UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

ORÁCULOS DISTRIBUIDOS EN LA BLOCKCHAIN

TESIS PARA OPTAR AL GRADO DE MAGÍSTER EN CIENCIAS MENCIÓN COMPUTACIÓN

MEMORIA PARA OPTAR AL GRADO DE INGENIERO CIVIL EN COMPUTACIÓN

FRANCISCO JAVIER ANDRÉS MONTOTO MONROY

PROFESOR GUÍA:
ALEJANDRO HEVIA

MIEMBROS DE LA COMISIÓN:
INTEGRANTE 1
INTEGRANTE2
INTEGRANTE3

SANTIAGO DE CHILE
MES AÑO

RESUMEN DE LA MEMORIA PARA OPTAR
AL TÍTULO DE
POR: FRANCISCO JAVIER ANDRÉS MONTOTO MONROY
FECHA: MES AÑO
PROF. GUÍA: ALEJANDRO HEVIA

ORÁCULOS DISTRIBUIDOS EN LA BLOCKCHAIN

Este es un resumen muy resumido

Una dedicatoria corta. Por ejemplo, A los creadores de U-Campus

Agradecimientos

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1. Cryptocurrency

Digital currency refers to any currency stored and transferred electronically. A subset of the digital currencies is called virtual currencies: them are usually defined as a « *unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community*».

Based on the interaction of the currency with currencies outside the community there are three types of virtual currencies: The ones with almost no interaction with the outside money, this is usually the case of video games, where its currency is only valuable within the game. A second type is where the currency can be purchased directly using other currency. Here, we observe an unidirectional flow. The third type is when the flow is bi directional, the users can sell and buy the currency.

A cryptocurrency is a bi directional virtual currency, that uses cryptography for security and anti-counterfeiting measures. Virtual currencies are been historically linked to cryptography, the first known investigations to establish a virtual currency where lead by David Chaum, an American cryptographer. However, despite his and others effort (e-gold[1], Ecash, DigiCash, LibertyReserve, among others), virtual currencies never where massively adopted.

By late 2008, using a pseudonym, was released a short whitepaper with yet another virtual currency protocol specification. A few months later, during 2009 its implementation was made available as open source code. The main difference with previous implementations was its lack of a central organization, this new coin was completely decentralized. The software started to being run by some early enthusiasts and Bitcoin gave the step from an idea to an usable coin. The first years was the coins were exchanged for free among the community users. However, at some point the community was big enough and its members started to give value to the coin, then the first exchanges from and to other coins started to take place. Bitcoin transitioned into a bi directional flow virtual coin.

[1] https://www.wired.com/2009/06/e-gold/

Then the first online exchanges between bitcoin and other currencies started to appear, the coin started to gain traction as people outside the community were able to buy and sell coins. As the money became popular, the idea was taken and a whole generation of cryptocurrencies were born. Today the market capitalization of Bitcoin (this is the amount of money times its value in USD) is over US$ 25,000,000,000 USD.

1.2. Gambling

Gambling is the activity of predicting events and placing a wager on the uncertain outcome, with the intent of winning money or valuable goods. Among the most common gambling forms we can find lotteries, casino and sport results.

Usually there is a big amoung of money or valuable goods at stake, this inevitably intails a lot of interest on them, and governments are not the exception. Gambling is heavily regulated and taxed it is also not unusual that lotteries are owned by the state. Legal gambling can provides significant government revenue in some states, as Monaco or Macau, China.

Gambling not only takes place in casinos or lotteries, it can involve two or more individuals with no intermediaries. But both ways share a common obstacle, they need to trust in the other parties to pay if they lose. Even if the bet takes place in a casino, where the law can enforce the bet, is not certain the casino will be able to pay after the resolution.

Una apuesta es una forma de juego basada en el azar o la predicción de eventos futuros, en la que toman parte al menos dos participantes. Cada participante realiza una predicción, disjunta de la del otro participante, sobre el evento y quien acierta es el ganador. El ganador recibe un beneficio pactado al momento de realizar la apuesta, en desmedro del perdedor. Usualmente el beneficio es dinero o un bien valioso, que el otro jugador provee.

Un problema inherente a las apuestas es la resolución de ésta, es decir que el perdedor transfiera lo apostado al ganador. Una solución para este problema es transferir los bienes apostados a una tercera entidad en la que ambas partes confíen, para que una vez resuelta la apuesta haga llegar los bienes al ganador. Otra solución es apostar en entidades reguladas, que de negarse a pagar tras perder el ganador puede concurrir a las autoridades encargadas de hacer cumplir la ley para obligar al perdedor a pagar. Las entidades más conocidas bajo esta modalidad son las casas de apuestas y los casinos.

