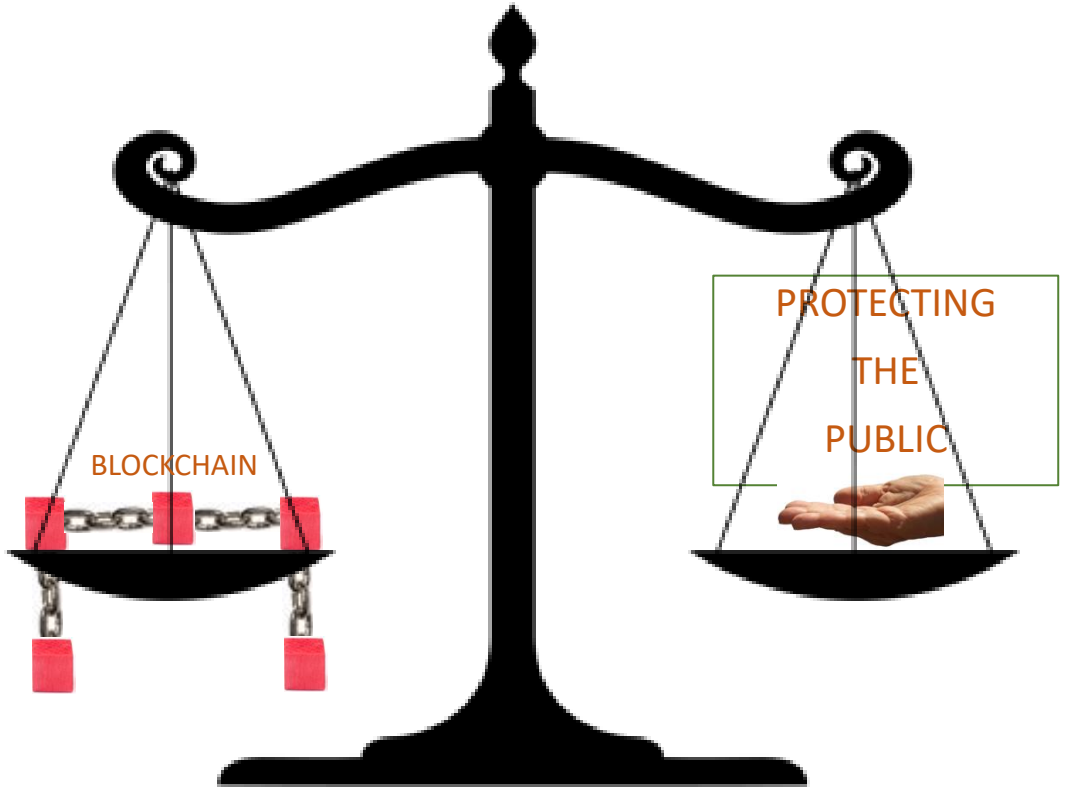
BLOCKCHAIN FOR LEGISLATORS
A USER'S GUIDE…



"DISRUPTIVE TECHNOLOGY PROMOTES PROGRESS"

"DESTRUCTIVE TECHNOLOGY …NOT SO MUCH"

PART 1 OF 4 – THE CRYPTOCURRENCY CRAZE…
In-depth Discussion Guide Available

WHY SHOULD LEGISLATORS AND REGULATORS CARE ABOUT CONVERTIBLE VIRTUAL CURRENCY?

(aka CRYPTOCURRENCY)

CAVEAT EMPTOR!!

BUYER BEWARE!!!!

"Know what you are buying?"

INFORMED DECISION MAKING!!!!!!

Society Rule#1: Humans have a way of Using, Misusing, Abusing Stuff
Wish#2: Due unto others…

"BUY NOW! THIS CRYPTOCURRENCY COULD BE WORTH 100X!!!"

Buy Low-Sale High / Get Rich Quick! – I'm in!!!

- February 16, 2023
  - $1.11T valued crypto industry (10yr achievement)
    - World Stock Market: >$94T; >44,000 companies
  - 8,755 cryptocurrency sites
    - $476B to $0 market cap. (52 > $1B)
    - Bitcoin: $24,600/coin (10 yr: $119.6L/$64,158H; 70%-95% Return!!)
    - One year: 2/3rds loss… volatile…a BIG crash!!
  - $70.64B 24Hr Trades
    - World trades ~ $34B
  - BIG MONEY MAKES IT A BIG DEAL!!!!

WHAT IS THIS CRYPTO STUFF???

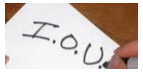
- Regular money can be touched – 

  Convertible Virtual Currency (aka crypto) is digital – computer code… untouchable.  

- With regular money, can own stuff – 

  Crypto is *ownership* in phantom value… (*own* a piece of the Blockchain network rock, can be in or out at the push of a button?) 

- Bonds are a debt owed a creditor - 

  Crypto can be loaned – but who would do it? 

- Laws and Regulations protect stock and bond consumers 

- Crypto is unregulated - 

  That Caveat thing again… (use, misuse, abuse)

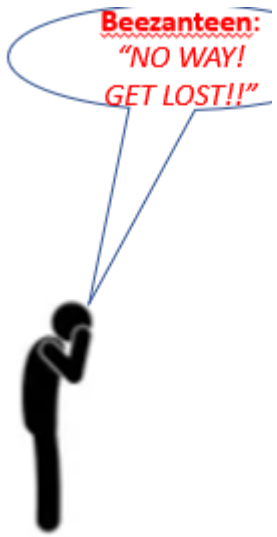
- HOW TO PROTECT THE INNOCENT? 

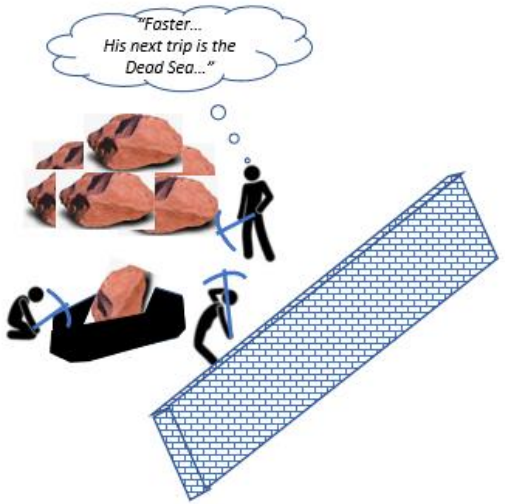
THE BIRTH OF 'CRYPTO'…

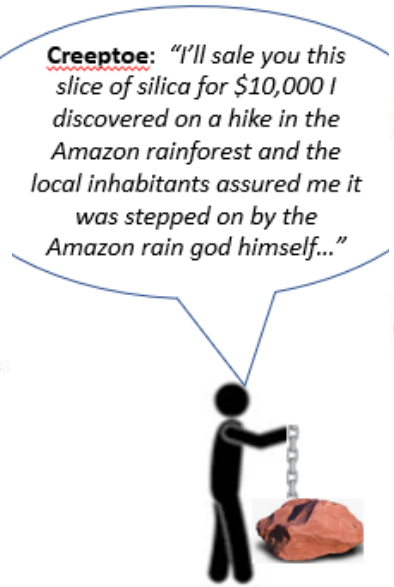
- First…some definitions:
- Fiat ('real') Currency:
  - Touchable money exclusively issued and regulated by a government, controlled by a central bank (control inflation), laws passed punishing those who counterfeit it.
  - 'Value' is recognized by its users and secured by the full faith and credit of the issuing government.
    - Think US Dollar/British Pound vs N K Won – *Which would you want in your wallet?*

- Convertible Virtual Currency aka cryptocurrency:
  - Non-touchable unregulated 'phantom' digital electronic currency issued by anyone, not controlled by a central bank, nothing to counterfeit, not used to control inflation, can exchange for real fiat money, stored in an electronic wallet.
  - 'Value' is only recognized by its users and secure only so long as that value recognition exists.
    - Interesting that ***decentralized unregulated crypto*** depends on ***centralized regulated fiat money*** for its value…

- Value is like Beauty…*in the eye of the beholder!*; Example







WHAT'S THA' HUFF ALL ABOUT???

- Is Crypto a regulated security?
  - Sponsors say NO! – merely unique computer code recognizing value (*Nonfungible Tokens – NFTs*)
    - Others YES! – meets the 4 part *Howey Test/Wells Letter*:
      - Currency Investment; Common Enterprise; For Profit; Reliance On Skill of Promoters

- Is Crypto a Commodity or Financial Service? Hmmmmmm!!
  - Looks like a duck, quacks and swims like one --- just might be a duck…

- Can Crypto be Used, Misused, Abused? SURE, like all stuff!
- Should Crypto be subject to: tax; anti-money laundering (AML); anti-terrorist (Know Your Client – KYC) Bank Secrecy Act Laws? Why not?

- Should Crowdfunding be regulated (despite JOBs Act exemptions)? Why not?
  - Crowdfunding: accept a little bit of real money from everyone over the internet/social media to finance a project in exchange for sponsor minted crypto – made up currency in which the investors recognize value. Real regulated money does not have the value volatility that unregulated crypto has: crypto an alternate to the failure of get rich quick dreams associated with real money.

- Should consumers be protected against:
  1. Fraud; Pump and Dump Schemes; Theft; Misrepresentations; Failure to disclose? ABSOLUTELY!
  2. Can Crypto be subject of Fraud; Pump and Dump Schemes; Theft; Misrepresentations; Failure to disclose misuse or abuse? Sure!!
  3. See item 1.
- Should *smart contracts* be subject to breach of contract laws? Why not?
  - Smart contract: a contract automatically executed (no matter what!) by computer code without human performance intervention – sort of like death – once started not reversible.

- Since Blockchain and Crypto totally rely on encryption technology (think password) to defend against malicious attacks (think thief or hacker), who is liable party if encryption technology computer coding fails? (No code is infallible – reason we all constantly get updates for our computers and mobile phones)

TO DO BUCKET LIST FOR LEGISLATORS

CONSUMER AND INVESTOR PROTECTION RIGHTS VS. MISUSE AND ABUSE

- Smart Contracts: Should Smart Contracts be deemed to be a legal 'contract' and breach of contract remedies available to damaged parties?
- Security: Should issuance of convertible virtual currency – CVC (aka cryptocurrency) be subject to Securities Laws and Regulations regarding consumer/investor protection rights? Deemed to meet the Howey security test?
- Commodity: Should issuance of CVC be deemed to be a commodity and subject to consumer protection laws?
- Financial Service: Should issuance of CVC be deemed to be a financial service and subject to consumer protection laws?
- Quantum Computing: Since QC technology is capable of cracking any known security or cryptographic systems, should, similar to the 'polluter pays' in environmental protection schemes, be required, before developing commercial QC systems, to publish relevant technology that will prevent the cracking of security and cryptographic systems by QC technology?
- Responsible Party: Should laws be passed that identifies accountable and responsible parties in a Blockchain network, in regard to issue specific liability faults? (Who is liable if: Cryptography systems fail?; Breach of smart contract?; Breach of consumer protection laws? Breach of investor protection laws?)
- Crowdfunding: Should the JOBS Act be amended to reduce the exemptions from investor protection disclosure and registration regulations in regard to crowdfunding used for CVC issuance projects?
- AML/KYC: Should laws be passed confirming CVC activities in whatever form are subject to (i) Anti-Money Laundering Laws (AML); (ii) Anti-Terrorist Laws (Know Your Customer – KYC), (iii) Tax Evasion Laws; Tax Form Disclosure of any and all CVC transaction activity?
- Exchange: Should laws be passed that any Crypto exchange must register and comply with relevant disclosure laws and conduct under existing laws as a currency exchange business?
- Insider Trading: Should any party involved with CVC transactions be required to report insider trading activities?

Quantum Computing
Insider Trading
Exchange
AML.KYC
Crowdfunding
Smart Contract
Responsible Party
Financial Service
Security
Commodity

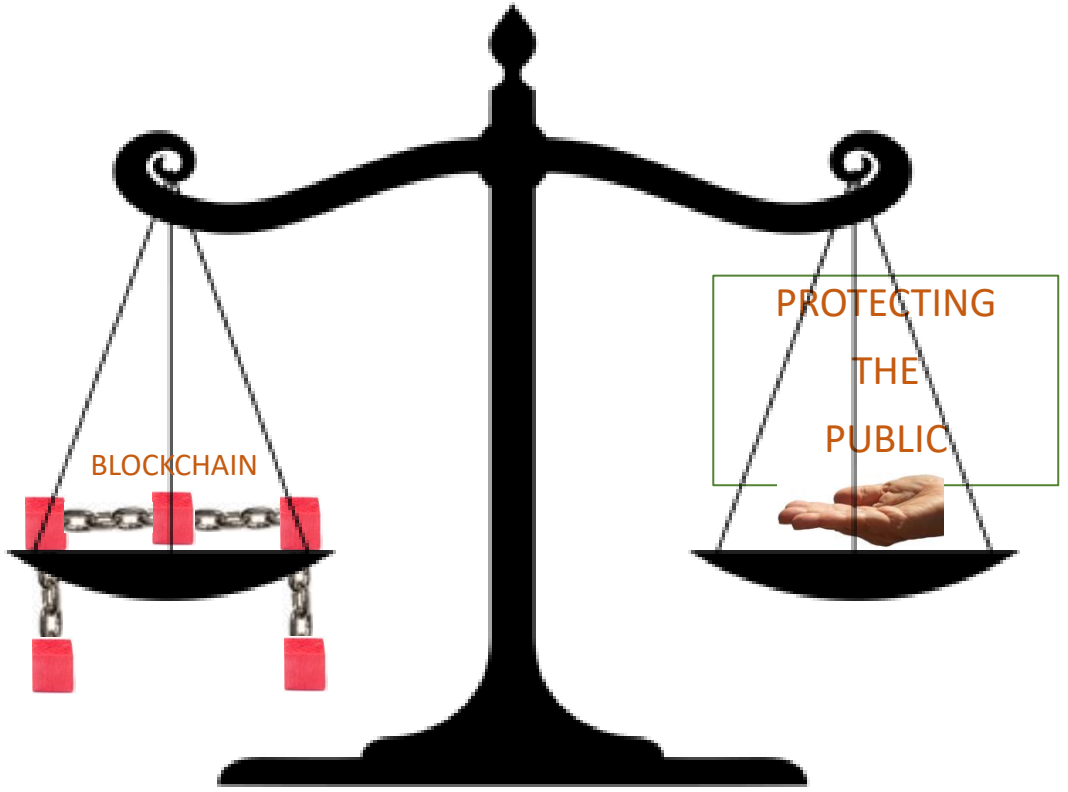
CAVEAT EMPTOR!!

