diet bitcoin

THE FUTURE OF CRYPTOCURRENCY BY ROBERTO ESCOBAR, BROTHER OF PABLO ESCOBAR

Cryptocurrency Coin (DDX)
White Paper

"I am the first person in the world, Roberto De Jesus Escobar Gaviria, to publicly come out and claim that Bitcoin was created by the American Government, and I am not going to be the last person to say this. The world is going to wake up. The world is going to see that this was created by them. And when they see it, it is too late, and when the CIA founds out that the world knows about this, the CIA is going to sell all of their coins, and they will destroy the value of Bitcoin…That's why I am creating my own cryptocurrency called dietbitcoin (DDX)."

Roberto De Jesús Escobar Gaviria, Founder of Escobar Inc published in his latest book "Pablo Escobar's dietbitcoin" released March 2018

WHITEPAPER VERSION 1.0 15 MARCH 2018

TABLE OF CONTENTS:

IMPORTANT NOTICES

PLEASE CAREFULLY READ THIS SECTION AND THE FOLLOWING SECTIONS ENTITLED "DISCLAIMER OF LIABILITY", "NO REPRESENTATIONS AND WARRANTIES BY ESCOBAR INC", "REPRESENTATIONS AND WARRANTIES BY YOU", "CAUTIONARY NOTE ON FORWARD-LOOKING STATEMENTS", "NO ADVICE", "RESTRICTIONS ON DISTRIBUTION AND DISSEMINATION", "NO OFFER OF SECURITIES OR REGISTRATION" AND "RISKS AND UNCERTAINTIES". IF YOU ARE IN ANY DOUBT AS TO THE ACTION YOU SHOULD TAKE, YOU SHOULD CONSULT YOUR LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S).

The dietbitcoin (DDX) (as defined in the White Paper) are not intended to constitute securities in any jurisdiction. This White Paper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction.

This White Paper does not constitute or form part of any opinion on any advice to sell, or any solicitation of any offer by Escobar Inc to purchase any dietbitcoin (DDX) nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision.

The distributor of the dietbitcoin (DDX)s will be an affiliate of Escobar Inc ("Escobar Inc"), and will deploy all proceeds of sale of the dietbitcoin (DDX)s

to fund Escobar Inc protocol, businesses and operations.

No person is bound to enter into any contract or binding legal commitment in relation to the sale and purchase of the dietbitcoin (DDX)s and no cryptocurrency or other form of payment is to be accepted on the basis of this White Paper.

Any agreement as between the distributor and you as a purchaser, and in relation to any sale and purchase, of dietbitcoin (DDX)s (as referred to in this White Paper) is to be governed by only a separate document setting out the terms and conditions (the "T&Cs") of such agreement. In the event of any inconsistencies between the T&Cs and this White Paper, the former shall prevail.

You are not eligible to purchase any dietbitcoin (DDX)s in the Escobar Inc SAFT pre-sale (as referred to in this White Paper) unless you qualify as an "accredited investor" under U.S. standards.

Accredited investors must purchase dietbitcoin (DDX)s through a SAFT contract until the network launch. Please contact us directly if you are an interested accredited investor.

No regulatory authority has examined or approved of any of the information set out in this White Paper. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of this White Paper does not imply that the applicable laws, regulatory requirements or rules have been complied with.

There are risks and uncertainties associated with Escobar Inc and their respective businesses and operations, the dietbitcoin (DDX)s, and the Coin Sale.

This White Paper, any part thereof or any copy thereof must not be taken or transmitted to any country where distribution or dissemination of this White Paper is prohibited or restricted.

No part of this White Paper is to be reproduced, distributed or disseminated without including this section and the following sections entitled “Disclaimer of Liability”, “No Representations and Warranties by Escobar Inc”, “Representations and Warranties by You”, “Cautionary Note On Forward-Looking Statements”, “No Advice”, “Restrictions On Distribution and Dissemination”, “No Offer of Securities Or Registration” and “Risks and Uncertainties”.

DISCLAIMER OF LIABILITY

To the maximum extent permitted by the applicable laws, regulations and rules, Escobar Inc shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this White Paper or any part thereof by you.

NO REPRESENTATIONS AND WARRANTIES BY ESCOBAR INC

Escobar Inc does not make or purport to make, and hereby disclaims, any representation, warranty or undertaking in any form whatsoever to any entity or person, including any representation, warranty or undertaking in relation to the truth, accuracy and completeness of any of the information set out in this White Paper.

REPRESENTATIONS AND WARRANTIES BY YOU

By accessing and/or accepting possession of any information in this White Paper or such part thereof (as the case may be), you represent and warrant to Escobar Inc as follows:

(a) you agree and acknowledge that the dietbitcoin (DDX)s do not constitute securities in any form in any jurisdiction;

(a.2) you agree and acknowledge that the dietbitcoin (DDX)s are issued and controlled solely by Tecnologias Gigantes, Inc in Belize. Tecnologias Gigantes, Inc is sole responsible for any incurred

liability from any cause, and has signed an exclusive agreement with Escobar Inc for licensing, terms of which are currently confidential.

