ABC - Anti-Bureaucracy Coin

Plataforma digital para Autenticidade descentralizada de identidades, assinaturas e documentos, utilizando protocolos blockchain

Edilson Osorio Junior, Miriam Tomie Oshiro, Helena Suarez Margarido

OriginalMy.com

Julho, 2017

Draft v1.4

	Business Overview	Dietpaper	Whitepaper
EN	business_overview[EN].pdf	abc_dietpaper[en].pdf	abc_whitepaper[EN].pdf
PT-BR	business_overview[PT-BR].pdf	abc_dietpaper[PT-BR].pdf	abc_whitepaper[PT-BR].pdf
CN	business_overview[CN].pdf		abc_whitepaper[CN].pdf

1. Resumo

Desde 2015 temos desenvolvido uma plataforma na qual disponibilizamos novas aplicações em blockchain com foco em gerar registros e provas fortes de autenticidade, de maneira descentralizada.

Tendo sido a 1a *regtech* que utiliza blockchain para casos no mundo real, nossas aplicações, que já se encontram disponíveis aos usuários brasileiros, promovem além do aumento exponencial de eficiência, a redução de custos (e.g., desmaterialização de papel, transporte e reconhecimento de autenticidade de modo manual em instituições tradicionais) e tornam obsoletos quaisquer órgãos centralizados responsáveis pelo registro e pela certificação de autenticidade de determinado conteúdo.

O Brasil está na 140ª posição[1] no índice de Liberdade Econômica, sendo internacionalmente reconhecido pela grande burocracia que atrapalha de maneira significativa o desenvolvimento de negócios no país. A burocracia formal é um negócio lucrativo em todos os países de Civil Law, o que inclui a América Latina e boa parte da Europa. Todavia, a centralização de informações é um problema mundial e viabiliza assimetrias de informação que, no limite, tornam pessoas e organizações suscetíveis a fraudes.

A chave para melhorar a redução dessas assimetrias é a autenticidade descentralizada, que pode ser alcançada por meio de redes descentralizadas que utilizem blockchains públicos a fim de oferecer com total transparência, acesso e confiança.

Neste documento nós apresentaremos:
- As aplicações ativas, em funcionamento e suas especificações
- A nova plataforma
- Token ABC - Anti-Bureaucracy Coin

2. Índice

3. Glossário

Para fins do presente, foram adotadas algumas definições de modo que palavras e/ou termos iniciados em letra maiúscula, incluindo variações em função de concordância nominal, terão os significado a seguir dispostos.

- Assinatura Digital: método criptográfico para validar documentos digitais ou informações, que prova de maneira cabal que a informação da qual foi originada, não sofreu qualquer tipo de alteração.

- Assinatura Eletrônica: utilização de qualquer mecanismo eletrônico para assinatura, não necessariamente criptográfico. Funciona como indício de prova, não tendo valor legal por si só, sendo o equivalente a uma assinatura em meio físico.

- Autenticidade: traduz a absoluta legitimidade, veracidade e/ou originalidade de algo. É a certeza de que determinada Informação provém da fonte indicada e que é íntegra, i.e. não foi alvo de modificações.

- Blockchain ID: método de registro e gestão de identidade em blockchains públicos descentralizados criado pela OriginalMy que permite a verificação de usuários sem a guarda de documentos ou informações privadas e/ou confidenciais.

- Civil Law: também conhecido como Code Law, é o Sistema Legal mais disseminado no mundo. Baseia-se no direito romano e é sistematizado por meio da codificação do direito. Nesses sistemas, a principal fonte do direito é a lei escrita (positiva).

- Common Law: Sistema Legal de origem anglo-saxã, no qual a principal fonte do direito nos usos e costumes, bem como precedentes já julgados pelo Poder Judiciário (Case Law).

- CPF: Cadastro de Pessoas Físicas emitido pela Receita Federal do Brasil. Trata-se do número de contribuinte de um indivíduo que seja residente fiscal no Brasil.

- Fé Pública: presunção legal (*juris tantum*) de Autenticidade dada a documentos e certidões emitidos por pessoas delegadas pelo Poder Público.

- GED: Gestão Eletrônica de Documentos. É uma tecnologia que provê um meio de facilmente gerar, controlar, armazenar, compartilhar e recuperar informações existentes em documento.

- Informação: conteúdo que possa ser armazenado e/ou transferido, de qualquer tipo, que tenha importância para uma pessoa e/ou organização.

- KYC: abreviação de *know your customer*, consiste no processo de identificação e verificação de identidades de clientes. São processos obrigatórios para participantes de mercados regulados, em especial os financeiros e de mercado de capitais, e têm

por finalidade coibir a prática de atos ilícitos de grande interesse público como lavagem de dinheiro, corrupção e terrorismo.

- Operação Lava Jato: conjunto de investigações, ainda em andamento, de crimes de corrupção, fraude, lavagem de dinheiro, organizações criminosas, evasão de divisas (dentre outros), conduzidas pela Polícia Federal brasileira. Até a presente data, 282 pessoas foram acusadas criminalmente e 107 foram condenadas[2], dentre elas políticos, servidores públicos e executivos da iniciativa privada. O prejuízo estimado aos cofres públicos monta em R$ 42 bilhões[3] (USD 13,42 bilhões).

- OTC OriginalMy: mercado de balcão a ser disponibilizado pela OriginalMy para compra e venda dos ABC tokens diretamente pela empresa que tomará por base valores do mercado secundário, de acordo com regras especificadas em *whitepaper*.

- Permalink: URL que aponta diretamente para uma postagem específica em website com múltiplas postagens (blog, redes sociais, etc).

- Plataforma OriginalMy: conjunto de aplicações desenvolvidas e disponibilizadas pela OriginalMy, pautadas nos conceitos de registro e Prova de Autenticidade em blockchains. Atualmente, é constituída por: (i) Blockchain ID, (ii) Prova de Autenticidade para documentos digitais, (iii) Prova de Autenticidade para conteúdo web e (iv) Assinatura Digital de documentos e contratos. Disponível em https://www.originalmy.com.

