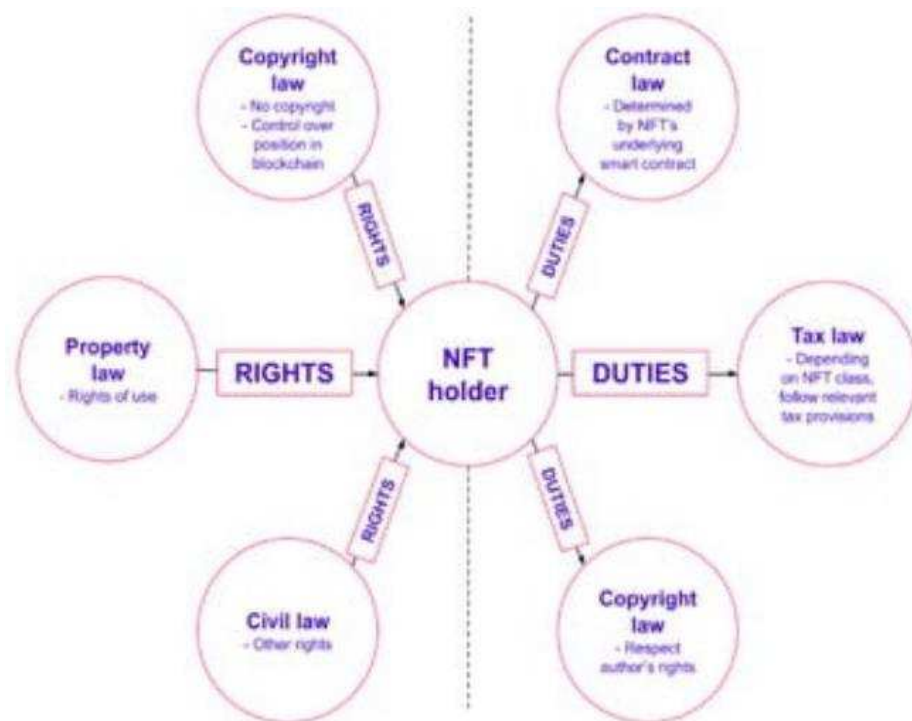
ADOPTION OF SMART CONTRACTS

- Why - certainty, speed, direct communication, low costs, fraud reduction, immutable and tamper-proof.
- Contract formation, identification of parties, governing law and enforceability, dispute resolution.
- Costs and liability.

- **Corporate and Regulatory Filings.** A “smart filings” to automate the release or renewal of regulatory (RoC, RBI, Stock Exchanges) filings, increase the speed of regulatory record searches and reduce errors, fraud, and operational costs; “smart records” system to automate retention and destruction of archival documents.
- **IPR Management.** Indisputable records for rights on patents, trademarks, and copyrights, with an irreversible, secure, time-stamped, and therefore reliable way to track first use; management of licensing rights on digital assets, royalty payments etc. - images, video files, audio recordings, and other digital content of photographers, musicians.
- **Public Record Management and Notarisation.** Secure and streamlined management of birth and death certificates, driving licenses, professional licenses, registrations, passports, visas etc. Apps like Stampery (integrated by Microsoft), to create a document’s digital fingerprint, validating time of creation, ownership and independent verifiability.
- **Dispute Resolution and Criminal Cases.** Secure, immutable and transparent platform for capturing identities and agreements of parties negotiations and terms of resolution; database of availability and expertise of qualified third-party mediators. Sharing and tracking of criminal charges, with law enforcement, courts, attorneys etc. having access.
- **Land Registry and Title Deeds.** Reliable records of property titles, deeds and ownership changes as they occur, with property owners, banks, insurance companies and municipalities having access, reducing future title search time and increasing transparency. Eg., Government of India’s Land Information System to secure land details.



Virtual Goods (Digital Goods/Wearables)



Delhi govt clears way for FSL to use blockchain technology against evidence tampering

The move is in line with the government's policy to plug tampering of evidence collected from crime spot.



ETGovernment

Updated On Jan 27, 2023 at 04:01 PM IST



The use of blockchain technology will not just ensure immutability of records but will further help in procuring much reliable digital evidence with effective audit trail capabilities.

In a latest technology adoption move, the Delhi government is reported to have cleared the use of blockchain technology by the Forensic Science Laboratory (FSL) to protect evidence. The move is in line with the government's policy to plug tampering of evidence collected from

<https://government.economictimes.indiatimes.com/news/technology/delhi-govt-clears-way-for-fsl-to-use-blockchain-technology-against-evidence-tampering/97373749>

BUSINESS 31 JANUARY 2023

Wahid Pessarlay

India's New Delhi deploys blockchain to streamline criminal investigation process

City officials of India's capital New Delhi have [announced](#) the use of blockchain or distributed ledger technology (DLT) in criminal investigations, which experts are calling a pioneering move.

New Delhi's government deployed [blockchain](#) in its Forensic Science Laboratory (FSL) to ensure that evidence obtained from crime scenes is stored using distributed ledgers to prevent interference, the Times of India reported. Officials cite the inherent transparency of DLT as a major reason for choosing blockchain over other technologies. They stated that the

The evidence is in: Chinese courts use judicial blockchain platform to store data



Image: Envato Elements

China's judicial blockchain platform has stored more than 2.6 billion pieces of evidence, a Supreme People's Court spokesman said at a press conference on Thursday, according to a [report](#) by the local media Legal Daily.

<https://forkast.news/headlines/china-courts-judicial-blockchain-platform/>



Use Cases

Applied in number of business vertical and use cases

- **Timestamp**
- **Provanance**
- **Chain of Custody**
- **Tokenization of assets**
- **Credentials, Certificates**
- **Land Records, Bonds**
- **More ongoing experiments**

\$1.5 trillion

Trillion dollar economy - Exchanges, NFT (IP), Decentralized Finance
(DeFi) & Many more

—

Blockchain auditing & forensics **mandatory skill** **for future?**

Comment Yes/No

What do you mean by Forensic Auditing of blockchain?

- Reading blockchain data, Smart Contracts or any other functional program or feature deployed on the blockchain
- Gather information from the blockchain analysis
- Inference of those discovered information to achieve goals
- Using gathered information to technically supplement XYZ claims
- Majority today: Auditing cryptocurrency transaction for variety of purposes.

Where do we start?

Trillion dollar economy - Exchanges, NFT (IP), Decentralized Finance
(DeFi) & Many more

How do acquisition happen?