BUYER BEWARE!!!!

"Know what you are buying?"

END PART 1

BLOCKCHAIN FOR LEGISLATORS
A USER'S GUIDE…



"DISRUPTIVE TECHNOLOGY PROMOTES PROGRESS"

"DESTRUCTIVE TECHNOLOGY …NOT SO MUCH"

PART 2 OF 4 – BLOCKCHAIN BASICS AND CONSENSUS VOTE…
In-depth Discussion Guide Available

WHY SHOULD LEGISLATORS AND REGULATORS CARE ABOUT BLOCKCHAIN AND DECISIONS?

(aka CONSENSUS PROTOCOL)

A GUIDE…
IN PLANE ENGLISH…

- WHAT IS BLOCKCHAIN TECHNOLOGY?
- REVEALING THE MYSTERYS OF THE TECHNOLOGY BLACKBOX 
- WHEN TO USE IT, WHEN NOT TO…
- WHAT IS GOOD AND NOT SO GOOD ABOUT IT…
- WHAT LEGISLATORS/REGULATORS CAN DO TO PROTECT THE INNOCENT AGAINST MISUSE OR ABUSE…

THE GUIDE…230 pages

- *Introduction*
- *Part 1: Explaining Blockchain and Its Technology*
  - *Good, Bad, Ugly – In Plane English*
  - *Special Section On Cryptography*
    - *(Caution: Some Math Included)*
- *Part 2: Key Blockchain Concepts Explained*
- *Part 3: Legislators/Regulators To Do Bucket List*

- *Appendix A: Computer Science For Non-Scientists*
- *Bibliography*

BLOCKCHAIN FOR LEGISLATORS – A GUIDE

DISRUPTIVE TECHNOLOGY – PROMOTES PROGRESS

DISTRUCTIVE TECHNOLOGY – NOT SO MUCH…

¡No!® Informed – I know; Decision – I No!

(March 2023)

FIRST THINGS FIRST…

TWO SIDES TO EVERY DIGITAL COIN…

1. ***Blockchain technology as a form of separatist's currency…***
   - ***Convertible Virtual Currency ('digital cryptocurrency')***
   - ***First use…***

2. ***Blockchain technology as an advanced data management tool…***

BLOCKCHAIN APPLICATIONS NON-CRYPTOCURRENCY

Managing Data Bases – Exchanging Data

- **Financial sector (fintech)**

  Efficient, low cost, auditable, secure exchange of value (currency, stocks, bonds, etc).

- **Real Estate**

  Public data base of real estate transactions.

  Free up dead capital by making non-financeable land, financeable if title is confirmed

- **Insurance**

  Managing claim history; micro-insurance

- **Government**

  Smart cities initiative (monitoring traffic and air quality; road management)

- **Other**

  e-residency ID ‘cards’, optimize public records, trusted authorship (rating agencies, weather outlets), intellectual property protection

WHEN NOT TO USE BLOCKCHAIN

"ONE SIZE DOES NOT FIT ALL"

1. ***A SINGLE ORGANIZATION…NO CONTACT WITH OUTSIDE PARTIES…***
   - ***DEPARTMENT "A" EXCHANGING DATA WITH DEPARTMENT "B"***
2. ***HIGHLY CUSTOMIZED, CONSTANTLY CHANGING DATA EXCHANGE***
   - ***RESEARCH LAB***
3. ***HUGE NUMBER OF TRANSACTIONS***
   - ***VISA CARD DAILY TRANSACTIONS!***

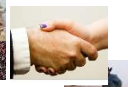
SECOND THINGS SECOND…
SOME FUNDAMENTALS OF BLOCKCHAIN

1. ***Internet is essential…***
2. ***Only practical way to 'mint'$_{issue}$ convertible virtual currencies.***
3. ***Cryptographic $_{(encryption/decryption)}$ technology is essential…***
   - ***Provides security (prevent hacker attacks)***
   - ***Recorded data is 'immutable' (can't be changed, permanent record)***
   - ***Privacy$_{sort\ of}$***

THE GOOD OLE' DAYS…
WAY BEFORE BLOCKCHAIN









- *Do it yourself …independent…decentralized…one on one deals*
- *Handheld abacus to count…*
- *A shovel to dig a hole…*
- *Handheld sextant to guide ships…*
- *Animal pelt traded for bucket of berries…handshake and your word sealed deals…look trust in the eye…*
- *Transportation by bridled horse or stick shift cars…*
- *Pony express messaging…*
- *Human and horsepower did the work…*
- *Something broke…you fixed it*
- *Bad guys, named Black Bart, wore black hats – common sense instinct to avoid them*
- *Few mysteries…except Alchemist dream changing lead into gold.*

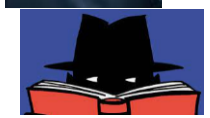
THE MODERN ERA… BEFORE BLOCKCHAIN









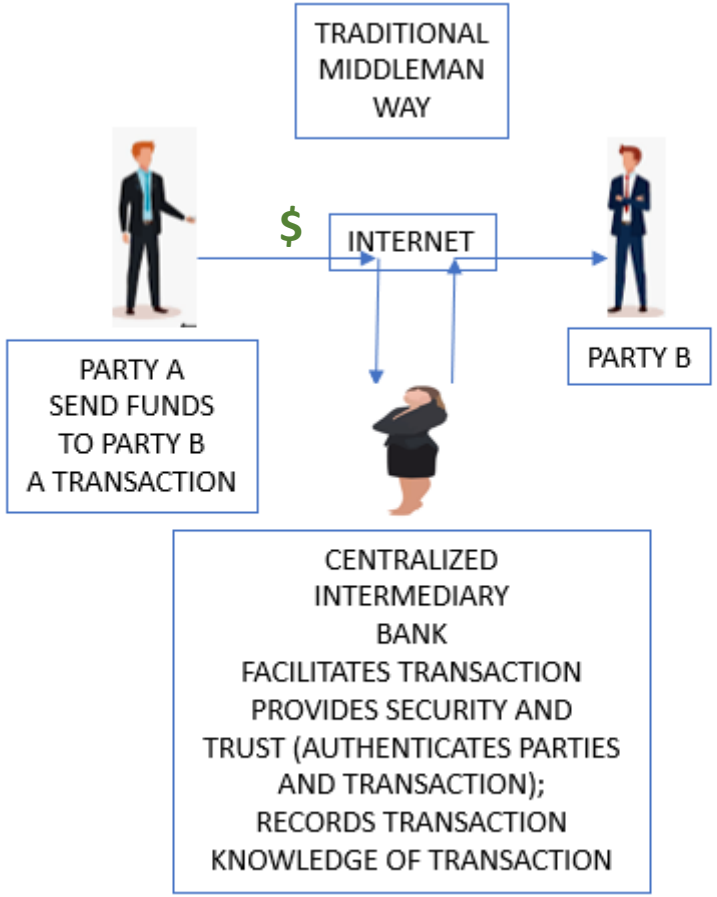



- *…Electrons captured, controlled…work is easier…centralized operations…banks provided trust…a middleman…no more one to one contact*
- *Computers count…*
- *GPS guides ships…*
- *Robots drills holes…*
- *A contract/lawyer/court/deed seals deals…*
- *Driverless cars…more important things to do…*
- *Instantaneous messaging and emails…*
- *Electrons do the heavy lifting…*
- *Something broke…replace it*
- *Bad guys, 24/7 computer jocks, stealing electronic wallets*
  - *No more get-away cars, drivers, masks, night time use of bolt cutters, no more black hats -- maybe black hoodies…*
- *Many technological mysteries…*

THE MODERN ERA…

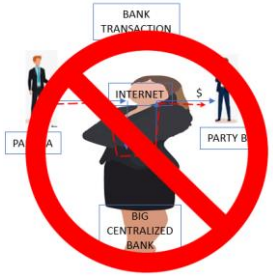
TYPICAL CENTRALIZED TRANSACTION

Using The Internet and Bank Websites, Party A Sends $$ From Their Bank to Party B's Bank
ONE STOP TRUST SERVICE…

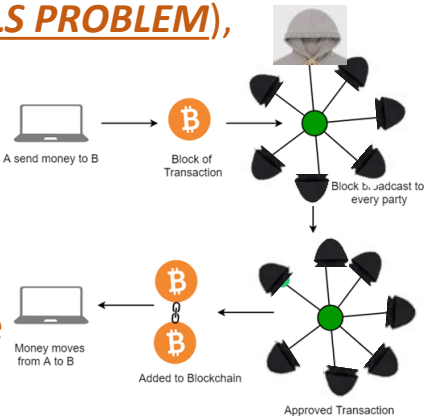


Not shown are cryptographic encryption and decryption steps for keeping information sent over the internet, safe and secure from Eve the eavesdropper snooping eyes.

THE BIRTH OF BLOCKCHAIN



- The mysterious 'Satoshi Nakamoto' (a pseudonym for him, her or them) authored a publicly published paper in 2008, unleashing the Blockchain Technology
  - First described use: a disruptive, separatist movement against central Bank authority regulated real 'fiat' money.
    - Big Brother Bank seen as too menacing?
  - Satoshi's Technology solved the problems of:
    - Obtaining consensus (agreement) of buying/selling cryptocurrency (solving ***THE BYZANTINE GENERALS PROBLEM***),
      - without a central authority (no bank – no one stop trust service),
      - among decentralized participants located throughout the world,
      - who do not trust one another;
      - honoring some privacy of the participants;
      - secure (…) from hacker attacks (solving ***THE DISCRETE LOGARITHM PROBLEM***); and
      - creating a verified record of all transactions (grouped in Blocks of *[~2,000]* transactions) that are
        - Immutable (can't be changed);
        - Nonreputiable (once recorded, user can't deny the truth of the record)



- Why did Satoshi remain anonymous?
  - And instead let world-wide Developers develop the technology…
  - **PERHAPS…Avoid possible prosecution under two U.S. laws???…**
    - Digital Millennium Copyright Act (DMCA), civil and criminal penalties - Blockchain **cryptanalytic violations of copyright protection** (i.e. cracking music and secure electronic document encryption codes)
    - Civil and criminal penalties associated with **prohibitions of cryptographic technology export** - protecting National Security and thwarting terrorism.
- Who is the real mysterious Satoshi Nakamoto? Only the Shadow knows…

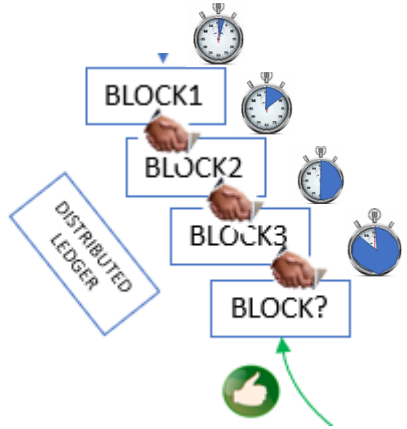
THE BLOCKCHAIN ERA…

- *Back to the Good ole' days decentralized, network…BIG disruptive paradigm change…*
- *No middleman, direct party dealing – peer to peer one-on-one contact – trading cryptocurrency or exchanging data ('transactions')…*
- *Connected to the internet…*
- *Where…*
  - *No one is trusted*
  - *The purity of emotionless 'auto-pilot' non-human computer programme mathematical algorithms provides the trust and security…safety from hackers*

	Good Ole Days	Modern Era	Blockchain Era
Structure…	Decentralized	Centralized	Decentralized
Trust provided by	A hand shake….	A bank…	Computer code (mathematical algorithms)
Security…	Steer clear of Black Bart; a six-shooter	Cryptography and Hash	Cryptography and Hash; Consensus Protocols…