- Proof-of-Work: protocolo utilizado para prevenção de ataques cibernéticos em massa, utilizando cálculos criptográficos complexos. Nele, o usuário realiza determinada tarefa antes de realizar a ação que pretende, provando ao validador que efetuou esforço próprio para, então, ter seu acesso ou ação principal aceita.

- Prova de Autenticidade: comprovação de que determinado documento digital possui Autenticidade.

- PTAX: taxa oficial de conversão de Reais para Dólares Americanos na data-base de 04 de outubro de 2017, calculada em 3,13:1[4].

- Registro de Autenticidade: é o armazenamento da Assinatura Digital em qualquer mídia.

- Roadmap: metas de desenvolvimento da OriginalMy para as metas previstas na Fase 01 do *crowdsale*, conforme especificado.

- Segurança da Informação: diz respeito à proteção da Informação com vistas a preservar sua confidencialidade, integridade, disponibilidade, autenticidade e legalidade, como definido no conjunto de normas ISO/IEC 27000

- Sidechain: grosso modo, são blockchains que validam dados de outros blockchains sem necessidade de modificação do código original dos últimos. Podem auxiliar em questões de escalabilidade, eficiência e custos de protocolos nativos.

- Sistemas Legais: modelos jurídicos que têm por objetivo a segurança jurídica. A forma pela qual se busca esse resultado explica o funcionamento de diferentes sistemas jurídicos e dos institutos que os compõem. Atualmente, as tradições predominantes do mundo são os Sistemas de Civil Law e de Common Law.

- Web-of-Trust: sistema de reputação que utiliza criptografia com níveis e encadeamento de recomendações para reforçar a confiança em agentes diversos.

4. Conceito

4.1 Segurança da Informação e tecnologias baseadas em blockchain

As boas práticas de Segurança da Informação regem sobre a proteção, o uso e o acesso à informação, bem como sua disponibilidade aos usuários, enquanto sua integridade e autenticidade permanecem preservadas, com exposição do conteúdo de acordo com o controle de acesso adequado.

Os principais atributos da Segurança da Informação[5], determinados na antiga ISO/IEC 17799 (inspirada na norma BS 7799), que posteriormente veio a ser revisada em uma série de normas da família 27000, são:

- **Confidencialidade:** garantir que o acesso à informação seja feito somente por pessoas autorizadas;
- **Integridade:** salvaguardar a exatidão e completeza da informação e dos métodos de processamento;
- **Disponibilidade:** garantir que os usuários autorizados tenham acesso à informação e aos ativos correspondentes sempre que necessário;
- **Autenticidade:** garantia de que a informação e/ou os usuários em um processo de comunicação, são quem dizem ser; e
- **Legalidade (ou conformidade):** é o valor legal para as informações dentro de um processo de comunicação.

Ainda, segundo alguns autores, a Segurança da Informação trata também do *não-repúdio ou irretratabilidade*, que é o atributo que garante a **impossibilidade de se negar a autoria** em um processo de comunicação.

As tecnologias baseadas em blockchain normalmente são aderentes aos atributos da Segurança da Informação, como exemplificado a seguir:

1. A **tríade superior dos atributos da segurança da informação** é nativa nos protocolos dos blockchains públicos, sendo a confidencialidade garantida através da exposição apenas dos dados necessários para a identificação da transação, havendo

ainda alguns protocolos blockchain que garantem o anonimato em relação às transações. A integridade dos dados é garantida através de consenso, principalmente através da prova de trabalho (*Proof-of-Work)*. E a disponibilidade é feita através da descentralização e distribuição da rede, promovendo a possibilidade de um plano de continuidade dos negócios adequado;

2. A **autenticidade das informações** é garantida através do uso de assinaturas digitais e da autorização através de chaves privadas que ficam em posse exclusiva do autor, através de técnicas de criptografia assimétrica;

3. A **legalidade** se dá a partir do momento em que a previsão dos itens acima estão em conformidade com marcos regulatórios e leis que prevêem o tratamento adequado às informações e documentos digitais.

Tais tecnologias são, ainda, invioláveis e seus mecanismos de validação são utilizados a todo momento, sendo verificáveis de maneira simples e que garantem a integridade da informação[6].

4.2 A burocracia disfuncional

Em sentido amplo, a burocracia pode ser definida como uma organização que funciona de acordo com regras estritas pré-estabelecidas, de forma a garantir um ponto ótimo de "*precisão, velocidade, certeza, conhecimento dos arquivos, continuidade, subordinação estrita, redução de desacordos e de custos materiais e pessoas*"[7]. Esse conceito é fundamental para entender a forma de constituição de organizações complexas como sociedades, estados nacionais e empresas modernas capitalistas, pois através de regras rígidas estabelece-se a ordem, o controle e garante-se a eficiência no desempenho das funções destas instituições.

Assim, a burocracia tem por pressuposto características que, se aplicadas às organizações complexas, resultariam em categorias funcionais: racionalidade, normatização, hierarquia, especialização e impessoalidade[8].

Ocorre que, se por um lado a burocracia pode ser decisiva para a criação de organizações complexas eficientes, por outro pode resultar em concentração de poder por essas organizações, levando a disfunções sistêmicas e, no limite, a sistemas engessados que tenham como *quasi*-finalidade a perpetuação do status quo, em detrimento do interesse público.

Exemplo disso é o Brasil, onde o abuso de regras rígidas levou a um estado símbolo de uma burocracia disfuncional, ineficiente no trato de políticas públicas e coerção de ilícitos. Tanto é que desde 2014 vem sendo conduzida investigação do maior caso de corrupção já noticiado na história[9], denominada "Operação Lava Jato", ainda sem conclusão.