(b) you agree and acknowledge that this White Paper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities in any jurisdiction or a solicitation for investment in securities and you are not bound to enter into any contract or binding legal commitment and no cryptocurrency or other form of payment is to be accepted on the basis of this White Paper;

(c) you agree and acknowledge that no regulatory authority has examined or approved of the information set out in this White Paper, no action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction and the publication, distribution or dissemination of this White Paper to you does not imply that the applicable laws, regulatory requirements or rules have been complied with;

(d) you agree and acknowledge that this White Paper, the undertaking and/or the completion of the Coin Sale, or future trading of the dietbitcoin (DDX)s on any cryptocurrency exchange, shall not be construed, interpreted or deemed by you as an indication of the merits of Escobar Inc, the dietbitcoin (DDX)s, and the Coin Sale;

(e) the distribution or dissemination of this White Paper, any part thereof or any copy thereof, or acceptance of the same by you, is not prohibited or restricted by the applicable laws, regulations or rules

in your jurisdiction, and where any restrictions in relation to possession are applicable, you have observed and complied with all such restrictions at your own expense and without liability to Escobar Inc;

(f) you agree and acknowledge that in the case where you wish to purchase any dietbitcoin (DDX)s, the dietbitcoin (DDX)s are NOT to be construed, interpreted, classified or treated as:

(i) any kind of currency other than cryptocurrency;

(ii) debentures, stocks or shares issued by any person or entity (whether Escobar Inc), rights, options or derivatives in respect of such debentures, stocks or shares;

(iii) units in a collective investment scheme;

(iv) units in a business trust;

(v) derivatives of units in a business trust; or

(vi) any other security or class of securities.

(g) you are fully aware of and understand that you are NOT eligible to participate in the pre-sale of dietbitcoin (DDX)s if you are NOT an "accredited investor" under United States standards;

(h) you have a basic degree of understanding of cryptocurrencies, blockchainbased software systems, cryptocurrency wallets or other related coin storage mechanisms, blockchain technology and smart contract technology;

(i) you are fully aware and understand that in the case where you wish to purchase any dietbitcoin

(DDX)s, there are risks associated with Escobar Inc and their respective business and operations, the dietbitcoin (DDX)s, and the Coin Sale;

(j) you agree and acknowledge that neither Escobar Inc is liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this White Paper or any part thereof by you; and

(k) all of the above representations and warranties are true, complete, accurate and non- misleading from the time of your access to and/or acceptance of possession this White Paper or any part thereof (as the case may be).

CAUTIONARY NOTE ON FORWARD LOOKING STATEMENTS

This White Paper may contain certain forward-looking statements including, but not limited to, statements as to future operating results and plans that involve risks and uncertainties. We use words such as “expects”, “anticipates”, “believes”, “estimates”, the negative of these terms and similar expressions to identify forward looking statements. Such forward-looking statements involve known and unknown risks, uncertainties and other factors which may cause the actual results, performance or achievements of the Escobar Inc to differ materially from any future results, performance or achievements expressed or implied by those

projected in the forward-looking statements for any reason.

NO ADVICE

No information in this White Paper should be considered to be business, legal, financial or tax advice regarding Escobar Inc, the dietbitcoin (DDX)s, and the Coin Sale. You should consult your own legal, financial, tax or other professional adviser regarding Escobar Inc and their respective businesses and operations, the dietbitcoin (DDX)s, and the Coin Sale. You should be aware that you may be required to bear the financial risk of any purchase of dietbitcoin (DDX)s for an indefinite period of time. All information provided here within and any and all details pertaining to such information is under the sole discretion of Roberto de Jesús Escobar Gaviria and have been provided to Escobar Inc solely by Roberto de Jesús Escobar Gaviria through secure communication. Relying upon any information provided by one party may be deemed unreliable and anyone interested in purchasing any dietbitcoin (DDX)s shall consider prior to making such a decision, to research thoroughly the subject matter before making such a decision. Such decision is the sole liability of the purchaser.

RESTRICTIONS ON DISTRIBUTION AND DISSEMINATION

The distribution or dissemination of this White Paper or any part thereof may be prohibited or restricted by the laws, regulatory requirements and rules of any jurisdiction. In the case where any restriction applies, you are to inform yourself about, and to

observe, any restrictions which are applicable to your possession of this White Paper or such part thereof (as the case may be) at your own expense and without liability to Escobar Inc. Persons to whom a copy of this White Paper has been distributed or disseminated, provided access to or who otherwise have the White Paper in their possession shall not circulate it to any other persons, reproduce or otherwise distribute this White Paper or any information contained herein for any purpose whatsoever nor permit or cause the same to occur.