THE BLOCKCHAIN ERA…MORE

- *Chronologically recorded Blocks of transactions (2000+ at a time - buy/sale crypto) are linked together in a chain –*
  - *a digital 'data base' ledger;* 
- *Permanent records, auditable, <u>immutable</u>*
  - *(<u>can't be changed</u>),* 
- *Can't be <u>repudiated</u>*
  - *(<u>once recorded, a party to a transaction cannot deny its validity</u>);* 
- *Privacy (…) of transacting parties* 



THE BLOCKCHAIN ERA…
EXAMPLE DECENTRALIZED TRANSACTION

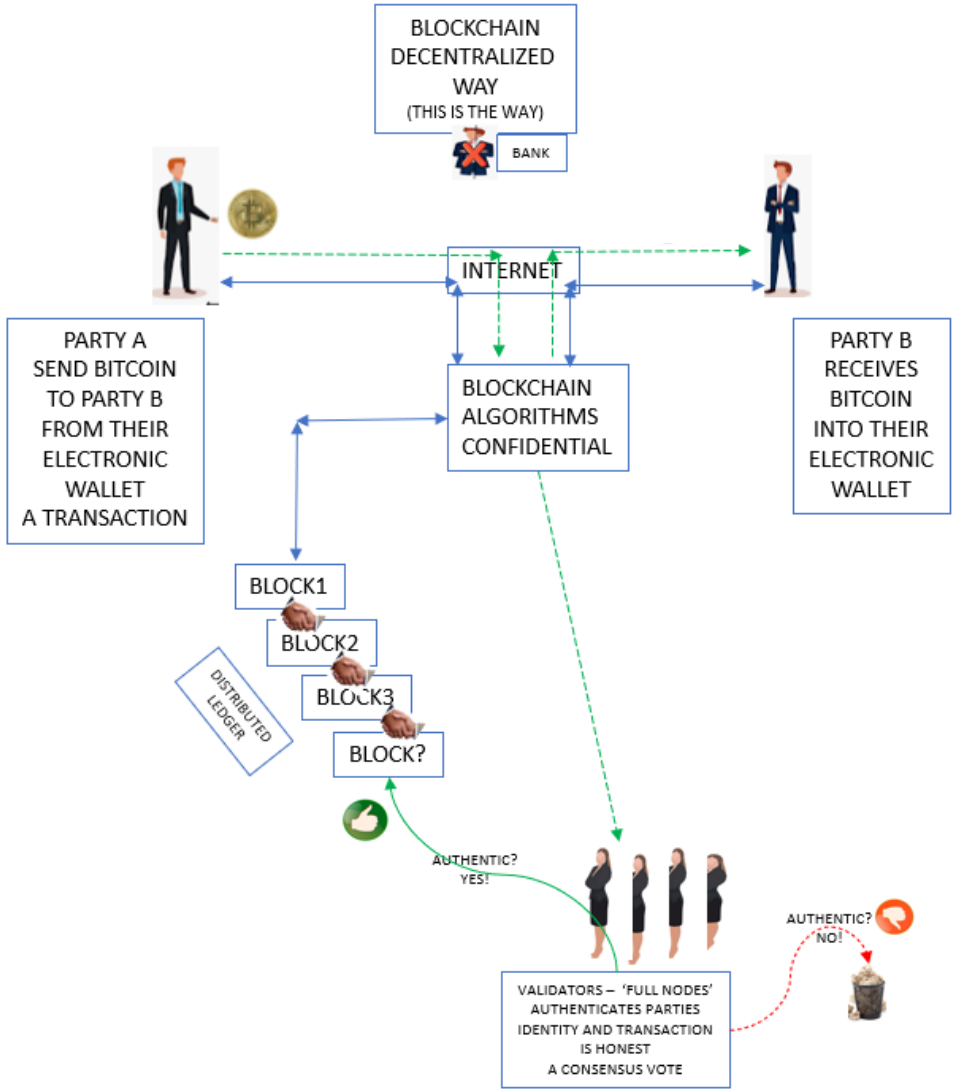
Party A Sends From Their Electronic Wallet, Cryptocurrency to Party B's Wallet

(no trust)

Not shown
encryption and decryption steps
internet information on
safe and secure.

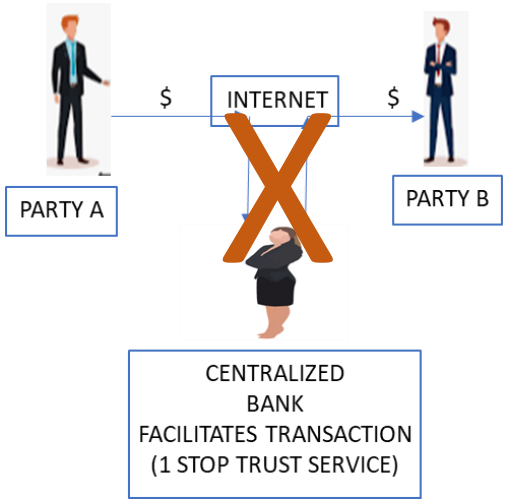
Encryption:
plaintext to unintelligible
cyphertext. ('Hello' to '$34Bc*4')

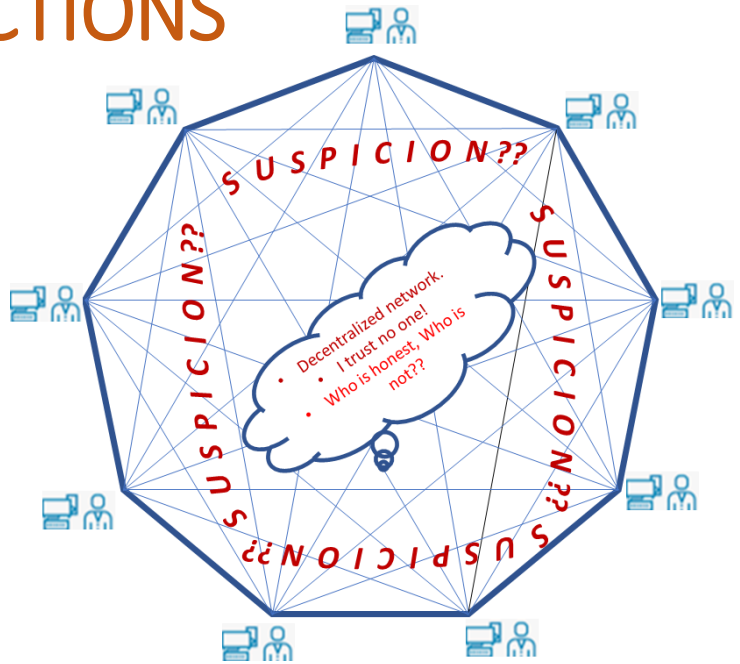
Decryption:
unintelligible cyphertext to
plaintext. ('$34Bc*4' converted to
'Hello')



WITHOUT A CENTRALIZED TRUSTED DECISION MAKER (A BANK),

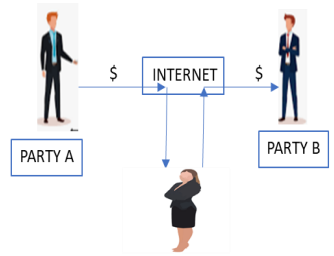
HOW DOES A DECENTRALIZED *PUBLIC* BLOCKCHAIN NETWORK MAKE DECISIONS WHERE NOBODY TRUSTS EACH OTHER? (APPROVE AND RECORD TRANSACTIONS TO THE NETWORK)



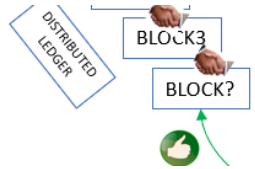


- Uncertain Decision: A "*Byzantine Generals Problem*"
- Solution: 'voting/administration agreement' called a Consensus Protocol
  - Popular types: Proof-of-Work; Proof-of-Stake; Delegated Proof-of-Stake
    -- MANY OTHERS…`

WHAT IS A CONSENSUS PROTOCOL?

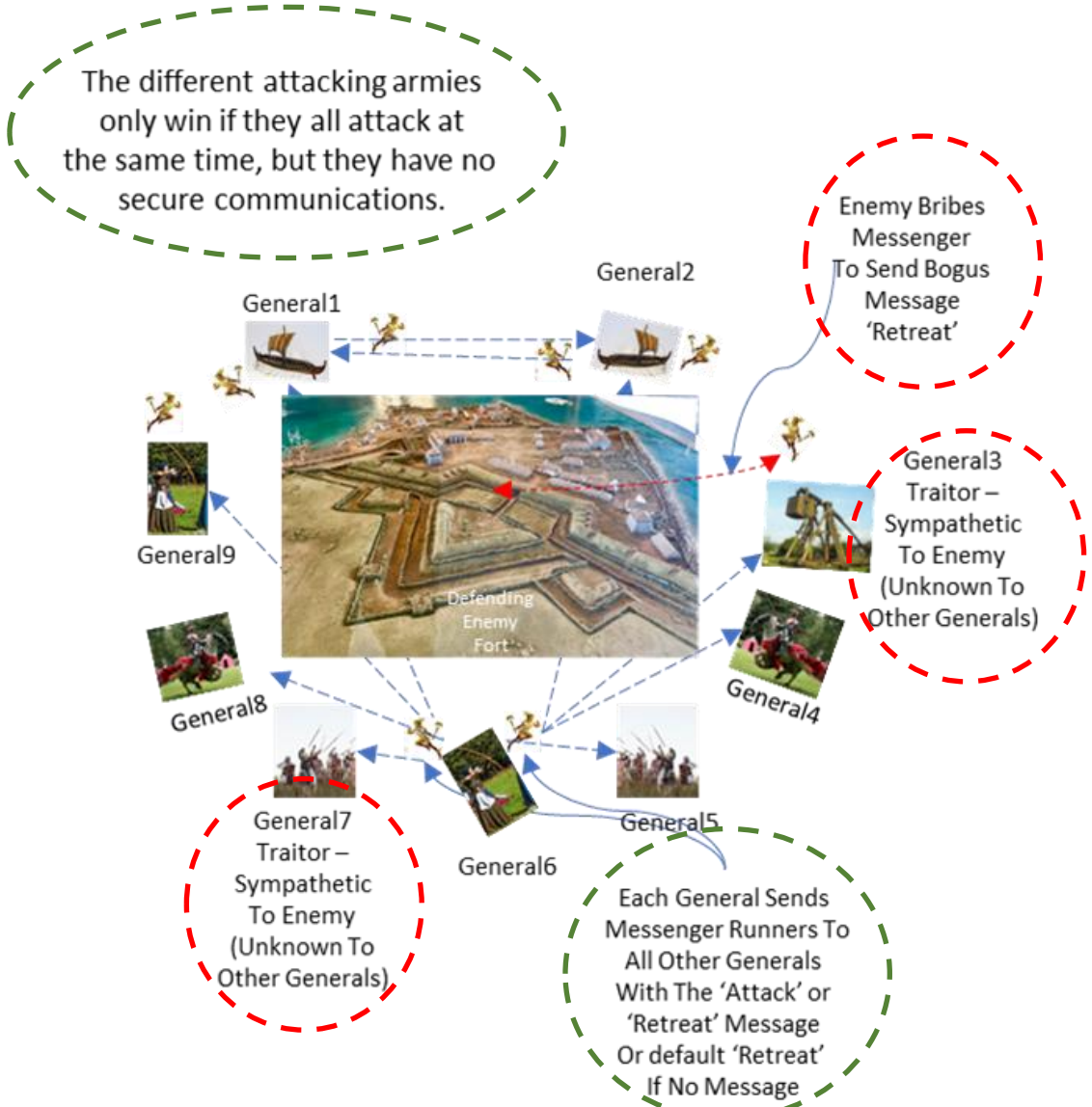


- In a conventional centralized system – a Bank provides a one-stop trust service
  - Transactions and Parties are confirmed and then completed – security provided by cryptography – computer code keeping stuff secret.
- In a decentralized separatists Blockchain cryptocurrency network, there is no one-stop trust service and nobody trusts each other.
- Consensus Protocol is an operating agreement that substitutes for a one-stop trust service.
- How?
  - Certain participants (10's of thousands of them called Full Nodes, Validators or miners) in the Blockchain …
    - compete (by solving a tough math puzzle$_{PoW}$ or putting up a deposit$_{PoS}$ of cryptocurrency) and
    - the competition winner incentivized by being paid a cryptocurrency fee, to authenticate parties and transactions
    - Non-winning validators by majority vote of the 10's of thousands, approve the winning validators request to permanently record Blocks of transactions to the Blockchain ledger.
    - Consensus Protocol structure is said to solve the ***Byzantine Generals Problem*** and ***Discrete Logarithm Problem*** – obtaining a truthful decision in an environment of distrust and security risks.