Em meio a esta crise institucional brasileira, nasceu a OriginalMy, com o objetivo de eliminar a burocracia disfuncional impregnada na cultura e na sociedade, que é responsável não

apenas por permitir casos de corrupção e lavagem de dinheiro, como também é um dos principais limitadores para o avanço da sociedade e exercício da livre iniciativa.

Mas não é somente o Brasil que sofre com este problema. Em todos os países de Civil Law podemos encontrar instituições, públicas e privadas, que lucram com o oligopólio da Fé Pública, estabelecendo processos demorados e a nada intuitivos para acesso a informações e verificações de Autenticidade. Na prática, a centralização das Provas de Autenticidade é uma das principais fontes para a assimetria de informações e abre espaço não somente para ineficiências de mercado, mas também para a prática de fraudes.

Em outros países, notadamente aqueles de Common Law, a centralização das Provas de Autenticidade geralmente está pautada em uma pessoa ou organização que possui algum direito sobre a Informação, sendo eventuais falsidades e/ou inexatidões punidas exemplarmente com base em institutos como fraude e falsidade ideológica. Contudo, por também haver a centralização, a comprovação de falsidade é uma *quasi* prova diabólica que nem múltiplos *subpoena* podem resolver. Assim, da mesma forma que ocorre em países de Civil Law, as consequências pela impossibilidade de se aferir Autenticidade de Informações trazem enormes prejuízos a empresas e à sociedade.

Verifica-se, então, que a centralização das Provas de Autenticidade, seja em países positivistas ou naqueles que se valem dos usos e costumes como fonte primária do direito, é o grande pilar que suporta a burocracia disfuncional. Maior evidência disso reside no fato de que as consequências mais comuns deste processo (suborno, tráfico de influência e a fraude) são sofridas diariamente por pessoas, organizações e governos, em diversos países.

Por conta disso, o mundo entrou em um ciclo vicioso pois, se por um lado há a imposição institucional de uma burocracia formal que coíba práticas ilícitas, de outro incentiva-se a centralização de Informações verificáveis. Assim, a tríade vontade-capacidade-oportunidade, que possibilita que pessoas e organizações tenham o poder de mentir e trapacear permanece intacta, o que pode levar à conclusão de que essas novas "camadas" de burocracia imposta possuem os mesmos defeitos que os sistemas atuais de gestão de Informação e aferição de Autenticidade. Logo, é de se esperar que o resultado seja, mais uma vez, o da disfuncionalidade.

Em um espectro totalmente inverso, estão as tecnologias que se utilizam de blockchains públicos e descentralizados: neles, o incentivo para que as pessoas participem apoiando o protocolo é maior do que o incentivo para que tentem fraudá-lo[10]. Ademais, a própria descentralização torna improvável que apenas uma pessoa ou organização concentrem todas as características necessárias para fraudar determinada Informação (vontade, capacidade e oportunidade) ou para fazer uso indevido dela.

Uma forma descentralizada de registro e aferição de Autenticidade de Informações poderá resultar na distribuição da Fé Pública entre proprietários e stakeholders de determinadas Informações, possibilitando ganhos incalculáveis a empresas e à sociedade global.

4.3 Registros e Autenticidade descentralizados

Sendo a tríade superior dos atributos da Segurança da Informação garantidas pelos protocolos blockchain, os atributos de autenticidade de dados e legalidade ainda dependem de aplicações externas para estarem em conformidade com os diversos marcos regulatórios e legislações existentes, preenchendo a forma prevista para que possa, para todos os efeitos, refletir um ato jurídico perfeito.

Nesse sentido, a Plataforma OriginalMy provê Autenticidade descentralizada para documentos e informações através da utilização de diversos blockchains públicos. Isso combinado com outros protocolos abertos, ajudou a criar sofisticados meios de Prova de Autenticidade para identidades, manifestações de autonomia da vontade (como cadastros, logins de acesso e assinatura de documentos) e para documentos digitais diversos.

Na prática, é possível realizar atos, incluindo a celebração de negócios jurídicos, com todos os requisitos legais de verificação de existência, validade e eficácia, incluindo comprovação cabal de identidade e não apenas a mera posse de uma senha ou chave privada.

Uma Informação Autêntica é aquela em que seja possível comprovar ser a original e que não sofreu qualquer alteração em sua integridade. Utilizando um algoritmo complexo de criptografia sobre a Informação original, é possível encontrar uma nova Informação que a represente de maneira inequívoca. A essa nova Informação é dado o nome de *hash* criptográfico, representado por uma sequência de caracteres de tamanho definido (como este: *c66663acfe3611b9ed95c79aad41dc6fca836363618807cfd4ee7b88ef15fa34)*. Este *hash* é a Prova de Autenticidade daquela Informação.

Perceba que através do *hash* não é possível deduzir qual era a Informação que o originou, muito menos reconstitui-la. A verificação de Autenticidade somente é possível aplicando-se novamente o mesmo algoritmo criptográfico sobre a Informação original. Se Autêntica, será apresentado o mesmo *hash*. Comparando os *hashs* da Informação original com o da Informação verificada, será possível identificar se a primeira sofreu modificações, pois em caso de qualquer alteração, o *hash* resultante será diferente.

Para garantir que ninguém substitua ou faça alterações no *hash* da Informação original, o OriginalMy o registra em um ou mais blockchains públicos que, por sua vez, passa a armazená-lo. Assim que o blockchain confirma o armazenamento, ele fornece um carimbo de tempo (*timestamp*) que representa o momento em que ele passou a ter conhecimento daquele *hash*. Essa é a Prova de Autenticidade de que certa Informação existia de maneira idêntica à verificada em determinado momento. E, após essa confirmação, essa Prova de Autenticidade é automaticamente replicada para todos os nós que compõem a rede de cada um dos blockchains onde o registro fora efetuado.

Dadas as características elementares dos blockchain públicos como imutabilidade, transparência, descentralização e distribuição dos dados, o OriginalMy provê a Autenticidade

descentralizada para documentos digitais, sem registrar ou tornar público o conteúdo das Informações dos usuários, mantendo, assim, sua privacidade e confidencialidade.