NO OFFER OF SECURITIES OR REGISTRATION

This White Paper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction. No person is bound to enter into any contract or binding legal commitment and no cryptocurrency or other form of payment is to be accepted on the basis of this White Paper. Any agreement in relation to any sale and purchase of dietbitcoin (DDX)s is to be governed by only the T&Cs of such agreement and no other document. In the event of any inconsistencies between the T&Cs and this White Paper, the former shall prevail.

No regulatory authority has examined or approved of any of the information set out in this White Paper. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of this White Paper does not imply

that the applicable laws, regulatory requirements or rules have been complied with.

RISKS AND UNCERTAINTIES

Prospective purchasers of dietbitcoin (DDX)s should carefully consider and evaluate all risks and uncertainties associated with Escobar Inc and their respective businesses and operations, the dietbitcoin (DDX)s, and the Coin Sale, all information set out in this White Paper and the T&Cs prior to any purchase of dietbitcoin (DDX)s. If any of such risks and uncertainties develops into actual events, the business, financial condition, results of operations and prospects of Escobar Inc could be materially and adversely affected. In such cases, you may lose all or part of the value of the dietbitcoin (DDX)s.

JURISDICTION

Any dispute arising out of or in connection with any contract related to and or the purchase of any dietbitcoin (DDX)s or any dispute regarding any dietbitcoin (DDX)s shall be held in the courts of a location to be determined by Escobar Inc at such time.

SPECIFICATIONS OF DIETBITCOIN INITIAL COIN OFFERING (ICO)

Initial Coin Offering (ICO):

ICO Crowdsale Info:	1,000,000 coins
Pre-ICO Round 1:	300,000 at $50
Pre-ICO Round 2:	300,000 at $100
ICO (1Round Only):	400,000 at $1,000

Coin Specification:

Name:	dietbitcoin
Symbol:	DDX
Total Coin Supply:	Appx. 1,800,000 at launch
Total Possible Supply:	21,000,000
Algo:	Sha-256
Type:	PoW
Mining Pool:	Coming soon

dietbitcoin

WHAT IS DIETBITCOIN?

dietbitcoin is a faster, lighter alternative to bitcoin.

dietbitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of dietbitcoins is carried out collectively by the network. dietbitcoin is open-source; its design is public, nobody owns or controls dietbitcoin and everyone can take part. Through many of its unique properties, dietbitcoin allows exciting uses that could not be covered by any previous payment system.

dietbitcoin

dietbitcoin uses a blockchain which is not controlled by any third party nor government agency. It is open source which allows for increased security. All transactions are recorded on the blockchain, which is decentralized and spread across a global network of computers.

You can store dietbitcoins on your desktop, laptop,

server, android wallet, iOS wallet, mobile devices, hardware wallet, or in the cloud.

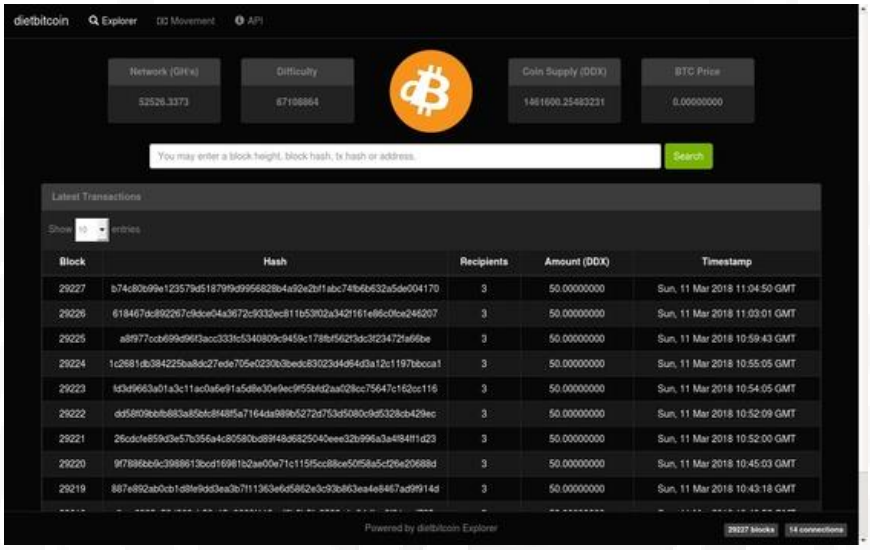
You can quickly and easily transfer dietbitcoins to anywhere in the world as long as you are connected to the internet. dietbitcoins can be received by any dietbitcoin address.