- Mining – Run advance computer 24*7 and make bitcoin with your computing power
- Purchase – Find someone or exchange. Hand over currency and convert to Bitcoin
- Service – Provide services and get paid in Bitcoin. Sell goods and get paid in bitcoin
- Frauds, Scams and other illicit activity
- Other cases like NFT – It can be website or P2P.

What happens at Exchange?

- Customer buys/earn cryptocurrency from various sources and deposits on exchange
- Customer purchase cryptocurrency and moves off the grid
- Customer purchase cryptocurrency and transfer to international accounts or party
- Customer creates account on international exchange transfer funds and purchase crypto there.
- Customer purchase crypto, move to another exchange, buy another currency, move back crypto to first exchange – arbitrage and layering
- Customer purchase crypto and convert to another crypto and pay for illicit activities

How exchange work?



What is wallet?

Email Address

Password

Email Service Provider – Gmail,
Yahoo, Hotmail etc

Email Address/Public Address

Password/Private Key

Wallet Service Provider – Open Source
Code, Exchange, Wallet Service provider,
Hardware etc

Bitcoin Address

1E1144JY6R7TCmj3BGzjpofqf9EqP9vLKJm

Private Key

6JCG34xv2a040op1BfSwPicBNUNCuk9Ht1qWMgWoMJWJpownAAi

Public Key

0798694TR67C50Z680FVRD54SX9L833137Y30K70062CCEF18L5213I9R471P0107

Offline/Non-KYC Wallet



Single Wallet Paper Wallet Bulk Wallet Brain Wallet
Vanity Wallet Spilt Wallet Wallet Details

Generate New Address Print

Bitcoin Address **Private Key**

 **SHARE** **SECRET** 

18kFoeb68j87RHVJxxZGDR6Dtugt28QRBa L3uYqS1MuiddXF46S83L8mR6byUecZcQxYcw3DL3yq65yTs4kyR

A Bitcoin wallet is as simple as a single pairing of a Bitcoin address with its corresponding Bitcoin private key. Such a wallet has been generated for you in your web browser and is displayed above.

To safeguard this wallet you must print or otherwise record the Bitcoin address and private key. It is important to make a backup copy of the private key and store it in a safe location. This site does not have knowledge of your private key. If you are familiar with PGP you can download this all-in-one HTML page and check that you have an authentic version from the author of this site by matching the SHA256 hash of this HTML with the SHA256 hash available in the signed version history document linked on the footer of this site. If you leave/refresh the site or press the "Generate New Address" button then a new private key will be generated and the previously displayed private key will not be retrievable. Your Bitcoin private key should be kept a secret. Whomever you share the private key with has access to spend all the bitcoins associated with that address. If you print your wallet then store it in a zip lock bag to keep it safe from water. Treat a paper wallet like cash.

Add funds to this wallet by instructing others to send bitcoins to your Bitcoin address.

TOP SECRET

Lets make cryptocurrency wallet

- Scenario 1: Good Citizen – Go to exchange, provide KYC and created wallet
- Scenario 2: Bad Citizen – Creates self hosted wallet
- Go to website: www.bitaddress.org
- Move mouse
- Bitcoin wallet is ready

TYPES OF WALLET

Self-custody

Software



Hardware



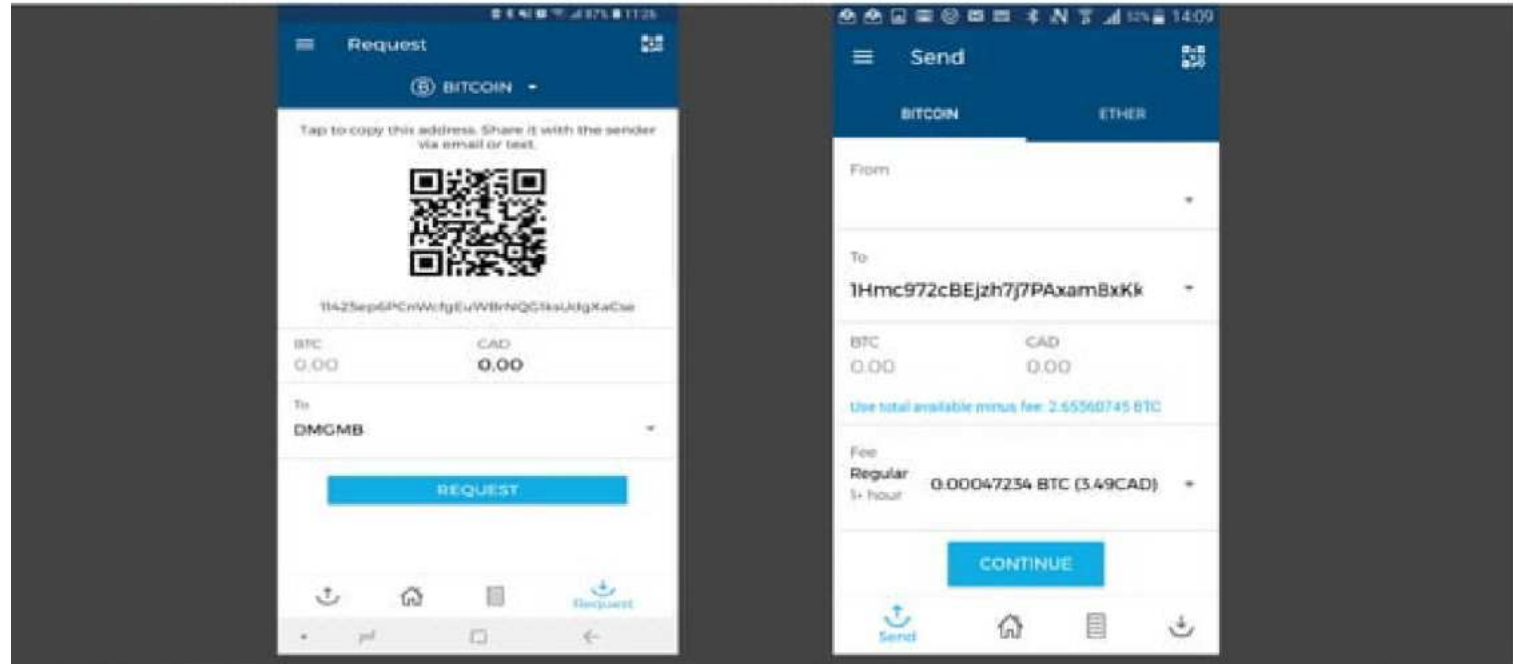
Custodial

[Third party]