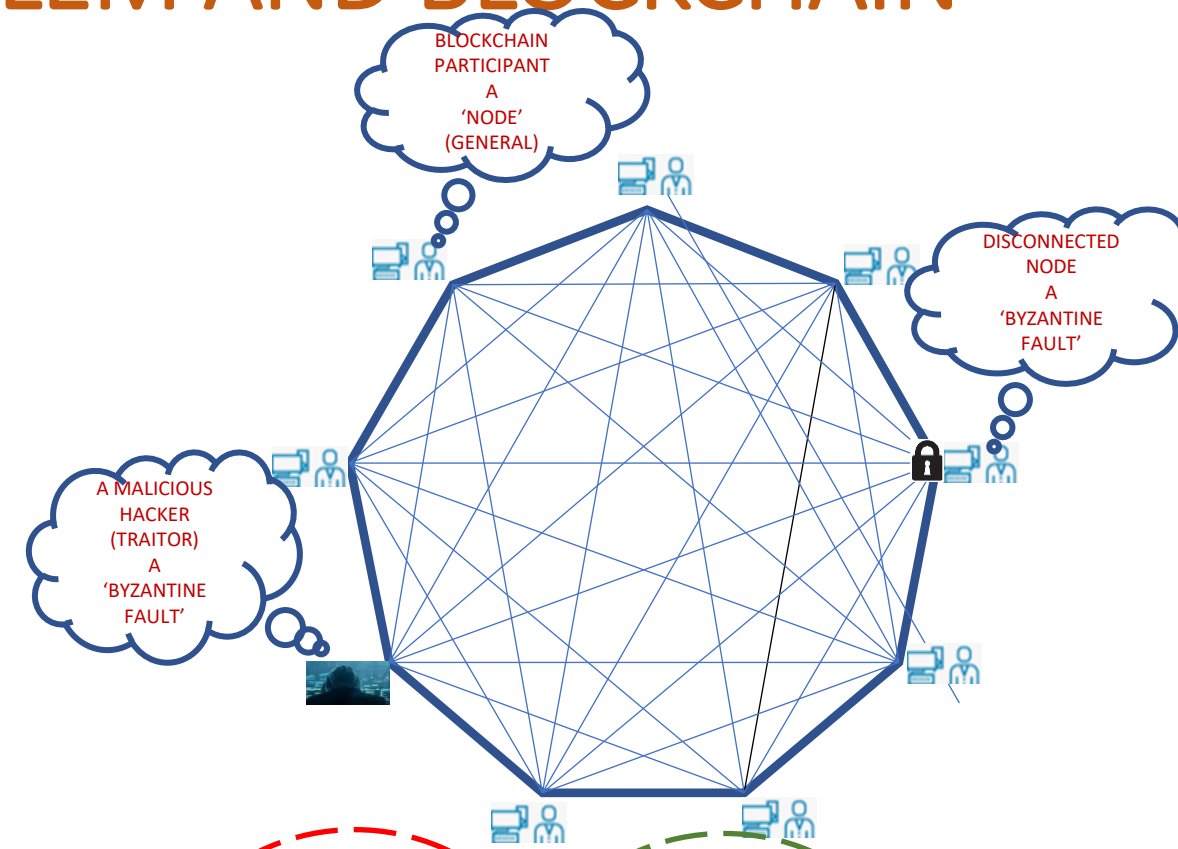
WHOA!…WHAT IS THE BYZANTINE GENERAL'S PROBLEM?

- How to obtain a majority truthful Yes/No decisions – when voters are not trusted.
- Example: 9 Generals (2 are Traitors$_{\text{but who?}}$) communicating only with messengers (1 is bribed$_{\text{but who?}}$): "Attack" or "Retreat". Who to believe?
- Traitor Generals and bribed messengers known as "***Byzantine Faults" (dishonest messages).***
- The ***GOLDEN FORMULA*** solution…
  - N >= 3m + 1
  - N: Total number of Generals (Loyal and Traitor)
  - m: Likely number of Traitor Generals
  - Message is reliable (majority reads Retreat or Attack) ***IF*** the total number of Generals are greater than or equal to 3 times the number of possible Traitors plus 1.
  - Or: m <= (N – 1)/3
  - Message is reliable (majority reads Retreat or Attack) ***IF*** total number of Traitor Generals are equal to or less than total number of Generals less 1 and that value divided by 3
  - ***"Byzantine Fault Tolerance" is*** high (good thing) when N is large and m is low.



BZANTINE GENERAL'S PROBLEM AND BLOCKCHAIN

- Honest, Faulty (unintentional) and Malicious (intentional) '*Nodes*' in a Blockchain network - same as Loyal / Traitor Generals.
  - ***A faulty or malicious Node is a Byzantine Fault Node.***
- The Table illustrates a range of Traitors / Faulty Nodes from 0 to 3,333,
  - And GOLDEN FORMULA calculation for the minimum number of Generals / Nodes
- Assuming 3,333 Traitors / Faulty Nodes (Byzantine Faults),
  - Total number of voting Generals / Nodes, must be equal to or greater than 10,000 – ensures reliable decisions.
- KEY MESSAGE:
  - Actual total number of Bitcoin / Ethereum Blockchain voting Nodes: >10,000 (***Consensus Protocol voters***);
  - Therefore, it would take > 3,333 Faults (Malicious Hackers and non-malicious) to invalidate Byzantine Generals Problem decision!
    - Highly unlikely that many faults!!!
  - SATOSHI IS RIGHT…DECENTRALIZED BLOCKCHAIN CONSENSUS PROTOCOL VOTING IS A SOLUTION TO THE BYZANTINE GENERAL'S PROBLEM



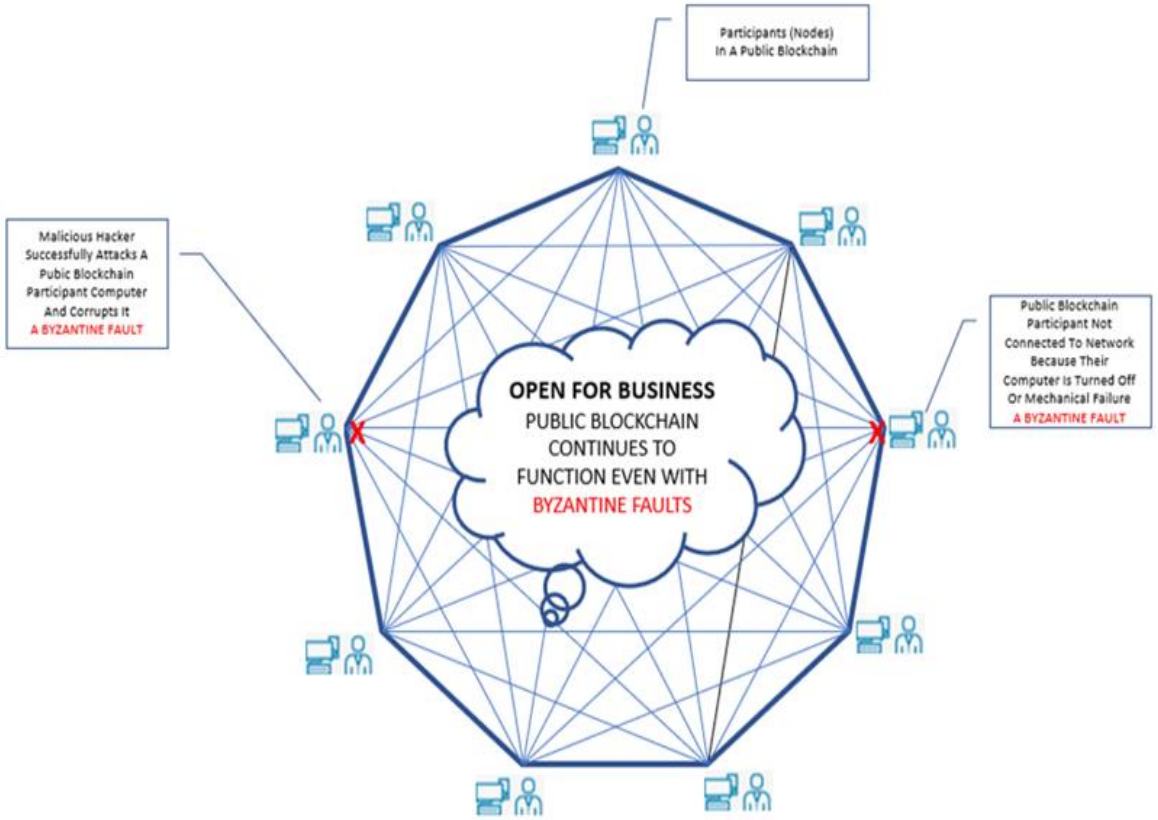
FAULTS <<3,000⁻⁻

Number of Traitor Generals, m (Counting a loyal General as a traitor if their messenger is bribed)	Minimum Number Of Generals N = 3m + 1 (Loyal + Traitor)
0	1
1	4
2	7
3	10
4	13
5	16
3,333	10,000

ACTUAL >>20,000⁺⁺

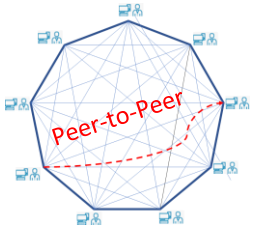
BYZANTINE GENERAL'S PROBLEM AND BLOCKCHAIN DOUBLE SPEND RISK…

- Blockchain network successfully operates with many Byzantine Faults.
- High (good thing) ***Byzantine Fault Tolerance***
- Practically impossible for risk of double spend cryptocurrency problem (a malicious party trying to spend the same 'coin' twice (or more) since
  - The Full Node validators would discover the permanent recorded Blockchain ledger already has logged in a spend
  - Transaction validator majority vote would disapprove the transaction (no matter how the faulty node votes)

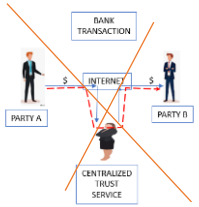


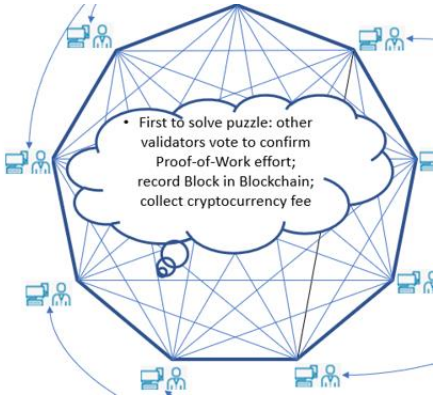
PROOF-OF-WORK
SOLVES THE BYZANTINE GENERALS PROBLEM

Party A Sends From Their Electronic Wallet, Cryptocurrency to Party B's Wallet



- Proof-of-Work (a Consensus Protocol)
  - A competitive process to authenticate transactions in the trustless decentralized PUBLIC Blockchain network
  - Substitute for centralized bank management
- Work includes:
  - Effort authenticating parties and transactions;
  - Investment expensive computer equipment;
  - Using much computer power to be the first to solve a electricity-consuming mathematical puzzle.
    - The difficulty level for solving the puzzle ('mining') in March 2022 was 27.55 trillion computer calculations!
    - Chances of solving the puzzle is 1 in 27.55 trillion !!!
    - 91,655 times more likely to win the Powerball jackpot with a single lottery ticket
- Competing validators (miners) motivated to solve the puzzle because
  - First to solve the puzzle
  - Earns a cryptocurrency service fee.
- Some validators pool (*joint venture*) their computers and share fee

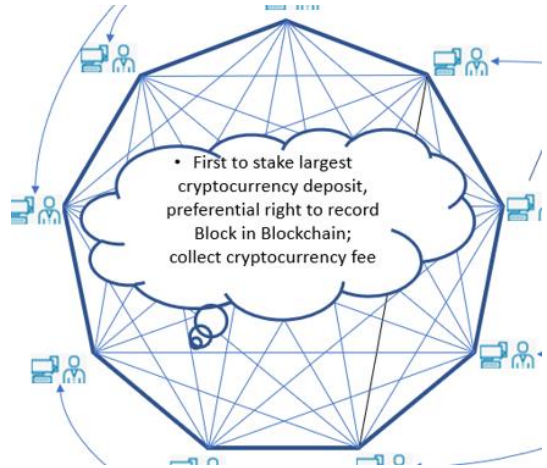




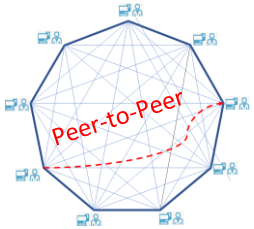
PROOF-OF-STAKE
SOLVES THE BYZANTINE GENERALS PROBLEM

Party A Sends From Their Electronic Wallet, Cryptocurrency to Party B's Wallet

- No 'Work' required…
- Competes to be 'winning validator' by staking (a deposit) of cryptocurrency and highest stake preferentially acts as winning validator.
  1. Authenticates parties and content of Block transactions,
  2. Permission to record the Block in the Blockchain and
  3. Receive a cryptocurrency validation service fee.
- Does not use large electricity demand as Proof-of-Work