DIETBITCOIN BLOCKCHAIN

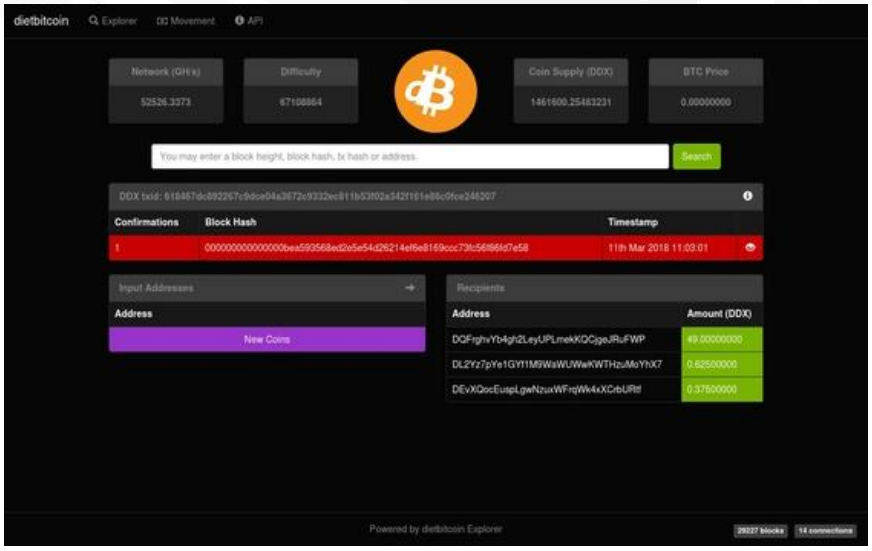
You can view the dietbitcoin blockchain ledger on Explorer 1 below. The coin is currently active, in existence and fully functional.

http://explorer.dietbitcoincore.org

Screenshot 1 of Blockchain explorer:



Screenshot 2 of Blockchain explorer:



OUR TEAM

ROBERTO DE JESÚS ESCOBAR GAVIRIA, FOUNDER

Roberto de Jesús Escobar Gaviria is the biological older brother of the notorious Colombian businessman Pablo Emilio Escobar Gaviria. Prior to his brother Pablo's untimely passing in 1993, Roberto was the accountant of all of Pablo's businesses and enterprises and his most trusted confidant. Roberto was responsible for the creation of offshore entities and the opening of bank accounts, as well as the management of same. In 2014 he founded the holding company Escobar Inc, a holding company for the intellectual property rights to his family name and his brother's name. Roberto is responsible for maintaining the estate of his brother. Roberto has written multiple books regarding his prior business activities. Roberto has made in excess of $100 billion dollars in profit throughout his very successful and long career.

OLOF K. GUSTAFSSON, CHIEF EXECUTIVE OFFICER

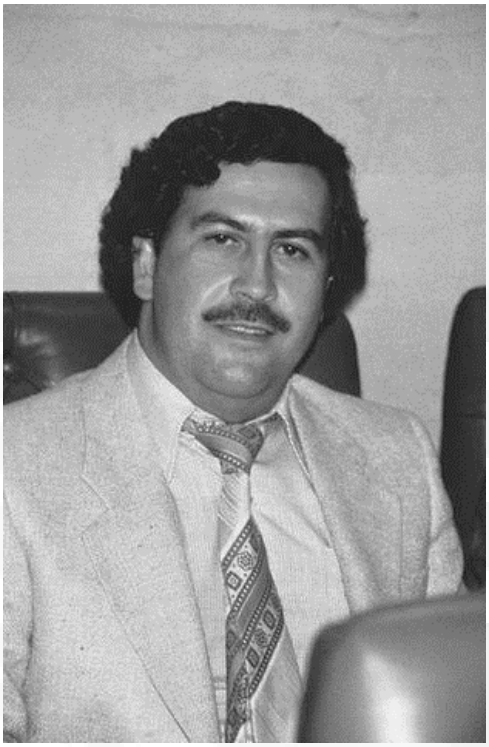
Olof K. Gustafsson has experience working in the informational technology and web technology space. He has also worked with several families and major brands through ownership of intellectual property rights. Mr. Gustafsson has been the Chief Executive Officer of Escobar Inc since 2014 by appointment of Roberto de Jesús Escobar Gaviria and has through his leadership led the company through several milestones which have developed and enhanced the enterprise value of Escobar Inc for the Escobar family and for Roberto de Jesús Escobar Gaviria.

DANIEL D. REITBERG, CHIEF OPERATING OFFICER

Daniel D. Reitberg has experience working in the cryptocurrency field by developing and investing in the development of blockchain technology. He has a wide variety of knowledge in technology and private investment management and trading by having traded his own portfolios over the last 20 years. His role at Escobar Inc has evolved through the years and he is currently managing the intellectual property rights and trademarks owned by the Escobar family at the discretion of Roberto de Jesús Escobar Gaviria. He is responsible for delegating day-to-day operations in co-operation with managers who in turn delegates to the employees and third-party consultants of Escobar Inc.

WHO IS PABLO ESCOBAR?

Pablo Emilio Escobar Gaviria was a renowned businessman based in Colombia, who owned several businesses which he operated together with his brother Roberto De Jesus Escobar Gaviria. At the peak of his career it is estimated he made more than $20 billion per year in profit, for a period of over 10 years.