Software Wallet

User Example of Sending /Receiving a Bitcoin



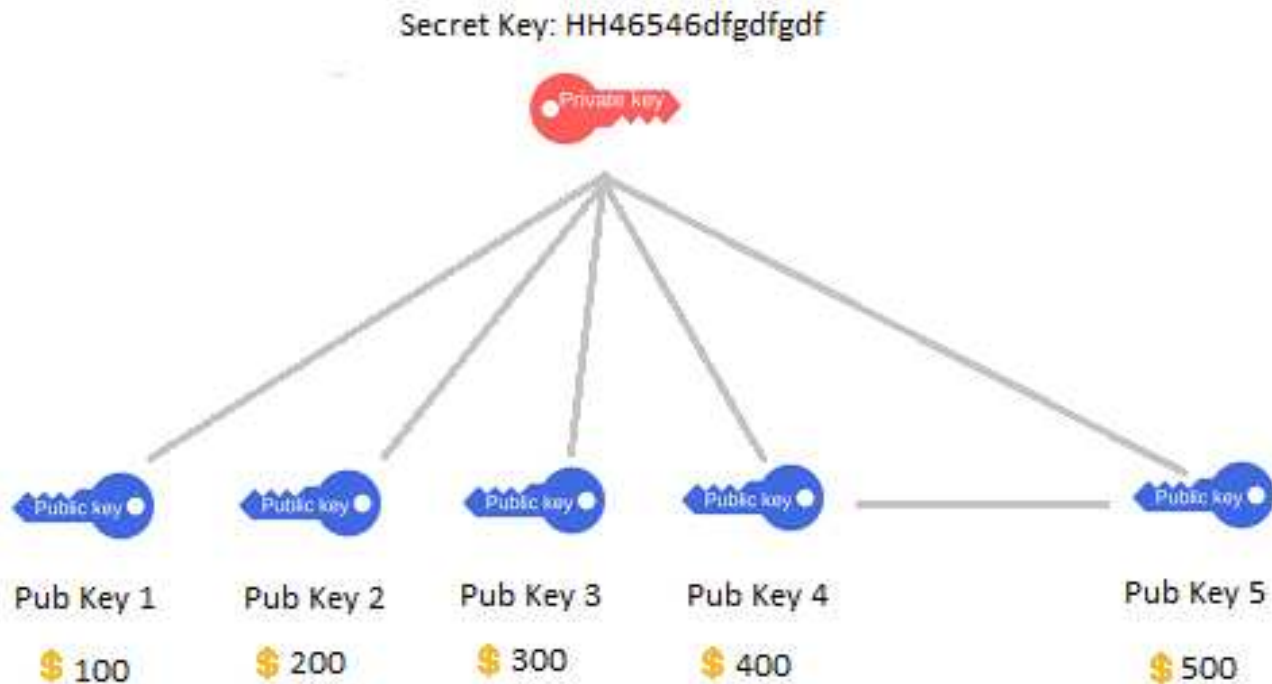
Cold Wallet



Wallets at Scale?

- Past – Limited bank accounts
- Future – Unlimited accounts
- Past – Some other 300 ways/scenarios of laundering
- Future – Technology driven activities/scenarios
- Past – Manual and cumbersome work (reached limited people)
- Future – Automated and at scale (Reaching millions)

Public & Private Key





Address	19QLHWh9URgT5DjTCQurNiuC7XRzHeNXu3
Format	BASE58 (P2PKH)
Transactions	96
Total Received	391.67141081 BTC
Total Sent	391.67141081 BTC
Final Balance	0.00000000 BTC

Transactions

Hash	634a139fb2e200915c6d68603c57da1ca75bc3629c3a641bdf3e6b...	2018-06-20 17:22
	19QLHWh9URgT5DjTCQurNiuC7XRzHeNXu3 3.00000000 BTC 1CSCdFdNM2ajjJZ876g8b9xx4JbTK4Dmm 0.00288396 BTC	1NXVpRyErJaN92Xnj7ppwtDvszaPbA1bn7 3.00000000 BTC 186Th7wGJF63sYp5Ed3tJMoEpFHSdjs4Ra 0.00213222 BTC
Fee	0.00075174 BTC (201.539 sat/B - 50.385 sat/WU - 373 bytes)	-3.00000000 BTC
Hash	884277a86656c2f8b72767c68380aea561182aff0bb62c583efd1ca...	2018-06-20 13:37
	18qkGhNZ3QFf5iuKG9dewPWF1WpoQCYr7d 1.75167843 BTC 1CWvGyV99FiXG2EnvQHLewXJi7FeJDLUrw 1.32225126 BTC	19QLHWh9URgT5DjTCQurNiuC7XRzHeNXu3 3.00000000 BTC 16cPSuG71y22u24mTqG3BhJ2sqaP9espaW 0.07268969 BTC
Fee	0.00124000 BTC (332.440 sat/B - 83.110 sat/WU - 373 bytes)	+3.00000000 BTC

Public Ledger – Blockchain Transactions

Hash	d067fdeba780c39127433262ee22a52c5980d2ad84ec0a3343ce4...		2018-06-15 14:33
	1BhNNZkCINjQ38Cqq8qBGgLXKYZwR9Rtz	1.99935254 BTC	→
	19QLHWh9URgT5DjTCqurNiuC7XRzHeNXu3	3.00000000 BTC	→
	1BaFKD2KRY9L8basnT8b9fGt9FTDNXz6XK	0.00494576 BTC	→
	16GpAEn6yhSsFVz3C2p7vwpMFribgNDc9C	5.00000000 BTC	→
	1GShboMwyFBwcChgTXFK4bVsDZstdj25RH	0.00418868 BTC	→
Fee	0.00010962 BTC (21.081 sat/B - 5.270 sat/WU - 520 bytes)		-3.00000000 BTC
Hash	55e0846fa7875021bbe7771e4e1817e9b042cb836858c1447e0530...		2018-06-15 14:33
	19QLHWh9URgT5DjTCqurNiuC7XRzHeNXu3	3.00000000 BTC	→
	3G25S1GRk61sJ3rQLrCsMSURNpXxJFgLeV	1.00060000 BTC	→
	1BhNNZkCINjQ38Cqq8qBGgLXKYZwR9Rtz	1.99935254 BTC	→
Fee	0.00004746 BTC (21.283 sat/B - 5.321 sat/WU - 223 bytes)		-3.00000000 BTC
Hash	1459bf2eff3d2803246091c73491ec3a9e9a57c0bd388dfa58c8a3...		2018-06-15 14:03
	1fdkzdpXnotg9WvzgjLrgsDiCEryDAXbj	12.71034309 BTC	→
	19QLHWh9URgT5DjTCqurNiuC7XRzHeNXu3	3.00000000 BTC	→
	1EhnNy4A8hWgdG4zq7jhGHp97wtNmux2YD	9.71031309 BTC	→
Fee	0.00003000 BTC (13.274 sat/B - 3.319 sat/WU - 226 bytes)		+3.00000000 BTC
Hash	cb1666d86b53f7766b397dcab123c915294288577a29bb3ad4fa2b...		2018-06-14 09:45
	1CWvGyV99FiXG2EnvQHLewXJi7FeJDLUrw	12.93333483 BTC	→
	19QLHWh9URgT5DjTCqurNiuC7XRzHeNXu3	3.00000000 BTC	→
	1tWLeMrXpcvrpT7kp9eYaXHdUNnaGxb4V	9.93330483 BTC	→
Fee	0.00003000 BTC (13.274 sat/B - 3.319 sat/WU - 226 bytes)		+3.00000000 BTC