Modelos de padrões e protocolos abertos tendem a ser mais efetivos do que padrões fechados, por serem auditáveis e terem comunidades dedicadas ao seu desenvolvimento.

Por este motivo, o OriginalMy utiliza diversos dApps[11] (decentralized applications) que podem ser acessados publicamente por outros sistemas de smart-contracts, compartilhando a infraestrutura para melhorar a eficiência de processos e controles.

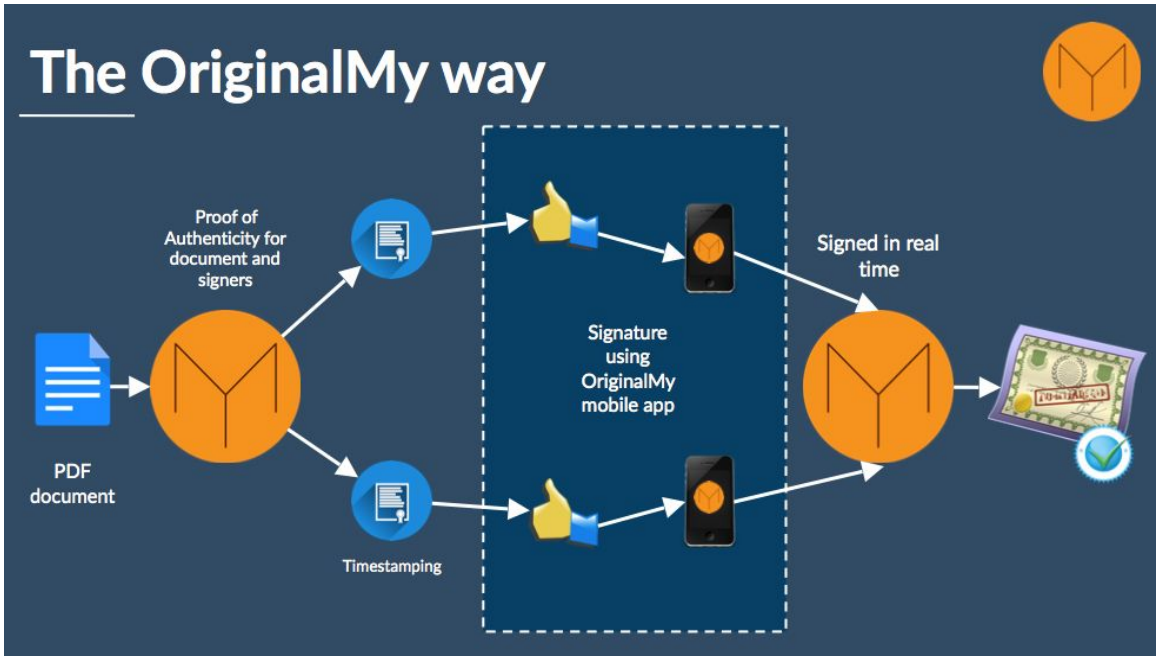


Fig.1: Exemplo de uso da plataforma OriginalMy: Assinatura de documentos e contratos com validação de identidade

5. Plataforma atual: Aplicações e histórico

5.1 Prova de Autenticidade

A plataforma OriginalMy foi lançada em 18 de Julho de 2015 durante a III Bitconf, evento que aconteceu em Florianópolis, Brasil. Naquele momento a plataforma fazia o registro em blockchain de Prova de Autenticidade de documentos digitais, utilizando assinatura digital do documento e *timestamp* provido pelo blockchain da rede Bitcoin.

5.2 Assinatura de contratos - 1ª versão (descontinuada)

Logo após o lançamento, verificamos demanda para soluções de assinatura dos documentos registrados em blockchain (i.e., prover seu consentimento ou concordância em relação ao conteúdo). Ao analisar quais eram os principais desafios legais em relação aos meios de

Assinatura Digital e/ou Eletrônica existentes, chegamos à conclusão de que o grande problema em ambientes digitais é a comprovação de que aquele que expressou sua vontade era de fato a pessoa que deveria tê-lo feito.

Sobre esse tópico especificamente, vale citar que tanto soluções tecnológicas tradicionais quanto aquelas desenvolvidas com uso de blockchains partem do pressuposto de que a posse de uma senha ou chave privada é suficiente para comprovação de identidade. Contudo, tal presunção tem se provado ineficaz para garantir Autenticidade, haja vista quantidade crescente de fraudes em meio digital (por meio de *hacks*, *malwares* ou simples "fraudes brancas[12]") e a relutância de indústrias reguladas em migrar cadastros e verificações para ambiente totalmente digital.

Nosso primeiro *approach* para solução desse problema ocorreu também em 2015, quando desenvolvemos a primeira versão do sistema de assinatura de documentos e contratos por meio de vídeo-depoimento. Sobre ele poderia ser aplicada verificação biométrica para detectar e avaliar diversos pontos de controle como nível de stress da fala, micro-expressões da face, dentre outros.

Contudo, apesar de validado do ponto de vista legal, o modelo não obteve a aderência esperada pois trazia um custo de transição importante: as pessoas estão acostumadas a assinar um documento, não a declarar por meio de vídeo que estão de acordo com seu conteúdo.

Assim, passamos a estudar e desenvolver um novo modelo de assinatura eletrônica que tivesse a mesma consequência jurídica, porém com uma usabilidade mais amigável. Entendemos que para que uma Assinatura Eletrônica não seja questionada em relação à autoria, seria necessário uma camada de identificação do usuário resistente à fraude.

No início de 2016 começamos a desenvolver um novo modelo que pudesse, ao mesmo tempo, provar a Autenticidade de atos juridicamente perfeitos através da identificação inequívoca de usuários, ser utilizado na assinatura de documentos e contratos e reduzir a fricção verificada no modelo anterior de vídeo-depoimento.