Pablo Emilio Escobar Gaviria

His legacy is protected by Roberto Escobar through Escobar Incorporated (Escobar Inc) based out of the hometown of both brothers, Medellín, Colombia.

WHAT THE CENTRAL MANAGEMENT WILL DO TO ENHANCE DIETBITCOIN

Roberto Escobar has assembled a team of personnel that will undertake the responsibility to help him develop some aspects of dietbitcoin such as…:

….marketing efforts to improve the usage of dietbitcoin

…incentives to retailers and merchants to commence the usage of dietbitcoin

…daily management of mining operations

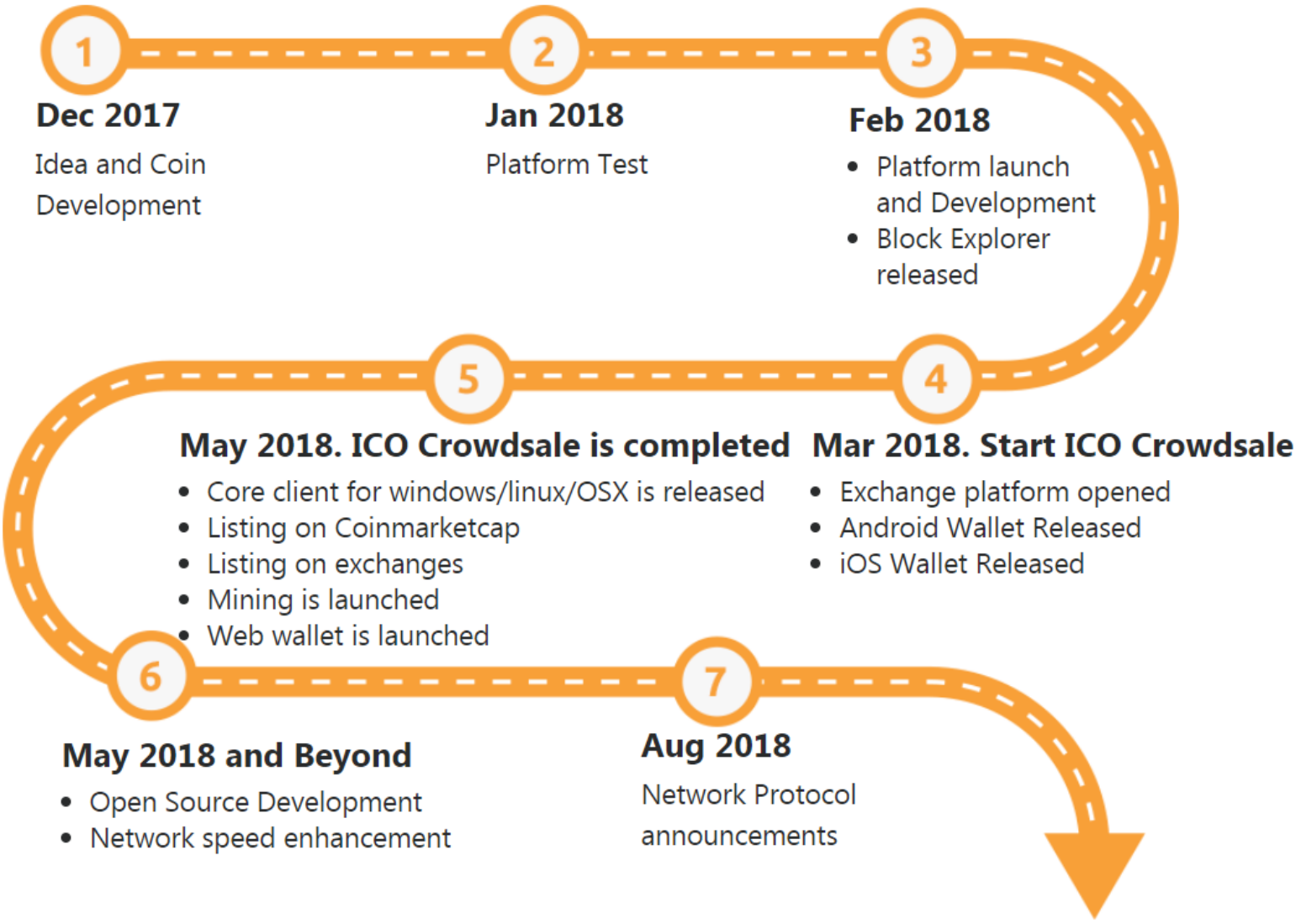
…daily management of all other tasks relating to dietbitcoin

…develop and maintain all applications including but not limited to (a) dietbitcoin core software, (b) web development, (c) android application development, (d) iOS application development, (e) point of sale and purchase application development

Please note that even though there is a central management team in place, the currency itself is completely decentralized. The management teams sole objective is to enhance the user-experience.