Types of cases

1. Fraudulent ICOs

- Fabricate a fake ICO, create marketing hype and persuade people to buy.
- Seen as a quick and innovative way to kickstart a company.
- Ethereum has become the breeding ground for these fraudulent ICOs.
- It is the ignorance of new investors who dream of huge gains in a matter of days by holding worthless ICO tokens.

2. Shady Exchanges

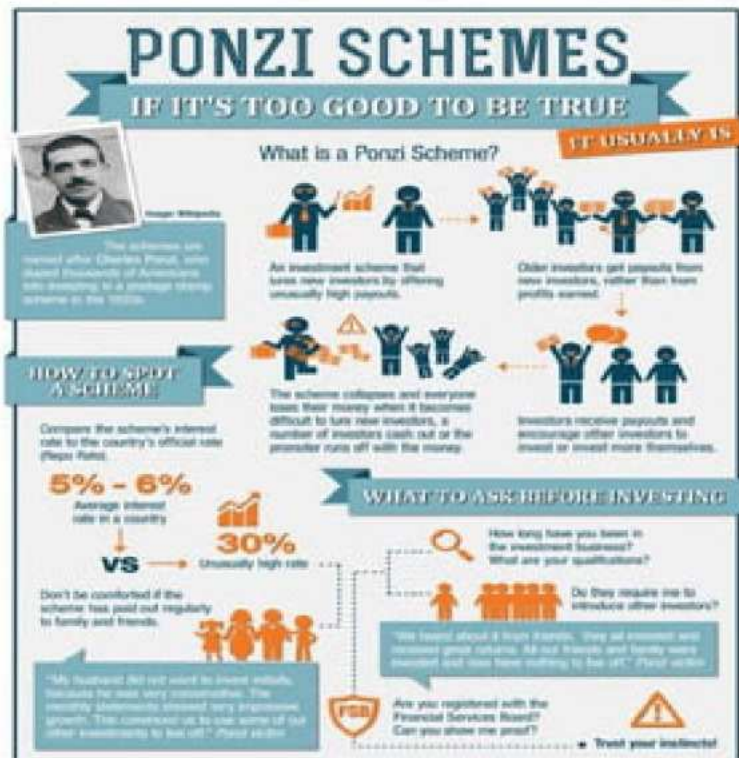
- The second most common form of scam that you will come across would be a 'shady exchange', sprung up overnight. Once you trust them and deposit your coins there, you have no way to get them back if the intentions are fraudulent.
- Also, some exchanges that start well can also eventually run away with your money any time because they fail to scale and innovate to stay competitive in the market.
- As well shady exchanges are targets for hackers as they generally have weak security due to little investment.

3. Fake Wallets

- With the launch of Bitcoin, many fake crypto wallet programs have also been launched.
- That's why it is a big **NO-NO** to pick any wallet randomly because there are chances that it will be fraudulent and you may end up losing your money.
- Though these wallets may promise you control of your funds, never trust them without proper due-diligence.

4. Pyramid or Ponzi Schemes

- This form of scam is easiest to spot but people still fall for it.
- If you find a crypto project that actively encourages the recruitment of new investors to maximize your profits, it is probably a Ponzi scheme. This system works on the model of scamming the one who enters the system later.
- Also, schemes that promise absurd returns are likely to be Ponzi schemes





6. Pump & Dump Schemes and Groups

- Pump & Dump groups are not something new in the traditional market and are also common in the crypto market.
- You will find many crypto groups with thousands of members. These groups are the tools to manipulate the prices of coins that have low market caps.
- In this way, people who act fast or first get the advantage and the people who are a bit late suffer from the plummeting prices in just a matter of minutes.
- There are several tools available in the market to monitor the volume increase in a particular crypto which helps in identifying such schemes.

7. Impersonators

- The most sophisticated form of scam.
- In this type of crypto scam, scammers make fake Twitter and Facebook account to impersonate the actual legit project or the person behind it.
- You will find many impersonators on Twitter acting like Vatalik Buterin or major coin CEO's who make announcements which are never true.
- Also, scammers have started acting as crypto exchange support staff to scam people of their crypto funds.

Why Crypto Adaption by Criminals?

- Because you are scared of cryptocurrency.
- Because you are laggard in adaption of innovation.
- Because they face highest resistance in conventional financial system.
- Believe, cryptocurrency is anonymous.
- Portability, Security & Ease of use.
- Has international liquidity and acceptance.
- Potential tax havens (Government unable to track?)

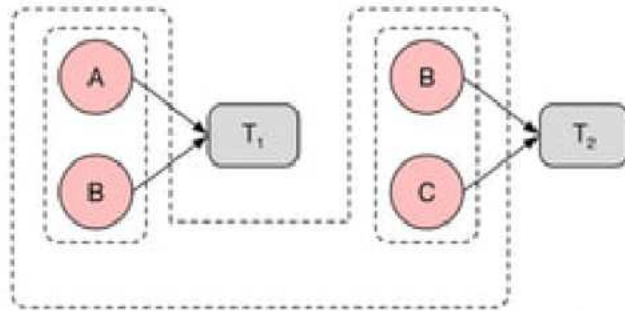
Lets look at some practical

Curious case of GainBitcoin in India.