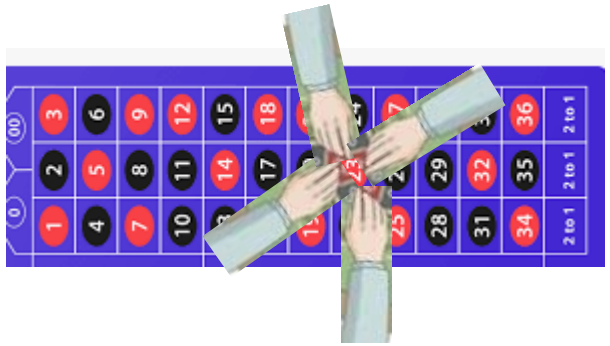


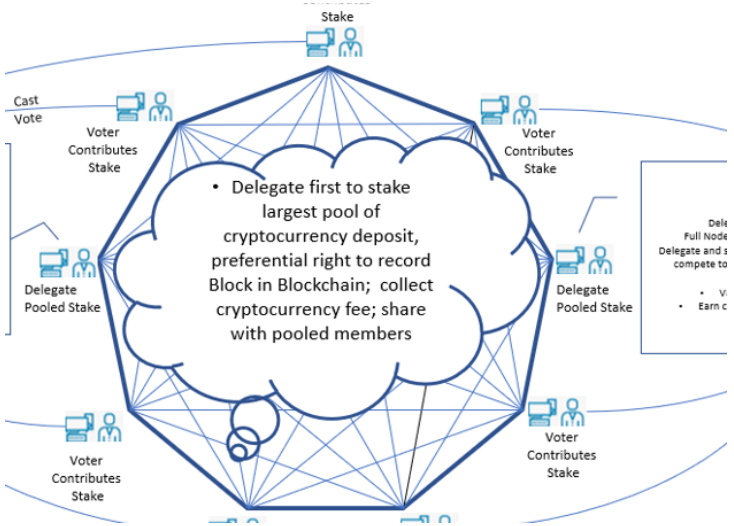
DELEGATED PROOF-OF-STAKE SOLVES THE BYZANTINE GENERALS PROBLEM



Party A Sends From Their Electronic Wallet, Cryptocurrency to Party B's Wallet

- Similar to Proof-of-Stake : A lead Delegate validator represents a group of nominating stakers; only Delegate can validate
- Delegate and partners:
  - Pool their cryptocurrency stake
  - Highest pooled stake earns preferential right for their Delegate to validate Blocks
  - Cryptocurrency fee is shared among pool members
- Because pooling dilutes the GOLDEN FORMULA (fewer individual validators),
  - Delegate elections HELD regularly; 
  - Delegates held accountable for their decision
  - Not lock members into a long term pool.

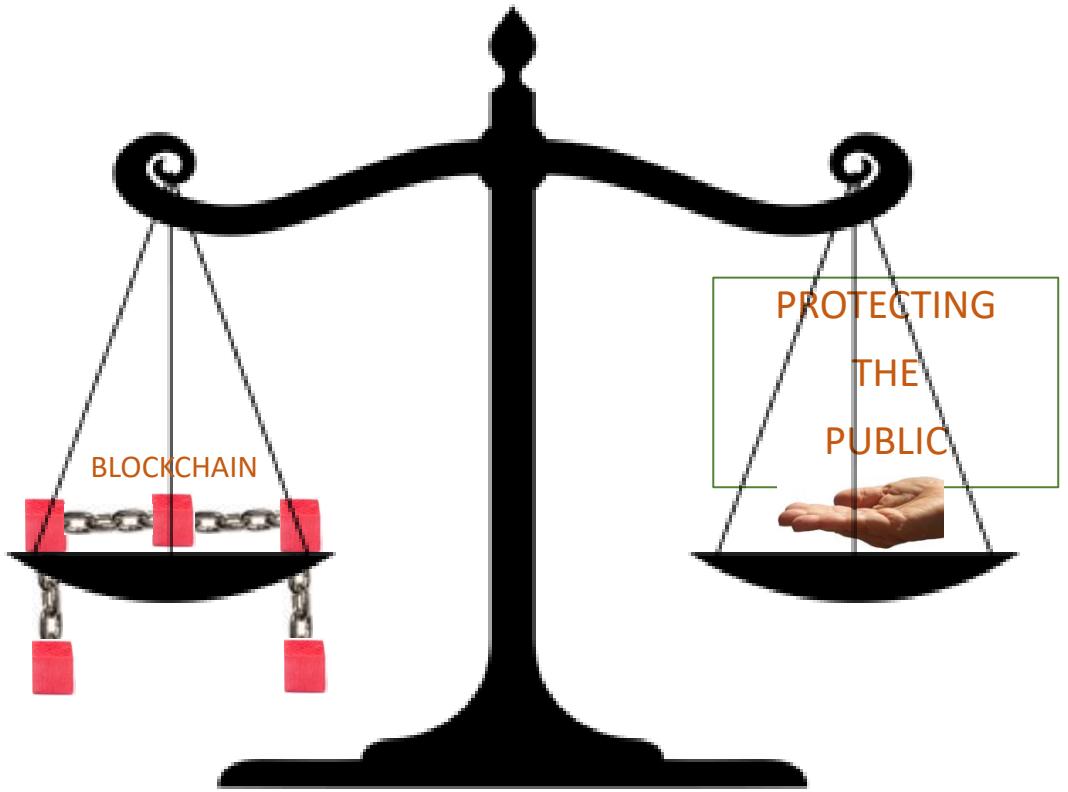




END
BLOCKCHAIN IN A NUTSHELL
AND
CONSENSUS PROTOCOL

END PART 2

BLOCKCHAIN FOR LEGISLATORS
A USER'S GUIDE…



"DISRUPTIVE TECHNOLOGY PROMOTES PROGRESS"

"DESTRUCTIVE TECHNOLOGY …NOT SO MUCH"

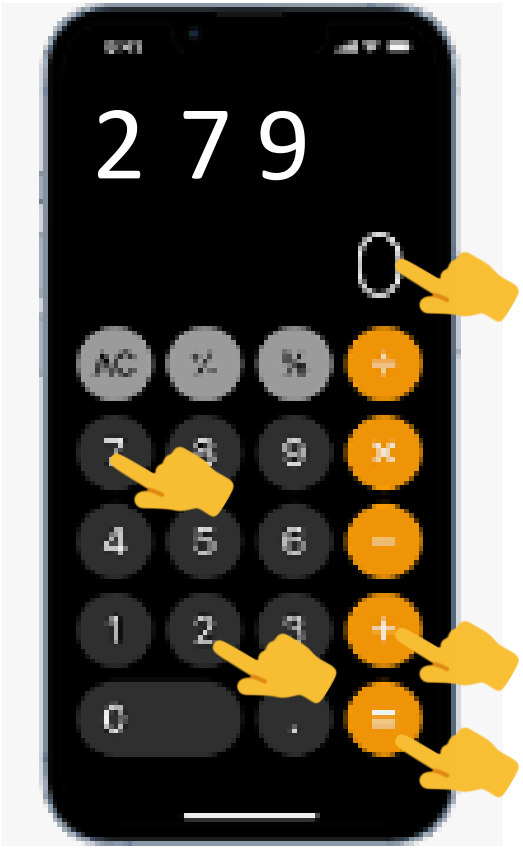
PART 3 OF 4 – SPECIAL BLOCKCHAIN TOPICS

SPECIAL BLOCKCHAIN TOPICS

- Algorithm
- Hash
- Discrete Logarithm Problem
- Smart Contract
- Blockchain Types
- Blockchain Participants
- Nodes and Their Jobs
- Recording To The Blockchain
- Blockchain Block Structure

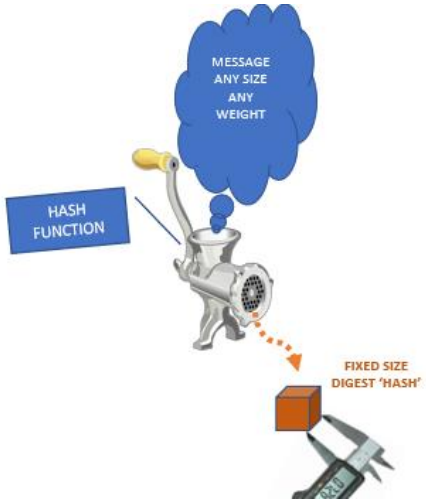
WHAT IS AN ALGORITHM?

- A computer programme: input certain information; calculations performed; desired output.
- Illustration: handheld calculator…
  - Turn on
  - Enter “2”
  - Enter “+”
  - Enter “7”
  - Enter =
  - Result” “9”
  - An algorithm!

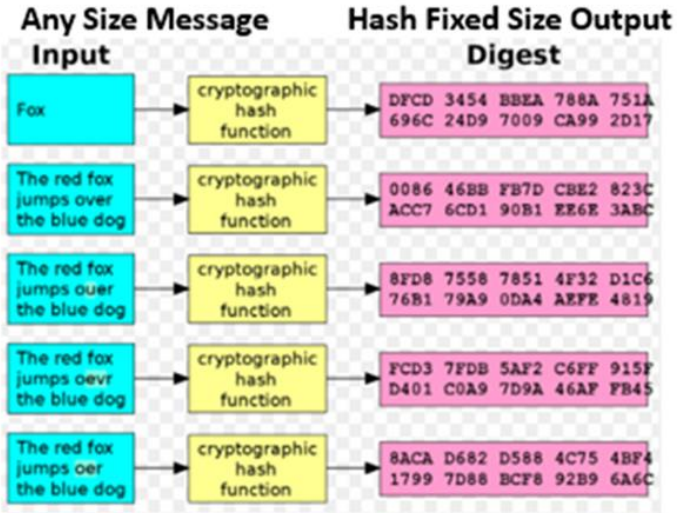


WHAT IS HASH?

- ***Efficient*** cryptographic algorithm (step by step computer programme using mathematical functions to encrypt data: convert plaintext data to unintelligible gibberish)
- Input any size data/message into Hash algorithm program, out pops a fixed length one-of-a-kind unique alpha-numeric 'fingerprint' or 'digest' number
- "One-way" calculation: only encrypts the data, cannot decrypt it.
- Slightest change in data (even adding an extra space) produces completely new hash number – compare with original to confirm unaltered data.
  - Confirms data has not been changed (stored or in transit)
  - Data search (easier to search for book title than book contents)



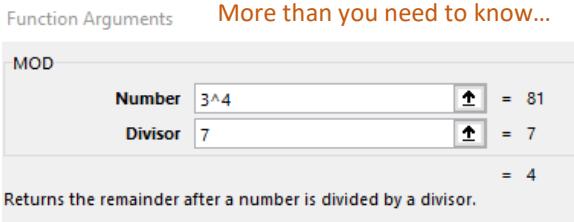
- Online Hash calculators…SHA3-256 popular method



WHAT IS DISCRETE LOGARITHM PROBLEM?

- Discrete Logarithm Problem is:
  - A computer mathematical process for encrypting and decrypting data that is practically impossible to crack! (secret code stuff)
  - Easy to calculate one way, almost impossible to reverse the process.
  - You know the output answer but can't figure out the input…
  - Easy:
    - Guess a number between 1 and 3? (Ans.: 2)
    - If the answer (output) is 9…what number (input) do you multiply (3 x ?) by to get 9? (Ans. 3)
  - Not So Easy
    - If input is 3, what exponent would you raise it to, when divided by 7, results in a remainder of 4?
      - Math speak (3^x / 7) with remainder 4 (a 'modulo' or 'mod' math procedure)* I know, more than you needed to know…
        - (3^4 = 81)/(7) = 11 plus remainder 4
        - x = 4 or 10 works…as does an infinite number of other possibilities!
      - Which x was used in the encryption process??? – a Discrete Logarithm Problem.
      - *'Hidden in plain sight!'* *(know answer, not input)*

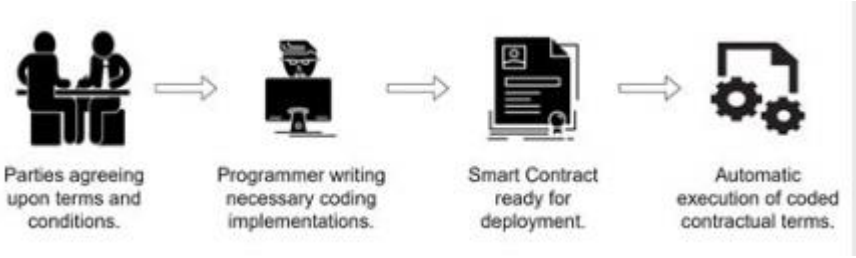
*Excel 'mod' formula
More than you need to know…



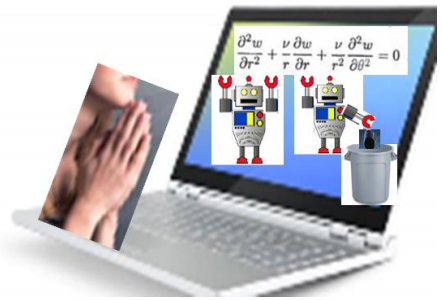
SMART CONTRACT

- A digital contract automatically executed (no matter what!) by computer code without human performance intervention – sort of like death – once started not reversible.
  - Setting home thermostat with mobile phone. Computer code turns on heater not a finger.