dietbitcoin

ROADMAP

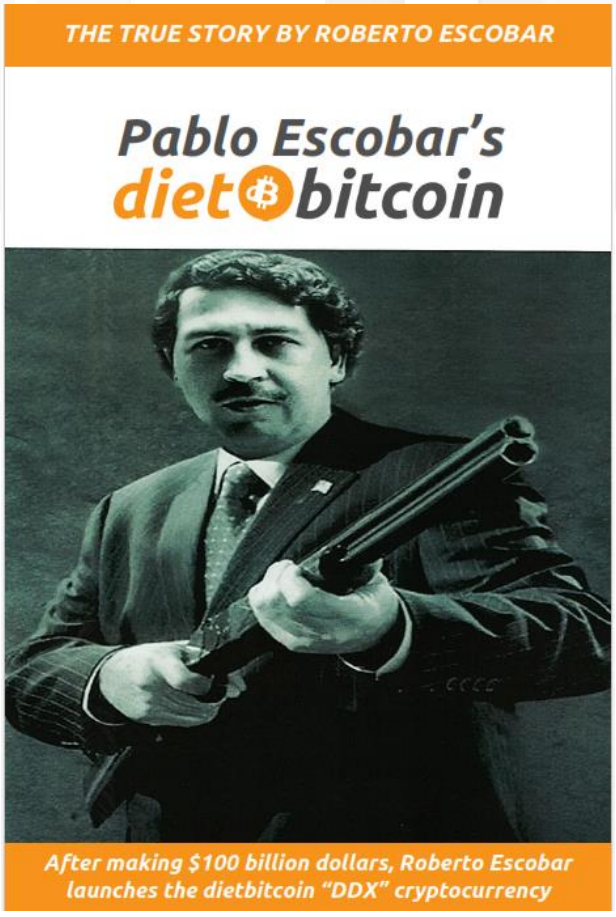


dietbitcoin

PABLO ESCOBAR'S DIETBITCOIN (THE BOOK)

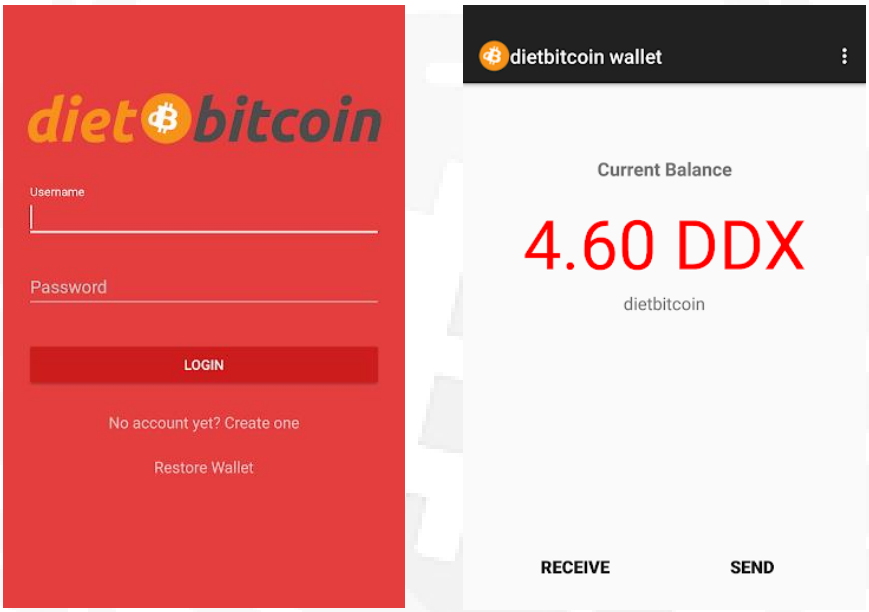
In the middle of 2017, Roberto Escobar had decided to create his own cryptocurrency which is now launched. You can read more details as to some of the reasons behind him launching this currency and follow his journey, in his latest book that is available for a FREE download at Amazon Kindle and Google Play Store as well as on the PDF link below.

Free Download of "Pablo Escobar's dietbitcoin" book: http://01100011.org/index.pdf



DIETBITCOIN ANDROID WALLET APPLICATION

The dietbitcoin android wallet application is already finished and available today for download in the Google Play Store. Anybody can take control of their dietbitcoin transactions while on the go with this secure, privacy-centric lightweight mobile app.



DIETBITCOIN IOS (APPLE) WALLET APPLICATION

The dietbitcoin iOS (apple) wallet application is set to be released on March 30, 2018.

dietbitcoin

DIETBITCOIN POINT OF SALE ANDROID APPLICATION

The application which enables users to spend their dietbitcoin and for retailers/merchants to connect to such a Point of Sale system is currently in development stage and set to release April 13, 2018. This will be enabled through a customized 10-inch tablet PC that will run a custom POS/POP application.