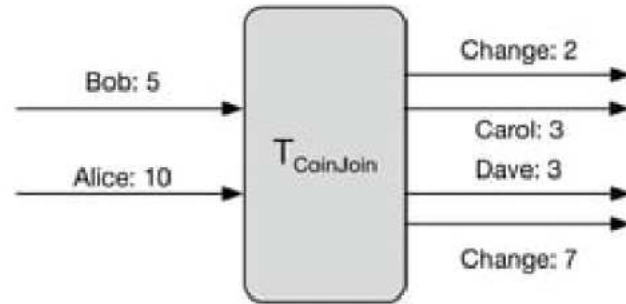
~1,00,000 customers
~5 lakh BTC volume



Fundamental



a **Multi-Input Clustering Heuristics:** Addresses *A* and *B* are inputs of transaction T_1 and must therefore be controlled by the owner of the corresponding private keys. The same holds for addresses *B* and *C* of T_2 . Since address *B* occurs in the set of inputs of T_1 and T_2 one can infer that addresses *A*, *B*, *C*, and *D* are controlled by the same actor.



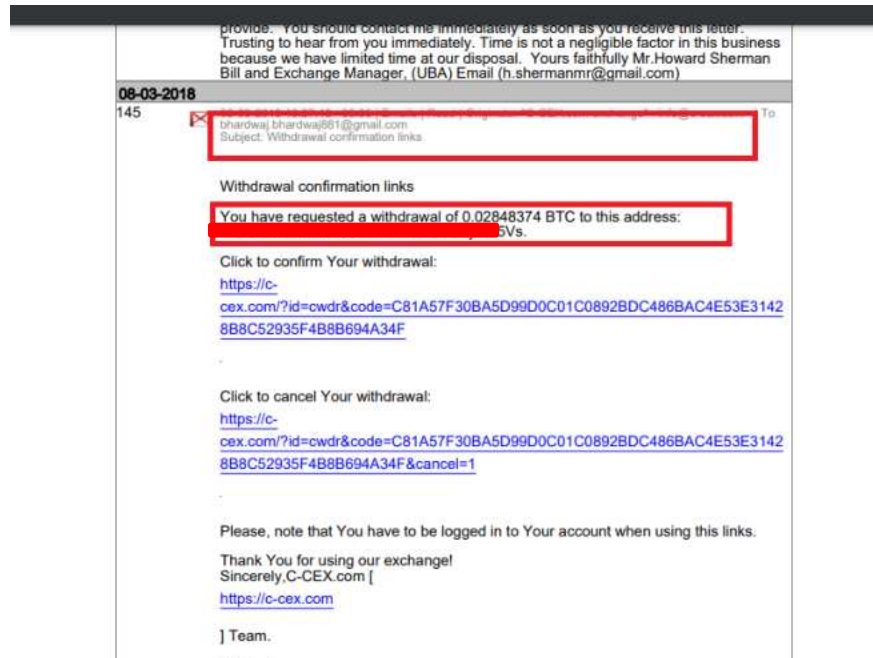
b **CoinJoin Transaction** (based on Möser and Böhme (2016)): several individual payments from multiple parties are combined into a single transaction.



Case Briefing

Email Discovery

With preliminary digital forensics, we were able to identify one of the wallets associated with accused.



Source: UFED Cloud Analyzer Report

Blockchain Forensic Analysis

Transaction Hash: dCTUZjAW5Vs

Wallet discovered with accused criminal was kept on watch list to monitor movement of cryptocurrency. On 5th February, 2021 at 18:21 hours crypto currency were consolidated and transferred to wallet which is further analyzed in next slide.

Transactions

Hash	248beeb180f1605b22e741681ef40c3742f2ffbbf4115e231b99c811b...	2021-02-05 18:21
	dCTUZjAW5Vs0.00556853 BTC dCTUZjAW5Vs0.00305341 BTC dCTUZjAW5Vs0.00673627 BTC dCTUZjAW5Vs0.00305341 BTC dCTUZjAW5Vs0.00556853 BTC dCTUZjAW5Vs0.00817697 BTC dCTUZjAW5Vs0.00763444 BTC dCTUZjAW5Vs0.00200000 BTC dCTUZjAW5Vs0.00673628 BTC dCTUZjAW5Vs0.00324831 BTC	bc1qehlw63ssgheusehdw4jddn45txwkzy3t...1.32652630 BTC
Fee	0.02259074 BTC (123.272 sat/B - 30.818 sat/WU - 18326 bytes)	-1.03808708 BTC
Hash	8c4797a3bc3fa015e29c3665556e594bc15fd900ac9e919ced3c6c...	2018-03-28 14:12
	1FdDmKQcMQmY8t1F4qzvgvL5g3XczF4zww6.00998000 BTC	31vZf6txWqb9TsH8ZZ3v9Ha8S2aXkteik10.00119119 BTC 13rYDj27QoMcNjMWbyaqVcCKh1NwjWW2DS0.00119261 BTC 1PNbnTn.iQ7MirKfbT6niBUJNKCGwAbst5b0.00119454 BTC

Blockchain Ledger Data

bc1qehl[REDACTED]

Upon analysis it was found that wallet had only 2 transaction. 1 input and 1 output indicating its use for layering. Hypothesis was further validated by time different between input and output wallet which us under ~1 hour.

Hash	8891cda0934624e7827400d627740876d6fee53978f0ec4b74c919...	2021-02-05 18:26
	[REDACTED] dn45txwkzy3tl... 1.32652630 BTC ➡	1FQqMT4X899o53t2RDsbxhSEJNtezUaGc3 1.32638038 BTC
Fee	0.00014592 BTC (75.216 sat/B - 32.499 sat/WU - 194 bytes) (129.133 sat/vByte - 113 virtual bytes)	-1.32652630 BTC

Hash	248beeb180f1605b22e741681ef40c3742f2ffbf4115e231b99c811b...	2021-02-05 18:20
	[REDACTED] TUZjAW5Vs 0.00556853 BTC ➡	bc1qehlwy63ssgheusehduwj4jddn45txwkzy3tl... 1.32652630 BTC
	[REDACTED] TUZjAW5Vs 0.00305341 BTC	
	[REDACTED] TUZjAW5Vs 0.00673627 BTC	
	[REDACTED] TUZjAW5Vs 0.00305341 BTC	
	[REDACTED] TUZjAW5Vs 0.00556853 BTC	
	[REDACTED] TUZjAW5Vs 0.00817697 BTC	
	[REDACTED] TUZjAW5Vs 0.00763444 BTC	
	[REDACTED] TUZjAW5Vs 0.00200000 BTC	
	[REDACTED] TUZjAW5Vs 0.00673628 BTC	
	[REDACTED] TUZjAW5Vs 0.00324831 BTC	
	Load more inputs... (114 remaining)	
Fee	0.02259074 BTC (123.272 sat/B - 30.818 sat/WU - 18326 bytes)	+1.32652630 BTC

Blockchain Ledger Data

1FQd

Upon analysis of wallet address it was discovered that wallet has directly deposit to 1NDy wallet which belongs to Binance.