Las tres formas de apuestas descritas comparten una debilidad común, todas requieren que los apostadores confíen en otro ente. En el primer caso y más simple, cada participante debe confiar en el otro. En el segundo, todos los participantes confían en un tercero, que no participa de la apuesta, para la resolución de ésta. En el tercer caso la confianza recae en el ente regulado y en las instituciones encargadas de aplicar la ley, que poco podrán hacer en caso de que el ente regulado haya gastado o perdido el bien.

Usualmente cuando hablamos de dinero imaginamos un billete o una moneda. Sin embargo, cuando decimos dinero digital es más complejo hacernos una imagen. Generalmente lo asociamos a pagos electrónicos, en los cuales no vemos el billete o moneda. El dinero digital

exhibe propiedades similares al físico, se diferencia en que permite transacciones instantáneas e intercambios entre distintos países sin importar fronteras.

Una criptomoneda es un tipo de moneda digital, donde se utilizan medios criptográficos para asegurar las transacciones y para controlar la creación de nuevas unidades. La idea de utilizar herramientas criptográficas en monedas digitales surge como tópico de investigación en los años 80, cuando David Chaum [3] introduce una nueva primitiva para realizar pagos imposibles de rastrear.

En el año 2012 el banco central europeo [1] define una moneda virtual como: «un tipo de moneda digital desregulada, que es emitida y usualmente controlada por sus desarrolladores, usada y aceptada entre los miembros de una comunidad virtual específica». Monedas virtuales según esta definición existen desde hace tiempo, principalmente en comunidades de juegos.

Hasta el año 2008 todas las monedas digitales conocidas, tanto en circulación como ya retiradas, compartían una cualidad fundamental con el dinero físico. Eran completamente controladas por una entidad central, tal como en el dinero físico lo hace el banco central. Durante el mes de Noviembre del 2008 Satoshi Nakamoto publica "*A peer-to-peer electronic cash system*" [4], la primera moneda digital completamente descentralizada[2]: *Bitcoin*.

Tan solo unos meses después de su publicación sería puesto a disposición de la comunidad un software implementando el protocolo propuesto. Empezaba así a circular una moneda que cambiaría radicalmente el escenario de las monedas digitales.

Chapter 2

Primero

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Definición 2.1 (ver [**KAR00**]) *Definición definitiva*

$$\frac{\mathrm{d}}{\mathrm{d}x}\int_a^x f(y)\mathrm{d}y = f(x).$$

Chapter 3

Segundo

Quisque facilisis auctor sapien. Pellentesque gravida hendrerit lectus. Mauris rutrum sodales sapien. Fusce hendrerit sem vel lorem. Integer pellentesque massa vel augue. Integer elit tortor, feugiat quis, sagittis et, ornare non, lacus. Vestibulum posuere pellentesque eros. Quisque venenatis ipsum dictum nulla. Aliquam quis quam non metus eleifend interdum. Nam eget sapien ac mauris malesuada adipiscing. Etiam eleifend neque sed quam. Nulla facilisi. Proin a ligula. Sed id dui eu nibh egestas tincidunt. Suspendisse arcu.

Maecenas dui. Aliquam volutpat auctor lorem. Cras placerat est vitae lectus. Curabitur massa lectus, rutrum euismod, dignissim ut, dapibus a, odio. Ut eros erat, vulputate ut, interdum non, porta eu, erat. Cras fermentum, felis in porta congue, velit leo facilisis odio, vitae consectetuer lorem quam vitae orci. Sed ultrices, pede eu placerat auctor, ante ligula rutrum tellus, vel posuere nibh lacus nec nibh. Maecenas laoreet dolor at enim. Donec molestie dolor nec metus. Vestibulum libero. Sed quis erat. Sed tristique. Duis pede leo, fermentum quis, consectetuer eget, vulputate sit amet, erat.

Donec vitae velit. Suspendisse porta fermentum mauris. Ut vel nunc non mauris pharetra varius. Duis consequat libero quis urna. Maecenas at ante. Vivamus varius, wisi sed egestas tristique, odio wisi luctus nulla, lobortis dictum dolor ligula in lacus. Vivamus aliquam, urna sed interdum porttitor, metus orci interdum odio, sit amet euismod lectus felis et leo. Praesent ac wisi. Nam suscipit vestibulum sem. Praesent eu ipsum vitae pede cursus venenatis. Duis sed odio. Vestibulum eleifend. Nulla ut massa. Proin rutrum mattis sapien. Curabitur dictum gravida ante.