Este modelo de assinatura foi atualizada para um novo, com melhor usabilidade, ficando disponível apenas para consulta em modo legado.

5.3 Projeto Mudamos+

Assim que o protocolo foi redesenhado, o ITS-Rio (Instituto de Tecnologia e Sociedade do Rio de Janeiro) nos convidou para prototipar soluções que pudessem viabilizar a assinatura de Projetos de Lei de Iniciativa Popular[13].

Utilizando o novo modelo de identificação de usuários e assinaturas desenvolvido pela OriginalMy, o ITS-Rio ganhou o prêmio Desafio de Impacto Social do Google.org em 2016[14]. Assim, desenvolvemos toda a camada de identidade e assinaturas, utilizando blockchain, baseado em uma versão customizada do protocolo que havíamos desenhado.

Especificamente para o Mudamos+[15], desenvolvemos uma Sidechain dedicada a registrar as assinaturas dos cidadãos e autenticá-las em blockchains públicos. Essas assinaturas são provenientes do aplicativo mobile Mudamos, que faz o KYC do usuário e emite uma identidade blockchain que fica armazenada no aparelho móvel.

Ainda, para aumentar a segurança e mitigar o risco de fraude, o app faz *Proof-of-Work* de cada assinatura efetuada (gerando um bloco com uma única transação), no próprio aparelho celular do usuário. Esse proof-of-work é baseado no algoritmo *hashcash*[16], o mesmo utilizado pelo Bitcoin para validar as transações e evitar a fraude.

Até a presente data, o Mudamos+ já possui mais de 270 mil usuários únicos registrados, 500 mil downloads e 240 mil assinaturas realizadas utilizando a engine customizada desenvolvida pelo OriginalMy, havendo diversos entes federativos no Brasil sinalizado a aceitabilidade de projetos de lei assinados por meio do aplicativo.

5.4 Prova de Autenticidade para Conteúdo Web

Após algumas demonstrações das primeiras aplicações, nos foi apresentada a necessidade de uma coleta de provas de conteúdo web autenticada em blockchain, com *timestamp*, de maneira automatizada. O conteúdo coletado poderia ser proveniente de atos caluniosos em redes sociais, por exemplo, e a prova seria utilizada em processo judicial para comprovar que determinado conteúdo estava disponível na Internet no momento especificado.

Para tanto, desenvolvemos um plugin para o browser Chrome que coleta o conteúdo visualizado no momento (de preferência através de um *Permalink*), gera um laudo com a fundamentação jurídica necessária para utilização como prova documental e registra automaticamente a Autenticidade deste laudo contendo o conteúdo coletado, em blockchain.

5.5 Blockchain ID: registro e gestão de identidade

Método do qual derivou uma versão customizada para o projeto Mudamos+, nosso método de registro e gestão de identidade (“Blockchain ID”) comprova que determinado usuário é quem alega, bem como todos os atos por ele praticados (autenticidade da autoria) através da nossa plataforma.

Iniciamos o desenvolvimento deste protocolo[17] em abril de 2016, utilizando como premissas a falta de confiabilidade dos modelos atuais de Assinatura Eletrônica e os requisitos para aferição de Autenticidade de identidades de acordo com o framework regulatório de vários países, bem como referência diversos protocolos existentes, dentre eles o BitID[18].

O Blockchain ID foi criado inicialmente para que a assinatura de contratos e documentos pudesse formalizar negócios jurídicos revestidos de existência, validade e eficácia, inclusive no tocante à forma, sem as fragilidades dos sistemas de Assinatura Eletrônica atuais, que não conseguem garantir e comprovar a autoria.

O método de registro e gestão de identidade desenvolvido e disponibilizado por meio do Blockchain ID se revelou incrivelmente efetivo, e ainda que existam melhorias incrementais importantes a serem desenvolvidas e implementadas (explicado adiante), passamos a utilizá-lo também como forma de KYC digital, possibilitando que usuários não precisem utilizar senhas para acessar sites ou preencher cadastros.

Dentre os principais diferenciais em relação às propostas de sistemas de identidade e KYC, que utilizam blockchain, existentes até o momento no mercado, podemos elencar:

1) Espera-se que não haja custo para o registro de identidade. Assim, a entrada na rede será gratuita e livre a todos os usuários que desejem obter seu Blockchain ID;

2) A recuperação do Blockchain ID não dependerá da anuência de terceiros, pois entendemos que a identidade é um direito humano e como tal não deve estar sujeito a poder ou ingerência de qualquer terceiro para sua outorga ou recuperação;

3) A utilização de biometria para acessar ou efetuar ações sensíveis garante que somente o dono do dispositivo possa fazer uso da identidade armazenada nele;

4) Em nenhum momento as informações do usuário são expostas publicamente;

5) A solução apresentada pelo OriginalMy é a única que apresenta validação imediata (complexa e automatizada) sobre os dados fornecidos pelo usuário no momento do cadastro.

6) Além disso, também é a solução mais completa existente no mercado pois possui os seguintes controles de segurança, em constante aprimoramento:

    a) Biometria;
    b) Usuário e senha;
    c) Cadastro completo de atributos;
    d) Validação dos dados de cadastro automatizado, com busca de informações em redes públicas, OCR e leitura de imagem;
    e) Blockchain ID armazenada somente no dispositivo;
    f) E, em caso de assinatura de contratos, faz prova de posse do documento.

5.6 Assinatura de Contratos - 2ª versão (atual)

Após concluída a camada de gestão de identidade, desenvolvemos a 2ª versão da plataforma de assinatura de contratos. Primeiramente, foi utilizada a rede Bitcoin e, após o aumento expressivo do valor de *fee* da transação em Maio de 2017, migrou-se para a plataforma Ethereum e, na sequência, para o Ethereum Classic.

A plataforma de assinatura de contratos foi lançada oficialmente em maio de 2017 durante a Conferência Consensus, em Nova Iorque. Disponível na Apple Store e Google Play, o aplicativo permite aos usuários brasileiros que se cadastrem (i.e., obtenham seu Blockchain

ID) e assinem documentos dos quais sejam signatários de maneira intuitiva e com redução substancial da fricção verificada no modelo inicial (vídeo-depoimento).