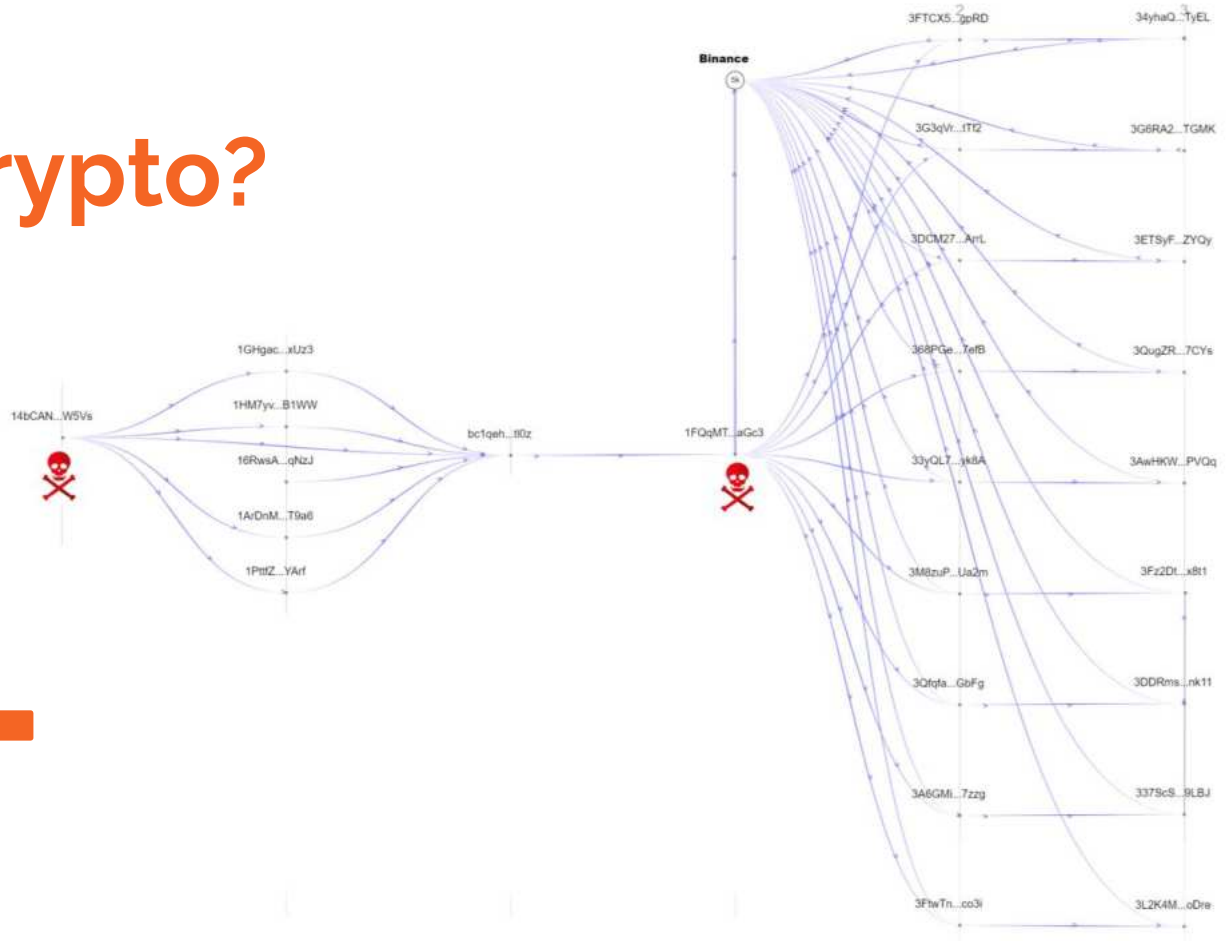
Hash	4f3f727ca759e93db3ec55e52b0696c31afbd5bf22347d190079b3b...	2021-02-20 20:42
	183e7brkkFkv6d6bEQScNSQDA8xu7jBJc3 0.10000000 BTC ➡ 1FQd 0.09977612 BTC	
Fee	0.00022388 BTC (116.604 sat/B - 29.151 sat/WU - 192 bytes)	+0.09977612 BTC

Hash	7239035be81c16714c54fe1db1cefe51d5edda618b7db88a6a8ee4f0...	2021-02-06 03:31
	1Nz 0.27891706 BTC ➡ 1NDyJtNTjm 24.13326064 BTC	
	1GL 0.50083650 BTC ➡ 3DyaRZaS3 0.00845771 BTC	
	148 0.00238770 BTC	
	1FQd 1.32638038 BTC	
	1Gns 9.99000000 BTC	
	1FA 0.05459007 BTC	
	1CL 0.00014954 BTC	
	1Gns 11.99000000 BTC	
Fee	0.00154290 BTC (123.038 sat/B - 30.760 sat/WU - 1254 bytes)	-1.32638038 BTC

Hash	8891cda0934624e7827400d627740876d6fee53978f0ec4b74c919...	2021-02-05 19:26
	bc1qehlwv63ssqheusehduw14jddn45txwkzy3tl... 1.32652630 BTC ➡ 1FQd 1.32638038 BTC	

Who eats crypto?

**Somewhere,
bitcoin will be
converted to
INR or Dollar.**

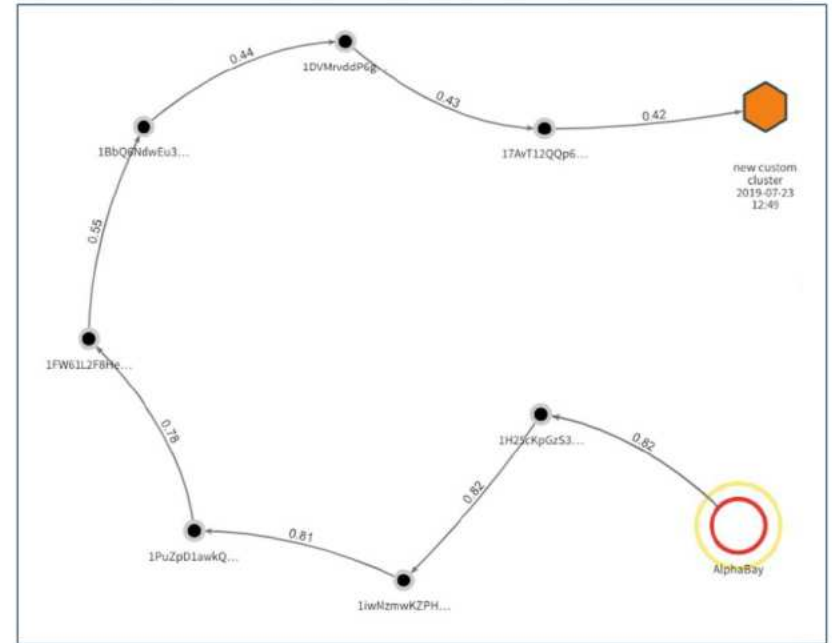


Peeling – Layering Crypto Transactions

- “Peeling” - method of moving funds through multiple addresses in quick succession to disguise source of funds
- Often value will decrease at each hop, to account for fees and to distribute the value amongst multiple wallets