See below a photo of one actual physical unit which is currently in development stage:

INNOVATION BEHIND DIETBITCOIN

INNOVATION IN PAYMENT SYSTEMS

The dietbitcoin protocol is not just about sending money from A to B. It has many features and opens many possibilities that the community is still exploring. Here are some of the technologies currently being researched and in some cases, turned into real products and services. The most interesting uses of dietbitcoin are probably still to be discovered.

CONTROL AGAINST FRAUD

An unprecedented level of security is possible with dietbitcoin. The network provides users with protection against most prevalent frauds like chargebacks or unwanted charges, and dietbitcoins are impossible to counterfeit. Users can backup or encrypt their wallet and hardware wallets could make it very difficult to steal or lose money in the future. dietbitcoin is designed to allow its users to have complete control over their money.

GLOBAL ACCESSIBILITY

All payments in the world can be fully interoperable. dietbitcoin allows any bank, business or individual to securely send and receive payments anywhere at any time, with or without a bank account. dietbitcoin is available in a large number of countries that still remain out of reach for most payment systems due to their own limitations. dietbitcoin increases global

access to commerce and it can help international trades to flourish.

COST EFFICIENCY

With the use of cryptography, secure payments are possible without slow and costly middlemen. A dietbitcoin transaction can be much cheaper than its alternatives and be completed in a short time. This means dietbitcoin holds some potential to become a common way to transfer any currency in the future. dietbitcoin could also play a role in reducing poverty in many countries by cutting high transaction fees on workers' salary.

TIPS AND DONATIONS

dietbitcoin has been a particularly efficient solution for tips and donations in several cases. Sending a payment only requires one click and receiving donations can be as simple as displaying a QR code. Donations can be visible for the public, giving increased transparency for non-profit organizations. In cases of emergencies such as natural disasters, dietbitcoin donations could contribute to a faster international response.

CROWDFUNDING

dietbitcoin can be used to run Kickstarter-like crowdfunding campaigns, in which individuals pledge money to a project that is taken from them only if enough pledges are received to meet the

target. Such assurance contracts are processed by the dietbitcoin protocol, which prevents a transaction from taking place until all conditions have been met.

MICRO PAYMENTS

Imagine listening to Internet radio paid by the second, viewing web pages with a small tip for each ad not shown, or buying bandwidth from a WiFi hotspot by the kilobyte. dietbitcoin is efficient enough to make all of these ideas possible.

DISPUTE MEDIATION

dietbitcoin can be used to develop innovative dispute mediation services using multiple signatures. Such services could make it possible for a third party to approve or reject a transaction in case of disagreement between the other parties without having control on their money. Since these services would be compatible with any user and merchant using dietbitcoin, this would likely lead to free competition and higher quality standards.

MULTI-SIGNATURE ACCOUNTS

Multiple signatures allow a transaction to be accepted by the network only if a certain number of a defined group of persons agree to sign the transaction. This could be used by a board of directors to prevent any member to spend parts of their treasury without other members' consent. This

can also be used by banks to prevent theft by blocking payments above a threshold if the user does not provide additional credentials.

TRUST AND INTEGRITY

dietbitcoin offers solutions to many of the trust problems that plague banks. With selective accounting transparency, digital contracts, and irreversible transactions, dietbitcoin can be used as a ground to restore trust and agreement. Crooked banks cannot cheat the system to make a profit at the expense of other banks or the public. A future in which major banks would support dietbitcoin could help to reinstate integrity and trust in financial institutions.

RESILIENCE AND DECENTRALIZATION

By its high decentralization, dietbitcoin created a different form of payment network with an increased level of resilience and redundancy. dietbitcoin can handle millions of dollars in trades without requiring military protection. With no central point of failure such as a data center, attacking the network is a more difficult project. dietbitcoin could represent an interesting step forward in securing local and global financial systems.

FLEXIBLE TRANSPARENCY

All dietbitcoin transactions are public and transparent and the identity of the people behind the payments is private by default. This allows individuals and organizations to work with flexible transparency rules. For instance, a business can choose to reveal certain transactions and balances only to certain employees just like a non-profit organization is free to allow the public to see how much they receive in daily and monthly donations.

AUTOMATED SOLUTIONS

Automated services usually have to deal with costs and limitations of cash or credit card payments. This includes all kinds of vending machines, from bus ticket booths to coffee machines. dietbitcoin is suited to be used in a new generation of automated services as well as to cut their operating costs. Imagine self-driving taxis, or a store where your basket lets you pay your purchases without waiting at the queue. Many ideas are possible.