Ademais, o documento digital assinado é também registrado, sendo possível às partes verificar sua Autenticidade por meio da Plataforma OriginalMy.

5.7 Sidechain

Os blockchains atuais possuem desafios em relação à escala, tanto no que tange as taxas de processamento de registros por segundo (tx/s) que eles comportam quanto o custo da transação (*fee*).

O blockchain da rede Bitcoin foi desenhado para comportar 7 tx/s, mas na prática efetua apenas 3 tx/s, enquanto o Ethereum, em tese desenhado para efetuar dezenas de milhares de transações por segundo[19], chegou ao seu limite com 15 tx/s.

Além disso, os blockchains de maior entropia possuem um custo muito alto para registro de Informações, o que limita ganhos de escala tanto pela vazão de transações quanto pelo seu custo.

Por estes motivos, passamos a utilizar uma versão customizada do projeto DCRTime da Decred[20] para o registro de Autenticidade de documentos, o qual é baseado no padrão opentimestamps[21] para fornecer escala no processo de *timestamping* de documentos digitais.

Com a implementação desta funcionalidade foi obtida expressiva melhoria no processamento de transações, abrindo a possibilidade de administrar milhões de transações por segundo sem perda de performance ou aumento expressivo de custo.

Pretendemos estudar a evolução desse formato também para a assinatura de contratos documentos, possibilitando ganhos ainda maiores de escala, tanto em volume de processamento como em redução de preços.

Futuramente, assim que concluída a implementação prevista para assinatura de contratos, a sidechain será disponibilizada como código aberto (*open-source*).

5.8 Blockchains múltiplos

No seu lançamento em 2015, o OriginalMy registrava a Autenticidade de documentos somente no blockchain da rede Bitcoin.

Com a evolução dos protocolos que utilizam blockchains, e dado sermos agnósticos em relação ao blockchain utilizado, hoje a Plataforma OriginalMy efetua os registros em 4 blockchains públicos além de outros privados, sendo os mais relevantes:

- Bitcoin: www.bitcoin.org

- Ethereum: www.ethereum.org
- Ethereum Classic: www.ethereumclassic.org
- Decred: www.decred.org

Desta maneira, a Plataforma foi arquitetada para ser bastante flexível, efetuando os registros de acordo com a necessidade dos clientes que fazem integração com nosso ambiente de APIs.

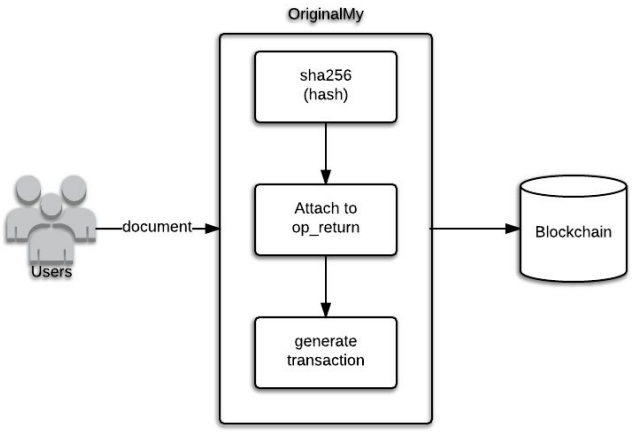
Ressalta-se, ainda, que a forma como a Plataforma OriginalMy foi arquitetada e desenvolvida permite aos integradores desenvolver seus produtos ou integrações sem necessidade de conhecer detalhes sobre blockchains existentes. A complexidade para lidar com a camada em blockchain dessas utilizações é de inteira responsabilidade da OriginalMy, o que permite escalabilidade na utilização das aplicações disponíveis por não serem necessários desenvolvedores com conhecimentos específicos de criptoprotocolos.

6. Especificações das Aplicações

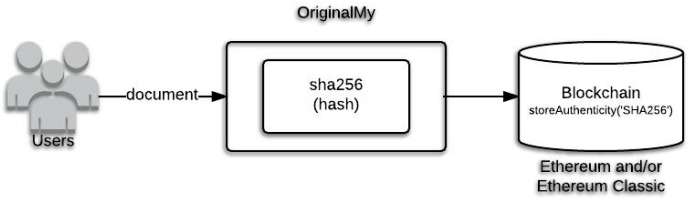
6.1 Prova de Autenticidade para documentos digitais

Inicialmente, o registro de Autenticidade era feito somente com o registro da Assinatura Digital do documento (SHA256[22]) e armazenado no campo op_return[23] de uma transação para aquela rede. Após a inclusão dos outros blockchains, o formato foi diversificado de acordo com o protocolo utilizado.

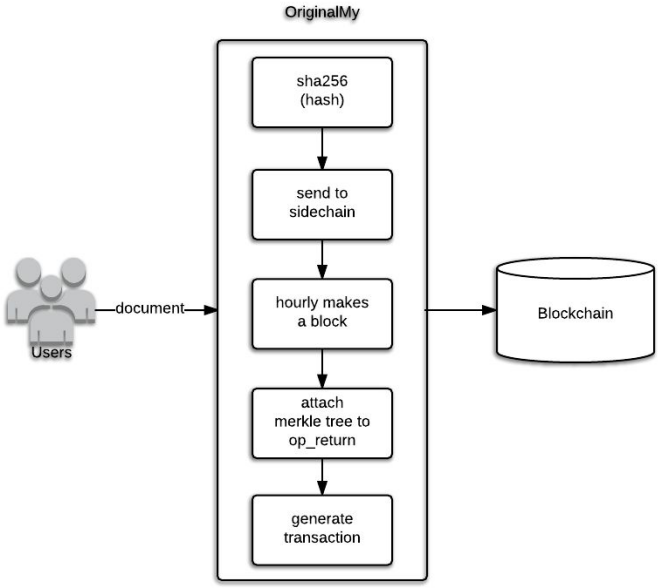
- Bitcoin: (sha256 + hora legal brasileira + marcador OM) no campo op_return