Example Case

- Account C had only one deposit
- The funds ultimately came from AlphaBay - through 7 intermediate addresses
- Transaction value slowly decreased as value was dispersed; typical peeling activity - half ended up at exchange while half was dispersed amongst other wallets



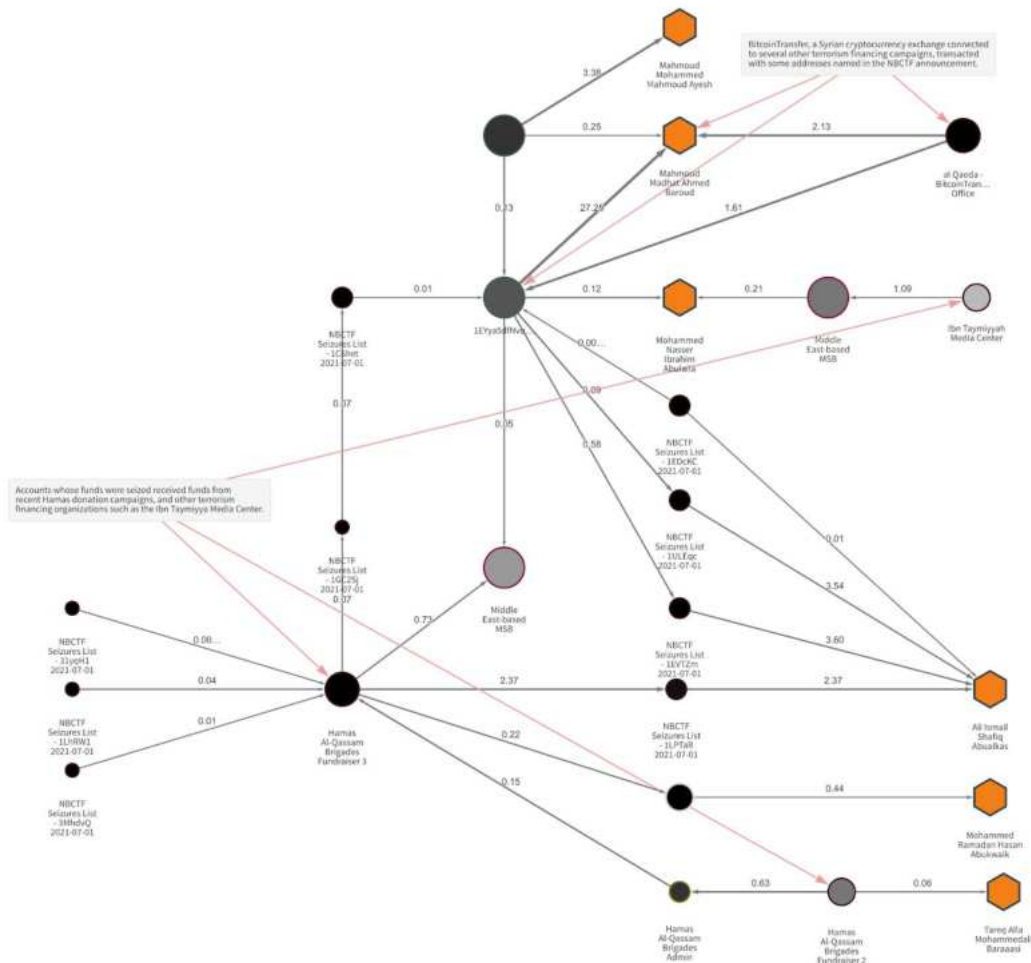
Israel's National Bureau for Counter Terror Financing (NBCTF)