Phasellus placerat vulputate quam. Maecenas at tellus. Pellentesque neque diam, dignissim ac, venenatis vitae, consequat ut, lacus. Nam nibh. Vestibulum fringilla arcu mollis arcu. Sed et turpis. Donec sem tellus, volutpat et, varius eu, commodo sed, lectus. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Quisque enim arcu, suscipit nec, tempus at, imperdiet vel, metus. Morbi volutpat purus at erat. Donec dignissim, sem id semper tempus, nibh massa eleifend turpis, sed pellentesque wisi purus sed libero. Nullam lobortis tortor vel risus. Pellentesque consequat nulla eu tellus. Donec velit. Aliquam fermentum, wisi ac rhoncus iaculis, tellus nunc malesuada orci, quis volutpat dui magna id mi. Nunc vel ante. Duis vitae lacus. Cras nec ipsum.

Morbi nunc. Aliquam consectetuer varius nulla. Phasellus eros. Cras dapibus porttitor risus. Maecenas ultrices mi sed diam. Praesent gravida velit at elit vehicula porttitor. Phasellus nisl mi, sagittis ac, pulvinar id, gravida sit amet, erat. Vestibulum est. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Curabitur id sem elementum leo rutrum hendrerit. Ut at mi. Donec tincidunt faucibus massa. Sed turpis quam, sollicitudin a, hendrerit eget, pretium ut, nisl. Duis hendrerit ligula. Nunc pulvinar congue urna.

Nunc velit. Nullam elit sapien, eleifend eu, commodo nec, semper sit amet, elit. Nulla lectus risus, condimentum ut, laoreet eget, viverra nec, odio. Proin lobortis. Curabitur dictum arcu vel wisi. Cras id nulla venenatis tortor congue ultrices. Pellentesque eget pede. Sed eleifend sagittis elit. Nam sed tellus sit amet lectus ullamcorper tristique. Mauris enim sem, tristique eu, accumsan at, scelerisque vulputate, neque. Quisque lacus. Donec et ipsum sit amet elit nonummy aliquet. Sed viverra nisl at sem. Nam diam. Mauris ut dolor. Curabitur ornare tortor cursus velit.

Morbi tincidunt posuere arcu. Cras venenatis est vitae dolor. Vivamus scelerisque semper mi. Donec ipsum arcu, consequat scelerisque, viverra id, dictum at, metus. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut pede sem, tempus ut, porttitor bibendum, molestie eu, elit. Suspendisse potenti. Sed id lectus sit amet purus faucibus vehicula. Praesent sed sem non dui pharetra interdum. Nam viverra ultrices magna.

Aenean laoreet aliquam orci. Nunc interdum elementum urna. Quisque erat. Nullam tempor neque. Maecenas velit nibh, scelerisque a, consequat ut, viverra in, enim. Duis magna. Donec odio neque, tristique et, tincidunt eu, rhoncus ac, nunc. Mauris malesuada malesuada elit. Etiam lacus mauris, pretium vel, blandit in, ultricies id, libero. Phasellus bibendum erat ut diam. In congue imperdiet lectus.

Aenean scelerisque. Fusce pretium porttitor lorem. In hac habitasse platea dictumst. Nulla sit amet nisl at sapien egestas pretium. Nunc non tellus. Vivamus aliquet. Nam adipiscing euismod dolor. Aliquam erat volutpat. Nulla ut ipsum. Quisque tincidunt auctor augue. Nunc imperdiet ipsum eget elit. Aliquam quam leo, consectetuer non, ornare sit amet, tristique quis, felis. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Pellentesque interdum quam sit amet mi. Pellentesque mauris dui, dictum a, adipiscing ac, fermentum sit amet, lorem.

Ut quis wisi. Praesent quis massa. Vivamus egestas risus eget lacus. Nunc tincidunt, risus quis bibendum facilisis, lorem purus rutrum neque, nec porta tortor urna quis orci. Aenean aliquet, libero semper volutpat luctus, pede erat lacinia augue, quis rutrum sem ipsum sit amet pede. Vestibulum aliquet, nibh sed iaculis sagittis, odio dolor blandit augue, eget mollis urna tellus id tellus. Aenean aliquet aliquam nunc. Nulla ultricies justo eget orci. Phasellus tristique fermentum leo. Sed massa metus, sagittis ut, semper ut, pharetra vel, erat. Aliquam quam turpis, egestas vel, elementum in, egestas sit amet, lorem. Duis convallis, wisi sit amet mollis molestie, libero mauris porta dui, vitae aliquam arcu turpis ac sem. Aliquam aliquet dapibus metus.