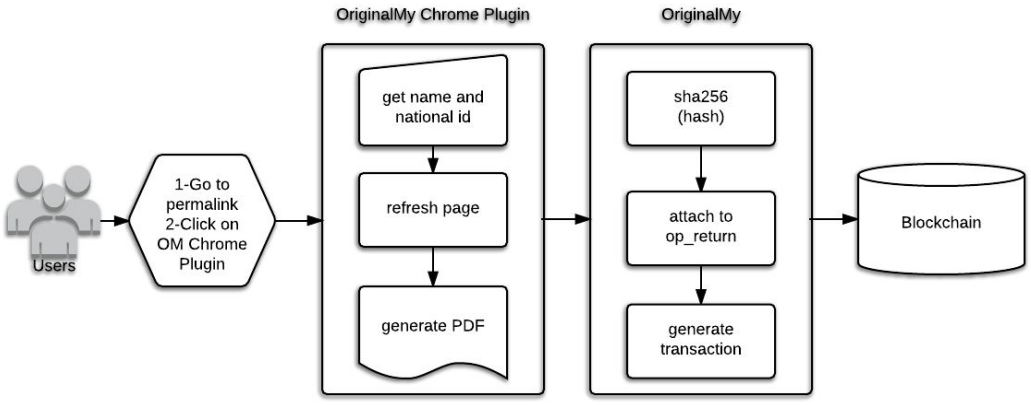
- Ethereum: https://github.com/OriginalMy/originalmy-dapp-addresses
    - Mainnet Ethereum >> Document Authenticity
- Ethereum Classic: https://github.com/OriginalMy/originalmy-dapp-addresses
    - Mainnet Ethereum Classic >> Document Authenticity



- Decred: (merkle tree + marcador OM) no campo op_return



6.2 Prova de Autenticidade para conteúdo Web



O processo de registro é o mesmo para a Prova de Autenticidade de documentos digitais, em cada um dos blockchains.

6.3 Blockchain ID

No momento em que o usuário faz seu cadastro através do app, ele passa por diversas validações automáticas ou em processo de automatização. Isso acontece em três etapas:

6.3.1 Cadastro pelo app e validações preliminares

1. Criação de usuário e senha;
2. Validação do e-mail;
3. Validação do número de telefone e do aparelho celular;
4. Validação do CPF em bases públicas;
5. Foto *selfie* do rosto do usuário, feito diretamente com o app;
6. Foto do documento, de maneira que seja possível identificar tanto o usuário como o número do documento de identificação; e
7. Criação de um Blockchain ID, cuja parte privada fica armazenada apenas no celular do usuário, sem contato com nossos sistemas ou outras pessoas. A informação pública é enviada para os nossos servidores para validação.

Os nossos sistemas, funcionários e colaboradores não têm (nem nunca terão) contato com as palavras utilizadas para gerar o Blockchain ID, sendo tal informação de conhecimento exclusivo do usuário que a criou.

O Blockchain ID fica associada ao número de CPF do usuário publicamente em um blockchain, permitindo a verificação 24 horas por dia, 7 dias por semana, sendo possível a criação de apenas 01 por usuário único.

6.3.2 Pesquisa automática em redes públicas

Após a criação da conta e do Blockchain ID, o sistema faz uma busca em bases públicas governamentais para efetuar a validação do CPF, confrontando os dados fornecidos com aqueles publicamente verificáveis.

6.3.3 Validação automática dos documentos

Após a validação do CPF, outros dados e Informações em redes públicas, o sistema envia automaticamente as Informações que necessitem de validação manual para a equipe de validação OriginalMy. Caso seja detectado algum tipo de inconsistência, o cadastro é bloqueado. O usuário só poderá utilizar seu Blockchain ID após fornecer informações válidas.

6.3.4 Outorga do Blockchain ID

O Blockchain ID é criado utilizando criptografia de chaves assimétricas baseada em tecnologias que utilizam blockchains.

As identidades blockchain são armazenadas publicamente em blockchain:

- Ethereum Classic: https://github.com/OriginalMy/originalmy-dapp-addresses

- Mainnet Ethereum Classic >> CPF IDs and wallets repository

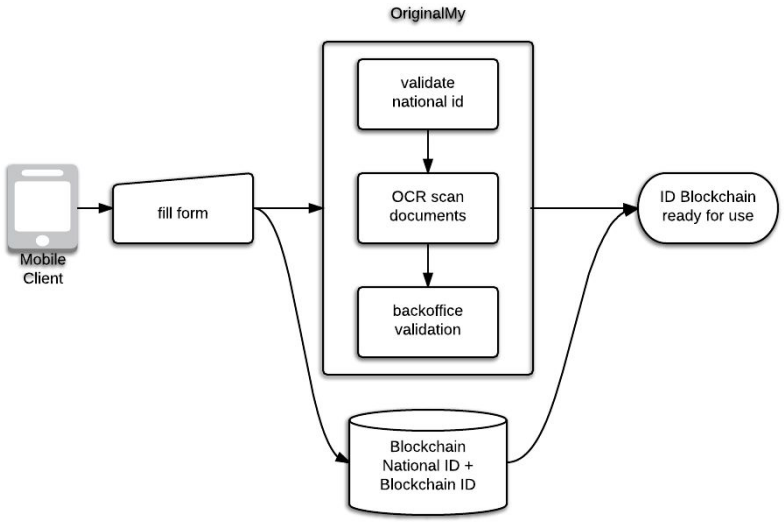
6.3.5 Recuperação do Blockchain ID

Em caso de troca de celular, reinstalação do app ou login em um novo aparelho, o sistema solicitará novamente a validação dos dados. Contudo, antes que o faça, fornecerá uma oportunidade para recuperar o Blockchain ID fornecido anteriormente.