PhilistAli Ismail Shafiq Abualkas
13iQsrwBYdrLpnitG5EV79o3PeHjH8XUBc

Mahmoud Madhat Ahmed Baroud
1GALPyvUDDXqA6H2eHQ9Y1yidfQ6T1Drvn

Tareq Alla Mohammedali Baraaasi
1Lm9BCDUKoBUk888DCXewM5p8bJyr83cEp

Mahmoud Mohammed Mahmoud Ayesb
164fawNZVwsR5SamAJypvCMtkMx4Xv1B3f



Terrorist Financing and Crypto – Hamas al-Qassam Brigades



First Stage



Terrorist Financing and Crypto – Hamas al-Qassam Brigades

Second Stage

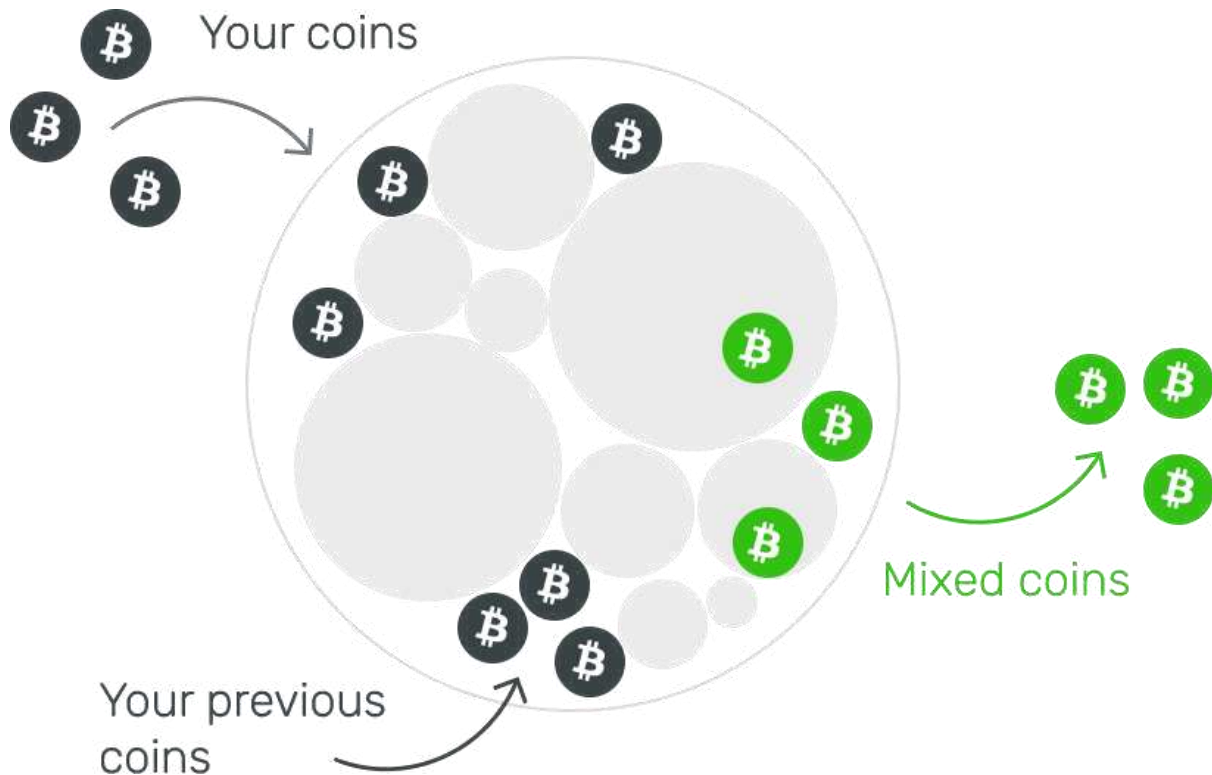


Terrorist Financing and Crypto - Al-Qaeda Campaign

- Focused on five different entities:
 - Leave an Impact Before Departure
 - Al Ikhwa
 - Malhama Tactical
 - Reminders From Syria
 - Al Sadaqah
- Fundraisers solicited via Telegram to “donate anonymously” to “support the mujahidim in Syria”
- Forfeiture complaint / warrants for:
 - 3 hosted wallets; and
 - 152 unhosted wallets
- Seizing an estimated ~\$150k worth of crypto



How does mixer work?



Bitcoin Fog – Nixing a Mixer

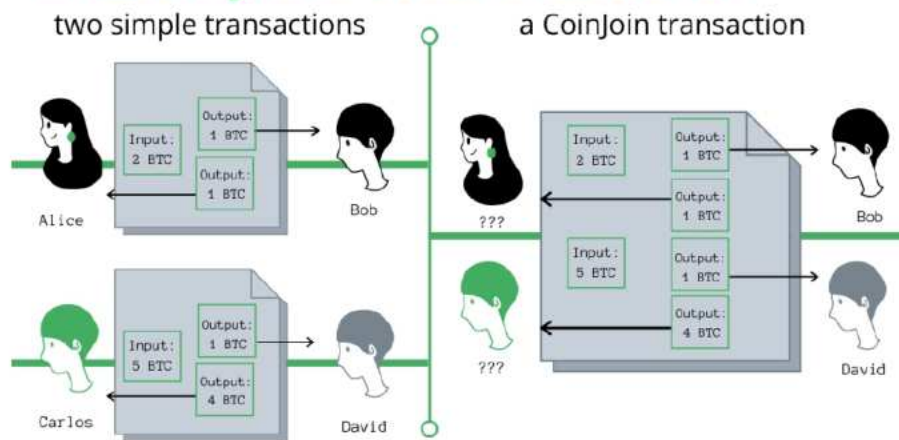
- Launched in 2011, allegedly involved in laundering funds from some of the earliest darknet markets, from Silk Road to AlphaBay
- Mixing service moved 1.2 million in bitcoin at estimated value of \$335 million
- Swedish-Russian national Roman Sterlingov arrested in LA airport
- Tracing to Sterlingov seems primarily done through LE databases from centralized exchanges – Liberty Reserve, Mt. Gox, BTC-e
- Tied email addresses to register for exchanges back to Sterlingov
- Vulnerability of centralized operations



Privacy Wallets and Joining Functionality

- Mixing services have a number of issues – “tainted” coins, centralization making them targets for law enforcement takeover
- Joining functionality like CoinJoin on Bitcoin addresses some of these weaknesses
- Privacy wallets like Wasabi and Samourai incorporate CoinJoin functionality – non-custodial, just a type of transaction
- Significant rise in use of privacy wallets in 2020, which featured in many high-profile cryptocurrency schemes
 - Wasabi used in laundering funds from Twitter hack to promote a Bitcoin scam
 - Wasabi wallet also used to move funds tied to \$280 million KuCoin exchange hack

A CoinJoin Transaction



Alice has 2 BTC and wants to send 1 BTC to Bob. Carlos has 5 BTC and wants to send 1 BTC to David. They can do two separate transactions, which reveal their addresses. Or they can combine their transactions into one CoinJoin which conceals their addresses.

Privacy Coins – Shielded and Secret

- Privacy coins lack public ledger to openly track the transaction flow, providing additional anonymity
- Examples include Monero (XMR), GRIN, and Zcash (ZEC)
- Mere use of privacy coins is not necessarily suspicious, but combined with other factors, may be indicative of a customer attempting to hide the source/destination

Example Case

- Customer B solely deposited in BTC
- Traded most of the BTC into XMR, and quickly withdrew
- Review of BTC deposits found significant darknet exposure
- Suspected Customer B is selling illicit goods on the darknet and using XMR to hide the destination of funds

#	Coin			Price	1h
☆ 1		Monero	XMR	\$50.10	-0.4%
☆ 2		Dash	DASH	\$78.80	-0.2%
☆ 3		Zcash	ZEC	\$58.79	0.2%
☆ 7		PIVX	PIVX	\$0.923063	-1.5%
☆ 5		Verge	XVG	\$0.00684370	0.1%

You can rely on:

- Blockchain Ledger (www.blockchain.com)
- Blockchain Forensic Tools
- Blockchain Forensic Expert
- OSINT
- Exchange Trading Data



Practical Problems

Data to Evidence

1. Admissibility of Blockchain Evidence
2. Different from Blockchain Based Evidence
3. National Exchanges: Section 91
4. What if exchanges are International?
5. *Section 65B in The Indian Evidence Act, 1872*
6. Desi Jugaad – *Statement Request from Criminal*

Questions?