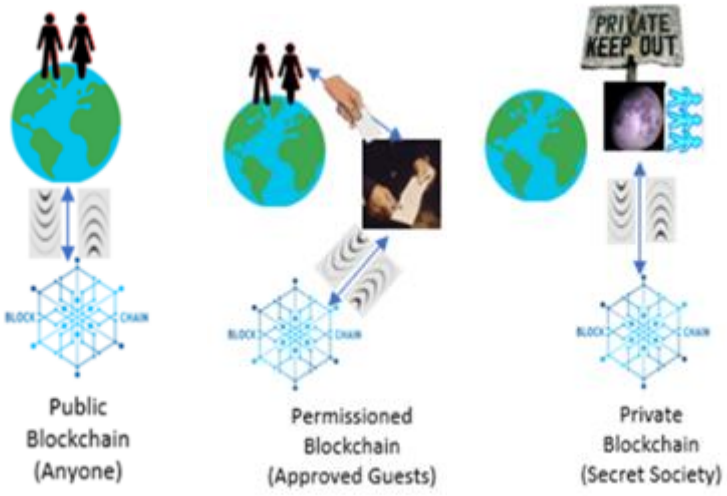
- Example:
  - A certain amount of funds are to be paid to a student when they reach college age in 20 years.
    - If instead of 20, 200 was 'accidentally' inserted, because of the immutable nature of Blockchain ledgers (can't be changed) the funds would not be paid until 200 years!
    - Unlike conventional 'contracts' that can be modified, Blockchains are different
    - Much debate if Smart Contracts should be treated as conventional contracts or merely the execution of programming code, and not a contract.



BLOCKCHAIN TRUST AND FLAVORS

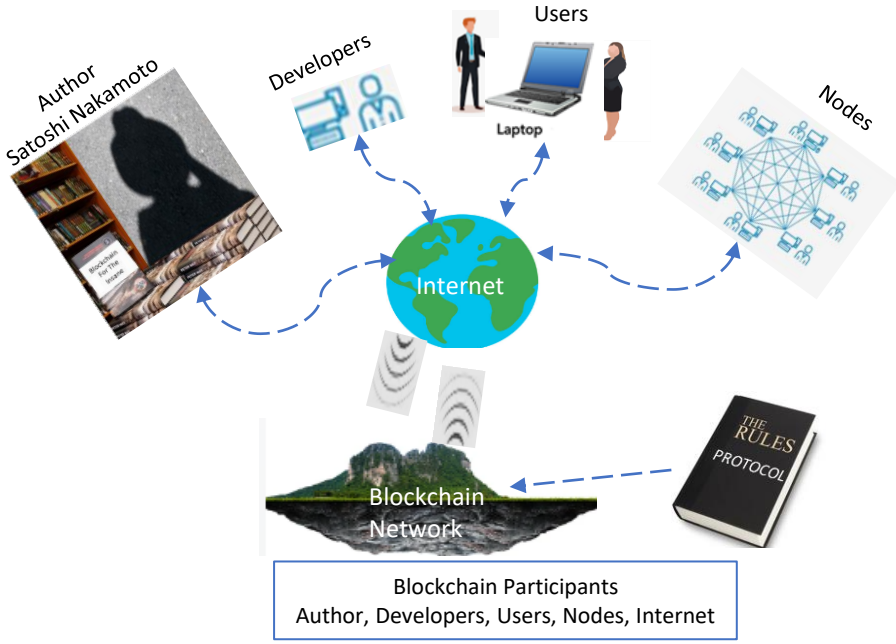


- Blockchain algorithms (computer programs) operate in a 'trustless' environment –
  - Emotionless electron 'auto-pilot' mathematical processes - displaces human trust.
  - This 'auto-pilot' trust includes security tactics against trustless cyber attackers and hackers (the bad folk).
- Three flavors of Blockchain:
  1. $\text{Public}_{\text{Trustless}}$ ('permissionless')
     - Open to the public to participate; Trust no one; Requires Convertible Virtual Currency to operate
     - Examples: Bitcoin and Ethereum Blockchains
  2. $\text{Permissioned}_{\text{Trusted}}$
     - Must obtain permission to participate; Optional to use Convertible Virtual Currency; Participants are known and trust each other
     - Example: Accounting consultant contracted to assist a client.
  3. $\text{Private}_{\text{Trusted}}$
     - Invited participants only; Does not require Convertible Virtual Currency; Participants are known and highly trust each other.
     - Examples: Government agencies sharing data.



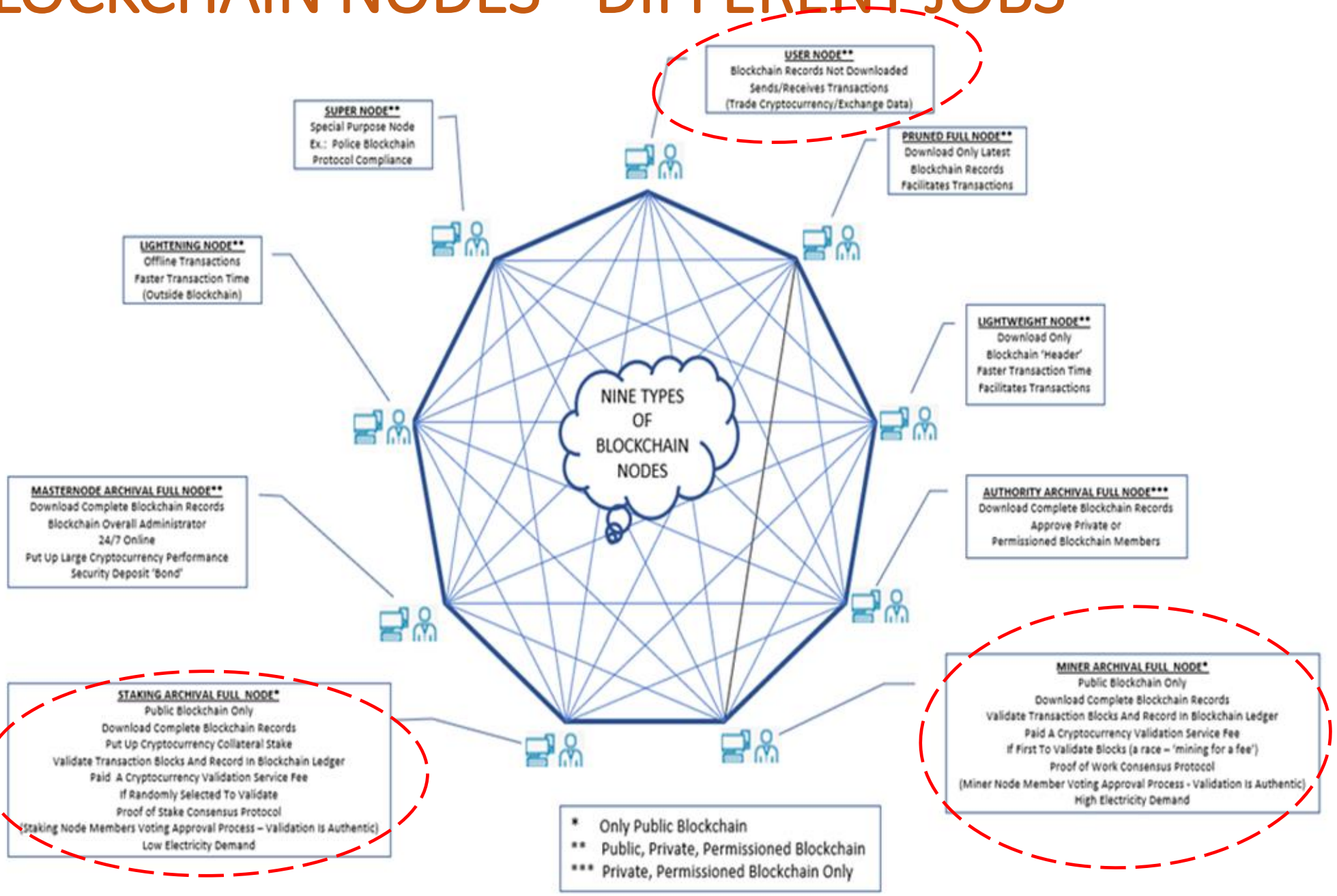
BLOCKCHAIN 5 PARTICIPANT FLAVORS

1. 'Author;: 'Satoshi Nakamoto'
2. Developers:
   - Core: administrators
   - Software: computer programmers
3. Users: Buyers and Sellers of convertible virtual currency (cryptocurrency); day-to-day users
4. Nodes (all participants):
   - Three characteristics:
     - Honest (truthful);
     - Faulty (unintentional fault – offline, power outage) *known as 'Byzantine Faults')
     - Malicious (*behaviour intended to disrupt, disable, destroy, or maliciously control a computing environment/infrastructure or destroy the integrity of the data or stealing controlled information, aka 'Byzantine Faults')*
5. Internet



BLOCKCHAIN NODES - DIFFERENT JOBS

- Nodes:
  - Many types, two most important (Public Blockchains)
  - **User Node** (day-to-day user; creates transactions, buy-sell cryptocurrency)
  - **Miner and Staking Archival Full Nodes** (validates transactions, records transactions in the Blockchain, receives cryptocurrency fee for validation service)



RECORDING BLOCKS TO BLOCKCHAIN

1. **Transaction initiated (User or Node)**

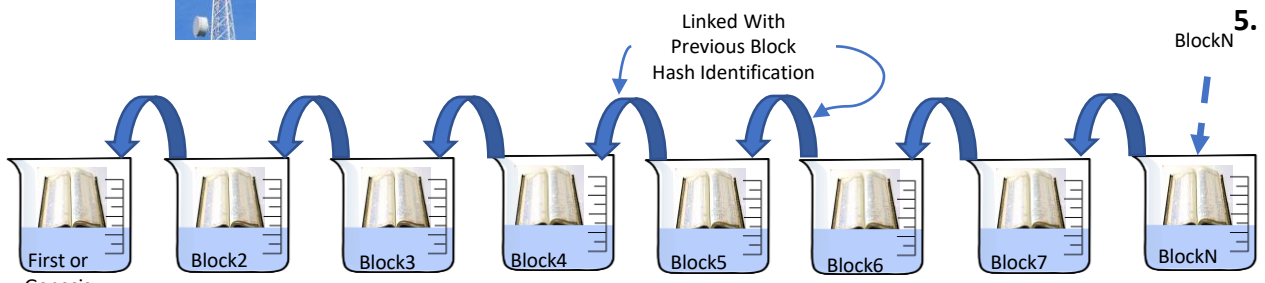
Smart contract or transfer of value
e.g. User A transact with User B
To transfer cryptocurrency
PC Connection to Internet
Access Into Blockchain

2. User transaction Broadcast in the Blockchain network Temporarily stored in 'Mempool'
Awaiting to be verified and Recorded to Blockchain

3. Mempool transactions Grouped into a Block of data Full node (miner) validates authenticity of transactions And first to solves costly mathematical Puzzle (if Proof-of-Work) or Puts up cryptocurrency security Deposit (if Proof-of-Stake) 'mining for new Block'

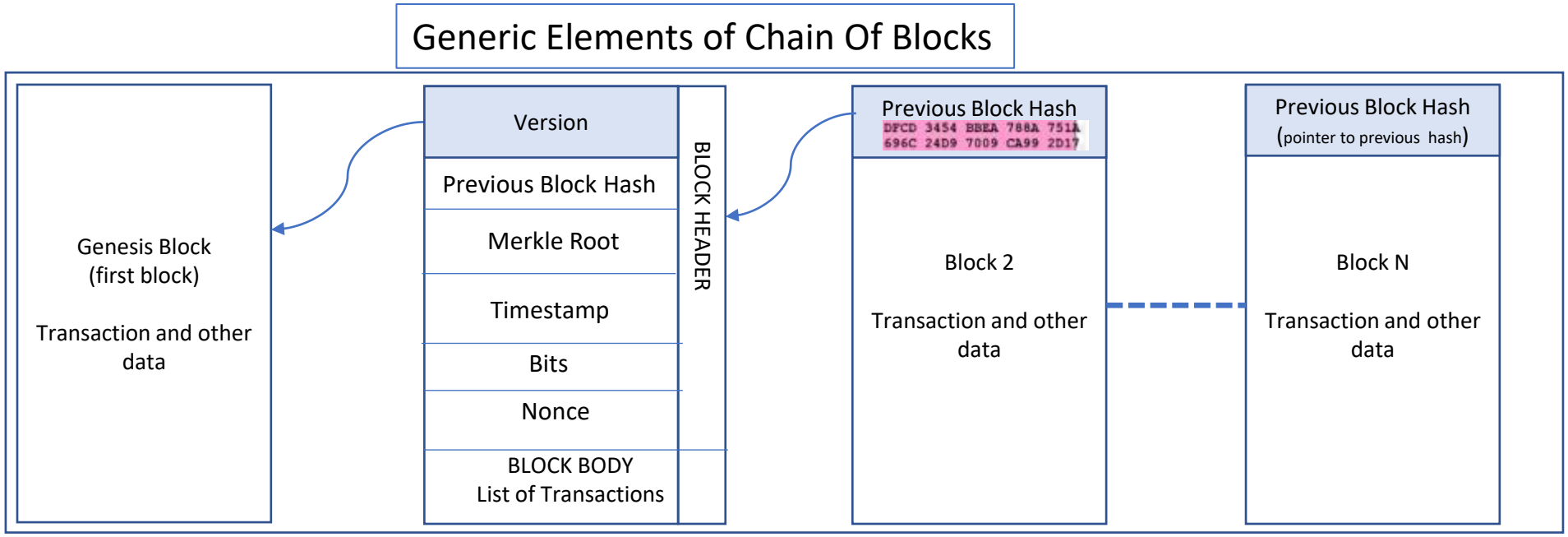
4. New Block Verified Consensus Voting Approval Achieved from other miners To add Block to The Blockchain (Cryptocurrency Mining Fee Paid)