Vivamus commodo eros eleifend dui. Vestibulum in leo eu erat tristique mattis. Cras at elit. Cras pellentesque. Nullam id lacus sit amet libero aliquet hendrerit. Proin placerat, mi non elementum laoreet, eros elit tincidunt magna, a rhoncus sem arcu id odio. Nulla

eget leo a leo egestas facilisis. Curabitur quis velit. Phasellus aliquam, tortor nec ornare rhoncus, purus urna posuere velit, et commodo risus tellus quis tellus. Vivamus leo turpis, tempus sit amet, tristique vitae, laoreet quis, odio. Proin scelerisque bibendum ipsum. Etiam nisl. Praesent vel dolor. Pellentesque vel magna. Curabitur urna. Vivamus congue urna in velit. Etiam ullamcorper elementum dui. Praesent non urna. Sed placerat quam non mi. Pellentesque diam magna, ultricies eget, ultrices placerat, adipiscing rutrum, sem.

Conclusión

Mauris ac ipsum. Duis ultrices erat ac felis. Donec dignissim luctus orci. Fusce pede odio, feugiat sit amet, aliquam eu, viverra eleifend, ipsum. Fusce arcu massa, posuere id, nonummy eu, pulvinar ut, wisi. Sed dui. Vestibulum nunc nisl, rutrum quis, pharetra eget, congue sed, dui. Donec justo neque, euismod eget, nonummy adipiscing, iaculis eu, leo. Duis lectus. Morbi pellentesque nonummy dui.

Aenean sem dolor, fermentum nec, gravida hendrerit, mattis eget, felis. Nullam non diam vitae mi lacinia consectetuer. Fusce non massa eget quam luctus posuere. Aenean vulputate velit. Quisque et dolor. Donec ipsum tortor, rutrum quis, mollis eu, mollis a, pede. Donec nulla. Duis molestie. Duis lobortis commodo purus. Pellentesque vel quam. Ut congue congue risus. Sed ligula. Aenean dictum pede vitae felis. Donec sit amet nibh. Maecenas eu orci. Quisque gravida quam sed massa.

Nunc euismod, mauris luctus adipiscing pellentesque, augue ligula pellentesque lectus, vitae posuere purus velit a pede. Phasellus leo mi, egestas imperdiet, blandit non, sollicitudin pharetra, enim. Nullam faucibus tellus non enim. Sed egestas nunc eu eros. Nunc euismod venenatis urna. Phasellus ullamcorper. Vivamus varius est ac lorem. In id pede eleifend nibh consectetuer faucibus. Phasellus accumsan euismod elit. Etiam vitae elit. Integer imperdiet nibh. Morbi imperdiet orci euismod mi.

Figure 3.1: Logo de la Facultad

Donec tincidunt tempor metus. Aenean egestas cursus nulla. Fusce ac metus at enim viverra lacinia. Vestibulum in magna non eros varius suscipit. Nullam cursus nibh. Mauris neque. In nunc quam, convallis vitae, posuere in, consequat sed, wisi. Phasellus bibendum consectetuer massa. Curabitur quis urna. Pellentesque a justo.

In sit amet dui eget lacus rutrum accumsan. Phasellus ac metus sed massa varius auctor. Curabitur velit elit, pellentesque eget, molestie nec, congue at, pede. Maecenas quis tellus non lorem vulputate ornare. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Etiam magna arcu, vulputate egestas, aliquet ut, facilisis ut, nisl.

Donec vulputate wisi ac dolor. Aliquam feugiat nibh id tellus. Morbi eget massa sit amet purus accumsan dictum. Aenean a lorem. Fusce semper porta sapien.

Campo 1	Campo 2
Valor 1	Valor2

Table 3.1: Tabla 1

Curabitur sit amet libero eget enim eleifend lacinia. Vivamus sagittis volutpat dui. Suspendisse potenti. Morbi a nibh eu augue fermentum posuere. Curabitur elit augue, porta quis, congue aliquam, rutrum non, massa. Integer mattis mollis ipsum. Sed tellus enim, mattis id, feugiat sed, eleifend in, elit. Phasellus non purus sed elit viverra rhoncus. Vestibulum id tellus vel sem imperdiet congue. Aenean in arcu. Nullam urna justo, imperdiet eget, volutpat vitae, semper eu, quam. Sed turpis dui, porttitor ut, egestas ac, condimentum non, wisi. Fusce iaculis turpis eget dui. Quisque pulvinar est pellentesque leo. Ut nulla elit, mattis vel, scelerisque vel, blandit ut, justo. Nulla feugiat risus in erat.

Bibliography

[1] Europen Central Bank. Virtual Currency Schemes. 2012. URL: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (visited on 01/03/2017).

[2] Jerry Brito and Andrea Castillo. *Bitcoin: A primer for policymakers*. Mercatus Center at George Mason University, 2013.

[3] David Chaum. Blind signatures for untraceable payments. In *Advances in cryptology*, pages 199–203. Springer, 1983.

[4] Satoshi Nakamoto. Bitcoin: a peer-to-peer electronic cash system, 2008.