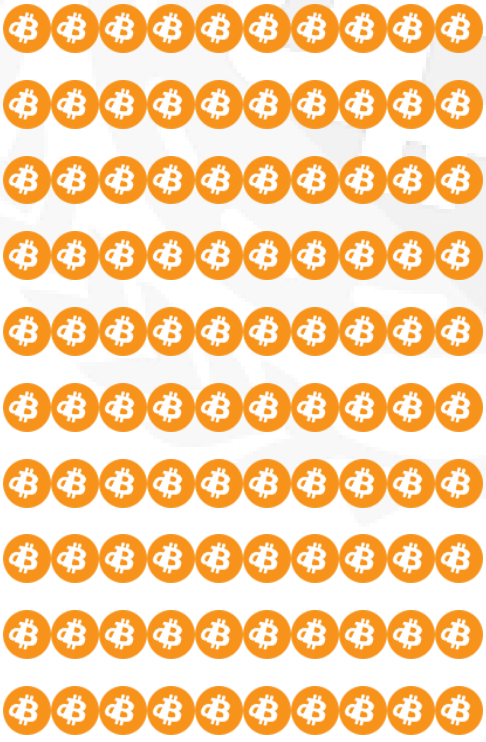
dietbitcoin

FINANCIAL PROJECTIONS

Roberto Escobar believes that it is possible for dietbitcoin to trade near 5000 USD per coin, due to the strategic alliances he will strike with several parties and contracts that will be negotiated, favorably for dietbitcoin users.

AS PER ROBERTO ESCOBAR, 1 DIETBITCOIN (DDX) TODAY….

COULD BE WORTH THE EQUIVALENT OF….



…UP TO 100 DIETBITCOIN (DDX)S WITHIN THE NEXT 1 YEAR IF ROBERTO ESCOBAR IS RIGHT IN HIS PREDICTION

PRICING STRUCTURE

UNTIL APRIL 15, 2018:

1 dietbitcoin (DDX) = USD $50.00

APRIL 15 – APRIL 30, 2018:

1 dietbitcoin (DDX) = USD $100.00

MAY 1, 2018 AND ONWARDS:

1 dietbitcoin (DDX) = USD $1,000.00

INITIAL ICO LIST PRICE:

1 dietbitcoin (DDX) = USD $1,000.00

DIETBITCOIN OFFICIAL WEBSITES

www.dietbitcoinICO.org
Purchase dietbitcoins here

www.dietbitcoin.org
General information about dietbitcoin

www.dietbitcoincore.org
Download dietbitcoin core client (at launch) to run a full node

http://01100011.org/index.pdf
Free download of Roberto Escobar's book "Pablo Escobar's dietbitcoin"

www.escobarinc.com
Official website for Escobar Inc holding company.

EXPLANATION OF THE PEER 2 PEER TECHNOLOGY BEHIND DIETBITCOIN (NOTE:ADVANCED READING)

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

INTRODUCTION

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions,

it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as

honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

TRANSACTIONS

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

The problem of course is the payee can't verify that one of the owners did not double- spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history

of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

TIMESTAMP SERVER

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

PROOF-OF-WORK

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA- 256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof- of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to

change the block would include redoing all the blocks after it.

The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of- work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

NETWORK

The steps to run the network are as follows:

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work for its block.

4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid and not already spent.
6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

INCENTIVE

By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady

addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

RECLAIMING DISK SPACE

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

SIMPLIFIED PAYMENT VERIFICATION

It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.

As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run

their own nodes for more independent security and quicker verification.

COMBINING AND SPLITTING VALUE

Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.

It should be noted that fan -out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

PRIVACY

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual

trades, the "tape", is made public, but without telling who the parties were.

As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

CALCULATIONS

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite

number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block q = probability the attacker finds the next block

qz = probability the attacker will ever catch up from z blocks behind

q z={q /1p z ifif pp≤qq}

Given our assumption that p > q, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after

it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value: =z qp

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

∞ k e – z–k if k ≤ z }

Σ · q / p

k =0 k ! { 1 if k z

Rearranging to avoid summing the infinite tail of the distribution...

z k e– z– k

1–Σ k! 1– q / p

k =0

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda
    = z * (q / p);
    double  sum  =
    1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson =
        exp(-lambda);
        for (i = 1; i <=
        k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

q=0.1

z=0 P=1.0000000 z=1 P=0.2045873 z=2 P=0.0509779 z=3 P=0.0131722 z=4 P=0.0034552 z=5 P=0.0009137 z=6 P=0.0002428 z=7 P=0.0000647 z=8 P=0.0000173 z=9 P=0.0000046 z=10 P=0.0000012

q=0.3

z=0 P=1.0000000 z=5 P=0.1773523 z=10 P=0.0416605 z=15 P=0.0101008 z=20 P=0.0024804 z=25 P=0.0006132 z=30 P=0.0001522 z=35 P=0.0000379 z=40 P=0.0000095 z=45 P=0.0000024 z=50 P=0.0000006

Solving for P less than 0.1%...

P < 0.001 q=0.10 z=5 q=0.15 z=8 q=0.20 z=11 q=0.25 z=15 q=0.30 z=24 q=0.35 z=41 q=0.40 z=89 q=0.45 z=340

CONCLUSION

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double- spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

JOIN TODAY

www.dietbitcoinICO.org