5. Permanently Record New Block to Blockchain (Ledger)



Blocks of data linked together in Blockchain (immutable, non-repudiable)

BLOCKCHAIN BLOCK STRUCTURE BITCOIN



- **Block:** Fixed length, 2000+ transactions plus Block Header information - Table of Contents of Block.
  - **VERSION (1-4):** All Blocks same version else a new Blockchain
  - **PREVIOUS BLOCK HASH:** Unique alphanumeric number hash or digest - a 'fingerprint' identity - of the previous Block; used to link Blocks
  - **MERKLE ROOT:** A summary single hash of all transactions in a Block
  - **TIMESTAMP:** A time of a Block
  - **BITS:** A alpha-numeric 'target' number used with solving the Proof-of-Work puzzle.
  - **NONCE:** Unique random generated one time use number used in Proof-of-Work scheme to solve a complex mathematical puzzle.
  - **Block Body:** Record of transactions in a Block

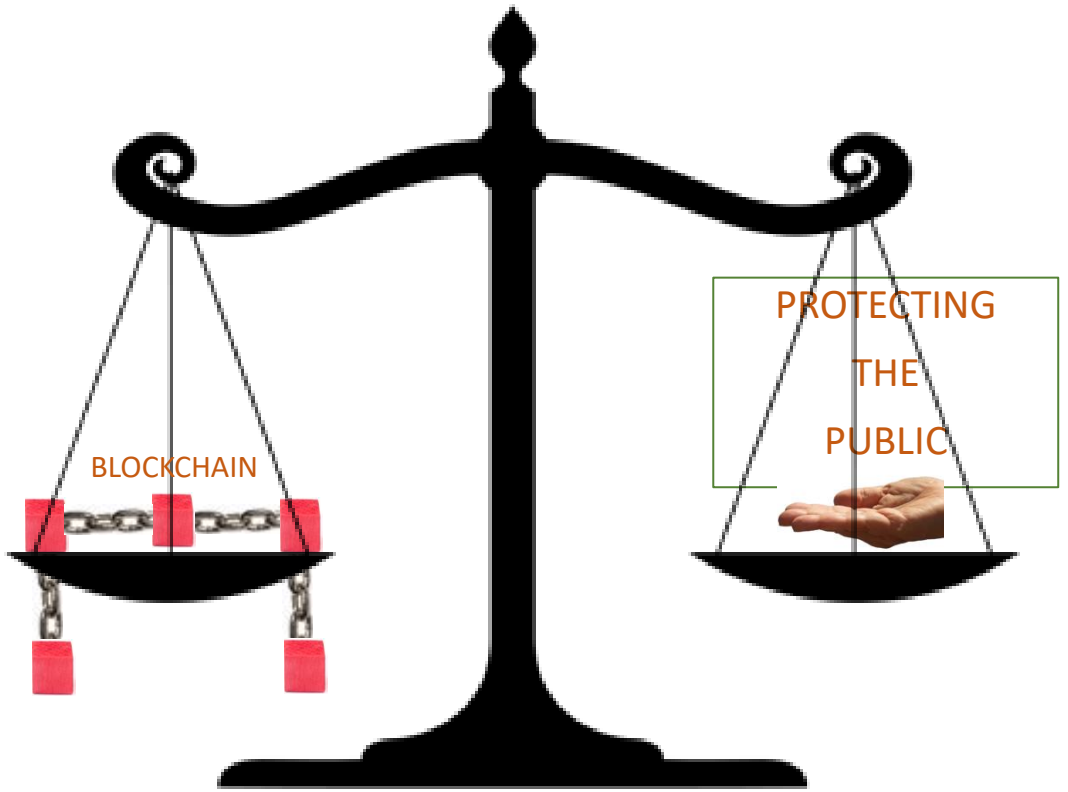
- Algorithm
- Hash
- Discrete Logarithm Problem
- Smart Contract
- Blockchain Types
- Blockchain Participants
- Nodes and Their Jobs
- Recording To The Blockchain
- Blockchain Block Structure

END

BLOCKCHAIN SPECIAL TOPICS

END PART 3

BLOCKCHAIN FOR LEGISLATORS
A USER'S GUIDE…



"DISRUPTIVE TECHNOLOGY PROMOTES PROGRESS"

"DESTRUCTIVE TECHNOLOGY …NOT SO MUCH"

PART 4 OF 4 – BLOCKCHAIN AND CRYPTOGRAPHY – SECRET STUFF…

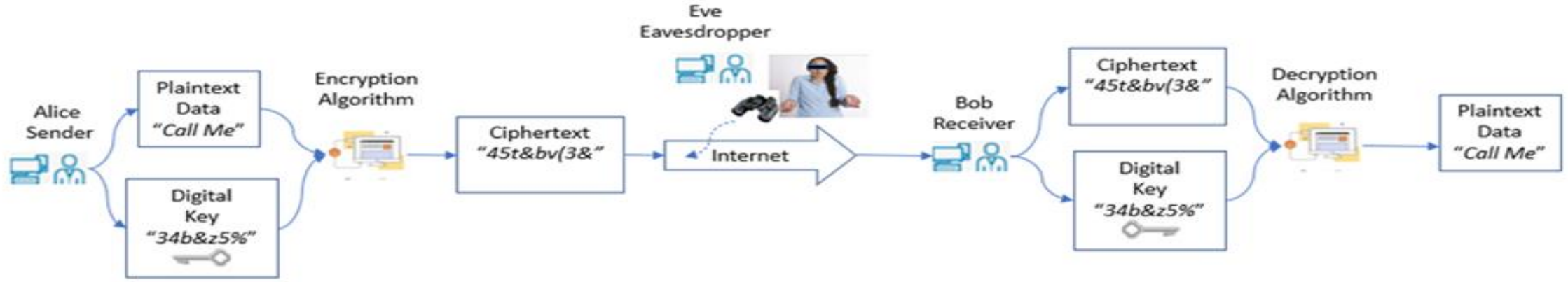
CRYPTOGRAPHY FUNDAMENTALS

- First – some definitions
  - Cryptography: science of keeping things secret. 
  - Encrypt: scrambling understood plaintext to unrecognizable babble: “Hello” = “@8h%b9”
  - Decrypt: unscrambling babble to plaintext: “@8h%b9” = “Hello”
  - Algorithm: computer programme instructions, often based on mathematical functions
  - Cypher/Cipher: same as algorithm; scrambled plaintext data
  - Key (digital): alpha-numeric string of characters (“34&Bt6+”) used to encrypt and decrypt data in an algorithm (used to lock/unlock data)
  - Plaintext: unencrypted understood plain language (English)
  - Protocol: set of rules and operating procedures
  - Authentication: truthful identity of a person or data
  - Trap-door: easy to fall into, hard to get out; a preferred cryptographic technique for encrypting data and unlikely to be cracked by a hacker
  - Prime Number: a number only divided by 1 or itself

WHAT IS ENCRYPTION?

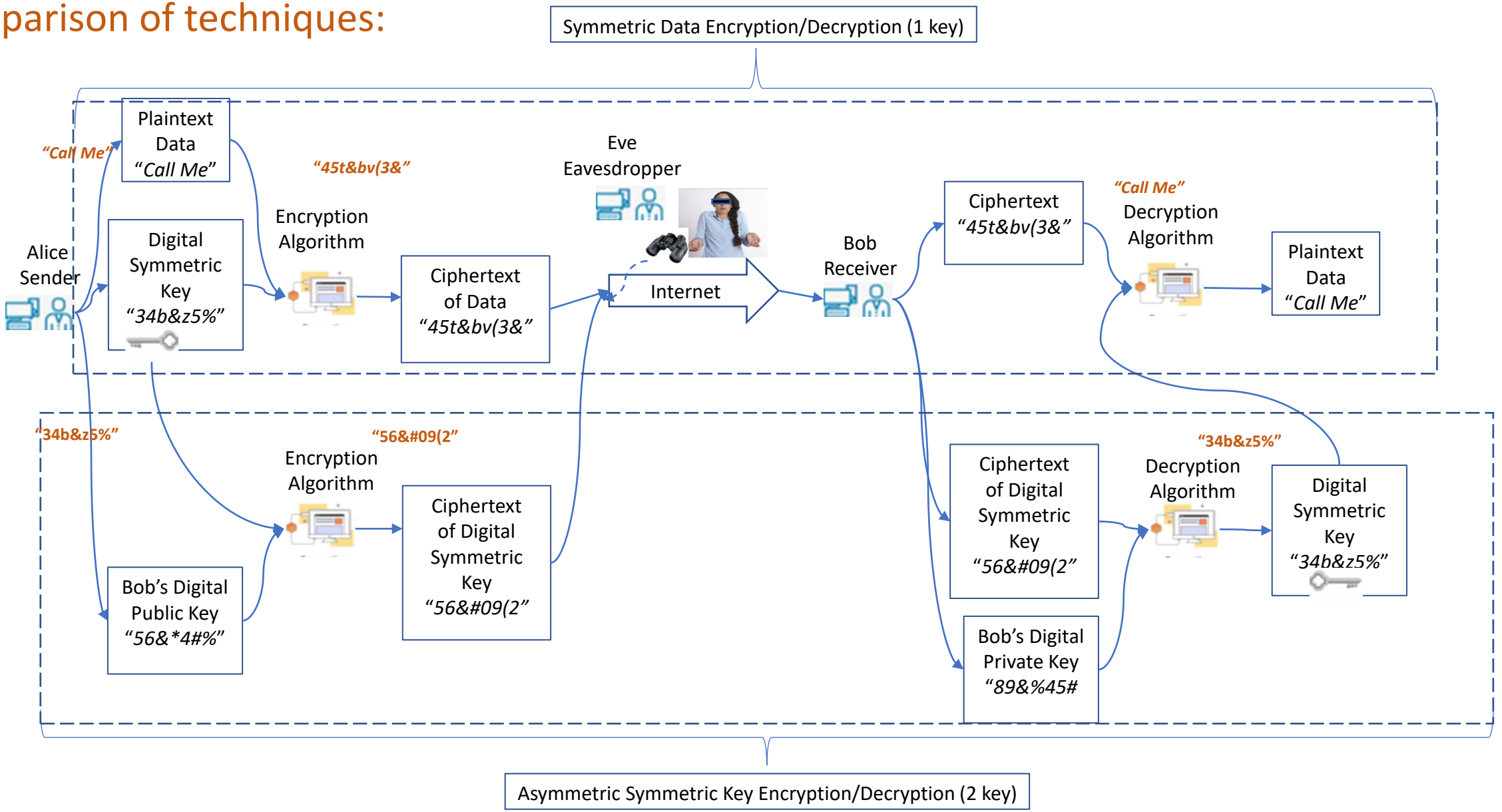
("Credit Card # Used Online")

- Scrambling understandable plaintext to unintelligible cyphertext.
  - ("Hello" becomes "6&Tk").
- How? Plaintext + Key + Algorithm = Cyphertext
- Why?
  - Keep secret from prying eyes or ears.
  - Protect Privacy; Security; Data integrity; Regulations (personal rights to privacy – medical)
- Alpha-numeric keys are used to encrypt data using a computer encryption algorithm.
  - Two types:
    - Symmetric Keys (1 key): One 'secret' key (locks/unlocks data – like house key)
    - Asymmetric Keys (2 keys): Public (everybody sees, locks data) and Private (keep secret, unlocks data) Keys
- Success of encryption measured as its 'hardness': how difficult to crack the encryption.



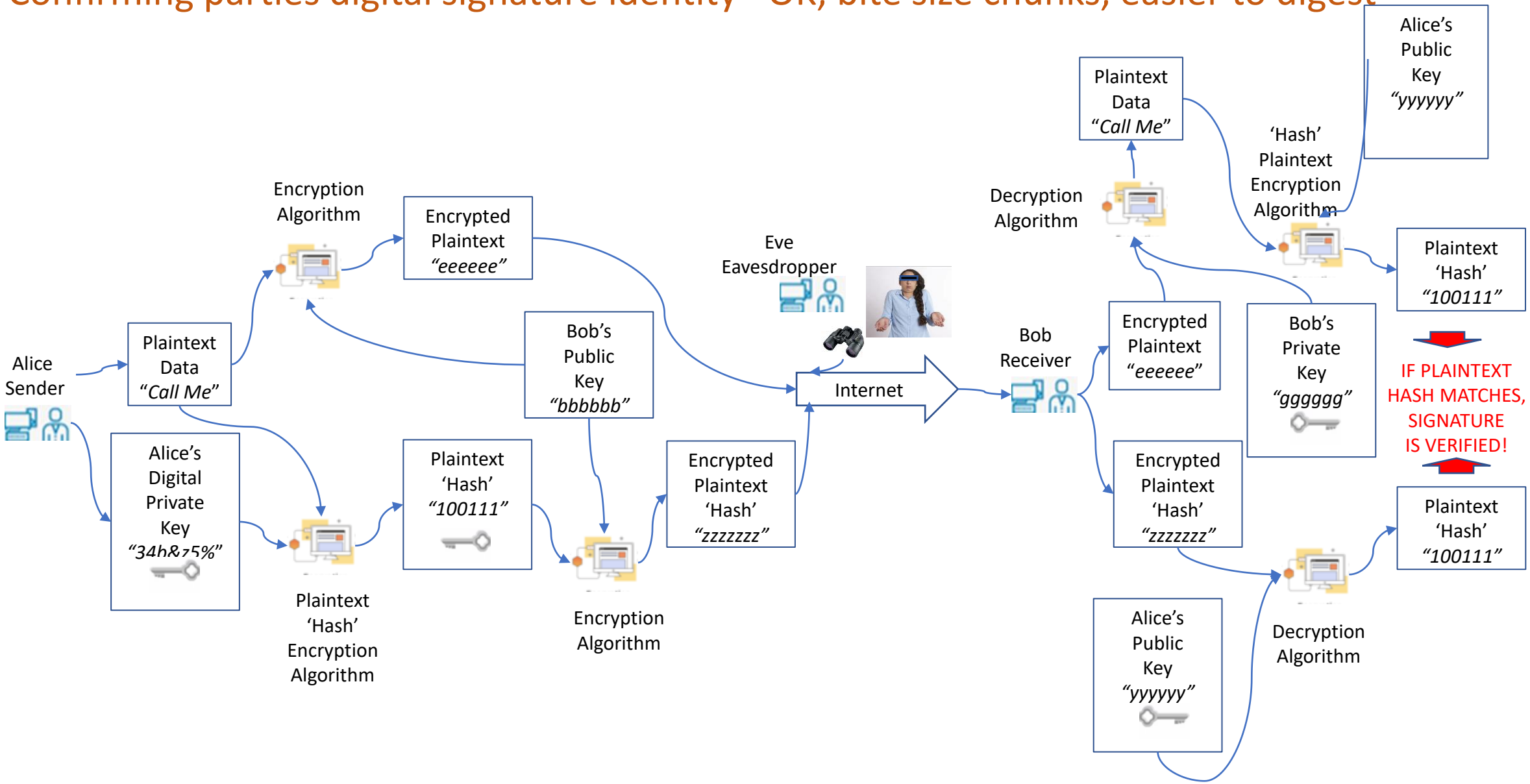
SYMMETRIC / ASSYMETRIC KEY ENCRYPTION

- Comparison of techniques:



DIGITAL SIGNATURE

- Confirming parties digital signature identity –OK, bite size chunks, easier to digest



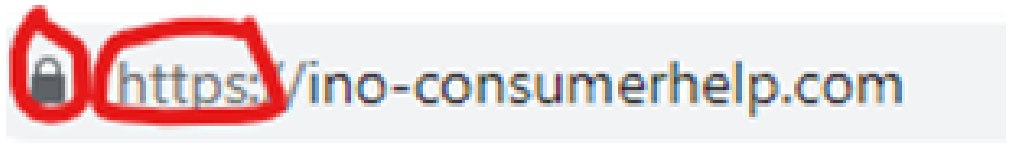
RANDOMNESS AND UNPREDICTABILITY?

- Randomness and unpredictability:
  - Good cryptographic qualities that make it difficult for a hacker to discover…
- Measure randomness with ‘entropy’:
  - High ‘entropy’ - highly chaotic*- unpredictable (good cartography);
  - Low ‘entropy’ - less chaotic* - predictable (poor cartography)
- Randomness calculated by use of:
  - Random Number Generator
    - (RNG, computer programme); not very random
  - Pseudorandom Number Generator
    - (PRNG, using occurrences in nature to determine randomness; number of bees that land on a flower in an hour; lava lamp bubble pictures); better randomness…

Extra: Us humanoids don’t like chaos – why when we look up at clouds we see people, animals or stuff, and not chaotic disorganized clouds…

INTERNET SECURITY?

- Internet security protected by cryptographic communication encryption computer programmes.
  - Authenticity credentials confirmed by independent Certificate Authority
- Logon to Internet: 'Handshake' link up protection with security systems
  - Confirms authenticity of data and internet users
  - Two security techniques:
    - Secure Socket Layer (SSL – old version)
    - Transport Layer Security (TLS – replace SSL)
- Websites best security protection (defend against hackers) is HyperText Transfer Protocol Secure – HTTPS.
  - Look for lock and HTTPS logo to confirm being used by Website.

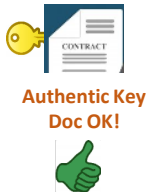


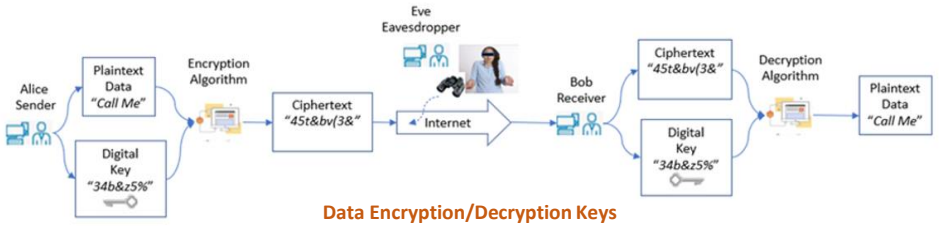
WHAT ARE CRYPTOGRAPHIC KEYS?

Plaintext +  + Algorithm = Security

- **Random alpha-numeric number file** (“9iK76&%gHjr$3#@b01z”), used in algorithms to lock/unlock data

- **Types of keys**:
  - **Signing Keys** digital signatures; prove identity
  - **Authentication Keys** authenticate computers/docs
  - **Data Encryption Keys** encrypt or decrypt data
  - **Session Keys** one time use – send encrypted data across internet
  - **Key Encrypting Keys** a key that encrypts another key
- **How protect**:
  - **Key Escrow**: one key, one file;
  - **Key Recovery** (‘sharding’): Split key, many files





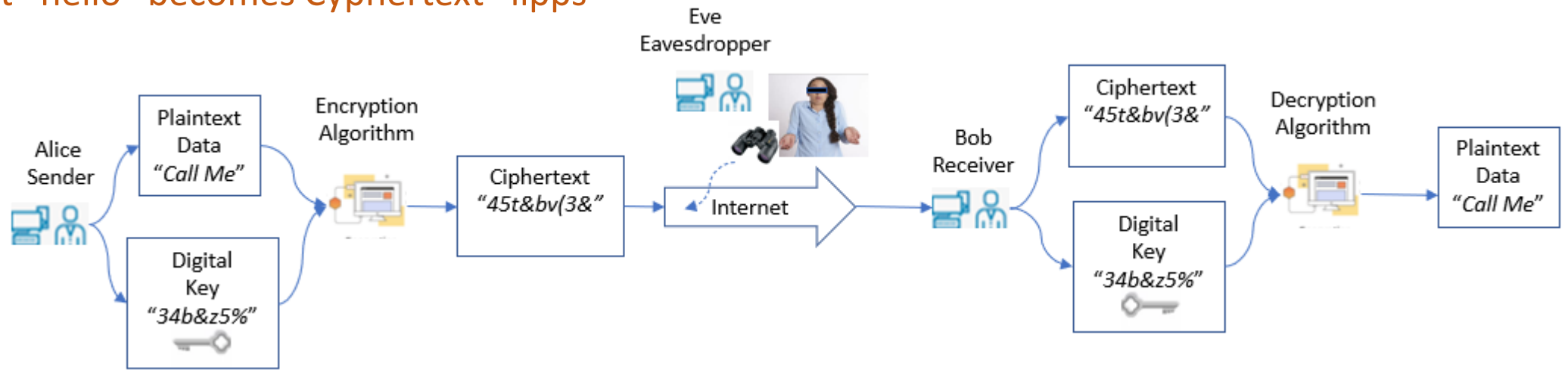
WHAT DO KEYS LOOK LIKE?

- Keys are long string of alpha-numeric characters or ‘numbers’.
- The characters in the keys can be numbers, letters or symbols.
- Example: “GD58%n&00009hKMln03gZ….” is a key.
  - Can contain 256 individual characters or more.
  - Computers convert each character in the key into a combination of 0s and 1s (binary code – the language of computers – ‘bits’ of data).
  - For example:
    - Assume a key is “2G$” (plaintext code)
    - In binary code (0s and 1s) 00110010 01000111 00111111 (computer code)
  - Example of what a real key looks like…


```
publicKey: "-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAvHV6ynCas8MQicMAJqYF
GrnANTyqFjwVKNCtOKFmhV1XrKI+iNVBJ0/MdZSu9B0ppEzgJwoAmFMmwyTAeCeO
OvFVWxmWIjtW3nA3qxpMvcA4oJk0UI6TyFyM/v/uLfHuBRbBkapQ2WCyrRFjb7h1
rSkZpWIGCpSy6e+rH9AW6VF26Knt8ZH2XWrqao3vtqmcMAGtsVOMBl6aavqSrlOU
gMY/36cDl91/9iv8lV0HfTIUvyf08MsZ0jKPG5k2gRXk7/yj4api1eoVYZY+A0I3
6AU6Zm00HAS8AbgbaivsdkMDuz6EQmbr+teulC212BXsTBZYIUFfj/0bYow/Gb7j
VJwAfLPgYzJueEdHXmO5T6wc5Ziwl4ZpPIv6zJr/rxo/BcLTfOKepOqyNDLGHa+z
IydIjWP9j4PMU2ph4sdjgDjVOgICzfEX5lQ5b+cANiMPydJyYD/KP7lNUf9dXVL2
VjUghZnXM6vIB6Nmoq9HfoljlczKhbfHyGPfJ3DBDnyuZAtA3URFBU6VcfgEjGj6
WJcx/Ns2w7EPIJ/zLU6mlchBsHZVwTUXOnVYetIiVmqgEhe87n3bFT5MHEw4xVbV
2qC9qVKd1NfLLeicwQ5shg4DRgSrkqZjm//sRosCgDncjo93w8cnX1K3K4x9D9Dn
yph0OOrPqZ9wQgaQuRPK8IMCAwEAAQ== -----END PUBLIC KEY----- ",
```

HOW ARE KEYS USED?

- Keys are used with algorithms to encrypt or decrypt data and information.
  - Plaintext + Key + $Algorithm_{encryption}$ = Cyphertext
    - "Chocolate is good food" + Key + $Algorithm_{encryption}$ = "ayKIEyMyWcFHz"
  - Cyphertext + Key + $Algorithm_{decryption}$ = Plaintext
    - "ayKIEyMyWcFHz"+ Key + $Algorithm_{decryption}$ = "Chocolate is good food"
- The individual (random) characters in the key are used in different algorithm recipes to convert plaintext characters to unintelligible cyphertext code for transmitting over the internet.
- Super Simple Example:
  - Assume random number generated key is *"abcdefghijklmnopqrstuvwxyz4"*
  - Algorithm is to match plaintext message with key message character and use 4th letter as cyphertext
    - (i.e. 4th character after "a" in key is "e").
  - Plaintext "hello" becomes Cyphertext "lipps"

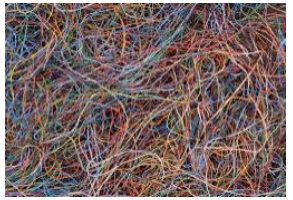


WHERE DO KEYS COME FROM?

- Cryptographic keys are generated from mathematical algorithms – many types.
- Two popular key generator processes:
  - RSA (Rivest–Shamir–Adleman authors); Process generates keys AND encrypts/decrypts data
  - Elliptic Curve Cartography; only generates keys; other algorithm needed to encrypt/decrypt
- All key generation techniques strive to produce unpredictable and random number looking Keys to protect against hacking (chaos is good).

Organized
Predictable
Not Random
Not Chaotic
'LOW ENTROPY'
Poor Encryption Quality

Pick A Whole
Number
Between
1 and 3?



Disorganized
Un-predictable
Random
Chaotic
'HIGH ENTROPY'
Good Encryption Quality

What exponent (x) can
I raise a number (5)
that results in a remainder R of 2
when the number (5^x) is
divided by 7?
5^x / 7 = Remainder of 2
[x = 4 or 10…+ infinite answers…]

PUBLIC AND PRIVATE KEYS

REALLY MORE THAN YOU WANTED TO KNOW!!

- **RSA Math (step by step calculations explained in the Guide)**…
  - *$C = P^e \bmod n$ [C, ciphertext = P, plaintext^e mod n] (the plaintext is converted from non-number characters to number characters and raised to the e power).*
  - **Public Key** is the expression [^{e} ***mod n].***
  - ***Private Key*** *is the expression*[^{d} ***mod n],*** *where* $P = C^d \bmod n$***.***

- **Elliptic Curve Cartography (step by step calculations explained in the Guide)**…(most are proprietary)…
  - **Private key** (randomly selected from n)
    - "n" the "quanta" or ("order") of the elliptic curve being the total number of whole prime number Points on the elliptic curve.
  - **Public key** (determined by Point Add and Point Doubling modular math of N times G or N*G, where G is the Generator Point.

  - If you have read this far you probably think I encrypted my plain English message…unfortunately this is plane English…

END

~~*CARTOGRAPHY*~~

BLOCKCHAIN CRYPTOGRAPHY

END PART 4