Para tanto, será solicitado o conjunto de 12 palavras que uma vez fornecido corretamente fará com que, o sistema restaure o Blockchain ID.

Todavia, caso o usuário não tenha as palavras ou erre o preenchimento por muitas vezes, então o sistema efetuará automaticamente o processo de criação de um novo Blockchain ID, como efetuado no processo de cadastro inicial.

O novo Blockchain ID sucederá o antigo e ficará vinculado ao usuário tanto em seu novo dispositivo, como publicamente, registrado em blockchain Assim, todo histórico de contratos assinados e documentos registrados restará intacto.



6.4 Assinatura de documentos e contratos

Conforme disposto, inicialmente os contratos eram assinados no blockchain da rede Bitcoin, tendo o protocolo sido posteriormente migrado para Ethereum Classic por motivos de custo e performance.

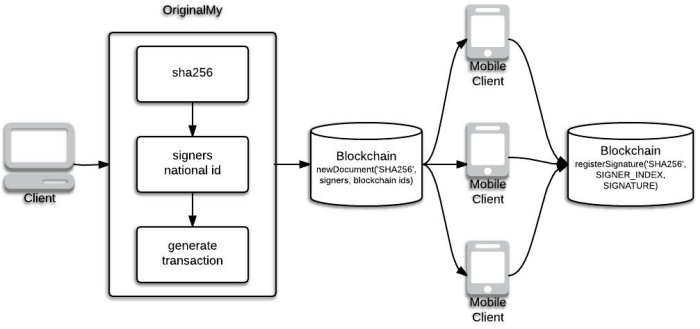
Nesse sentido, a rede Ethereum Classic, além de mais barata, é mais rápida para o registro de transações: enquanto na rede Bitcoin o tempo é de aproximadamente 10 minutos para que o registro de um documento apareça no aplicativo dos usuários para assinatura, o mesmo foi reduzido para 15 segundos por meio de utilização do Ethereum Classic.

6.4.1 Utilização do blockchain do Ethereum Classic

Atualmente documentos e contratos são assinados utilizando a Ethereum Classic como infraestrutura.

Após ter a sua identidade validada no nosso sistema, o usuário poderá utilizá-la para efetuar ações em ambiente digital, que vão desde o simples registro sem a necessidade de preencher formulários de cadastro (*sign up*) e logins em websites (*sign in*) até a celebração de negócios jurídicos complexos legalmente aceitos, vinculantes e executáveis.

A assinatura de documentos é feita através do aplicativo mobile OriginalMy (Android e iOS), comprovando a autoria e fazendo a prova de posse do documento no momento da assinatura



Após todos os signatários assinarem o documento, o smart-contract altera a flag *checkCompleted* para *True*. Quaisquer outros smart-contracts terceiros que estejam monitorando o processo de assinatura podem dar continuidade aos processos automaticamente.

6.4.2 Utilização do blockchain do Bitcoin

Apesar de não ser utilizado atualmente por questões de custo, este protocolo foi desenvolvido anteriormente à migração para outros blockchains e poderá eventualmente ser retomado.

Sendo o caso, consistirá no seguinte fluxo:

Registro:

1. No site OriginalMy é fornecido o documento original do contrato e listados os CPF's dos signatários
2. Criando 1 transação com as informações:
    a. Sistema gera um endereço de wallet para identificar o contrato (endereço do contrato)
    b. Registro no op_return: [sha256 + wallet do contrato + marcador OM]
    c. Busca no smart-contract de IDs (IdRepo) pela Identidade Blockchain dos CPFs listados
    d. Gerados endereços de wallet com CPF no hash160: [sig;CPF]Gerado endereço de wallet com hora legal brasileira no hash160: [t;timestamp]

e. Enviado dust para registrar CPFs e hora legal

Validação:
Verificar o endereço do contrato e encontrar as interações com o Blockchain ID do usuário.

Esta interação só ocorrerá caso o usuário faça a Assinatura do documento utilizando o aplicativo mobile, comprovando a autoria e fazendo a prova de posse do documento no momento da assinatura.
Exemplo de transação de registro de contrato:
https://blockchain.info/pt/tx/523e63ad8a1cd928e7a5292f7145af3596bb11475750b466319e74d77003ef24

Explicação:
tx: 523e63ad8a1cd928e7a5292f7145af3596bb11475750b466319e74d77003ef24

- 1HyuB5rM3ZpP1cHqTCJLGs65usNkzDZiUU: blockchainID do signatário1
- 1BXEycBEfCqYgPGebhkLBwKrp4VpbiHszV: nationalID do signatário1 (hash160 hex encoded)
- 1KaRgqmRSLwYFfeyHgpQaSnLsK3bVwpUqc: blockchainID do signatário2
- 1BXEycBDsSGSGmWqgd6KrQN4Hu8RKTDCCa: nationalID do signatário2 (hash160 hex encoded)
- 1BbaJGRHWCfX18bFKqyTSHGEm8QS7MBXAx: hora legal (hash160 hex encoded)

op_return

- sha256: 971bbbc7e67522ec7df3fd523bf9d83899f376d0b3c66d5a2776420b178a84743
- wallet do contrato: 15poB7iiLShugHLFpbfX5v3Nc4TkDbGJVR
- marcador OM: ORIGMY

Exemplo de transações de assinatura para este contrato:
https://blockchain.info/address/15poB7iiLShugHLFpbfX5v3Nc4TkDbGJVR

- wallet do contrato: 15poB7iiLShugHLFpbfX5v3Nc4TkDbGJVR

Verifique que *1HyuB5rM3ZpP1cHqTCJLGs65usNkzDZiUU* e *1KaRgqmRSLwYFfeyHgpQaSnLsK3bVwpUqc* interagiram com esse contrato. Isso significa que ambos assinaram o documento.

7. Nova Plataforma

O presente *crowdsale* tem por objetivo viabilizar uma nova fase no desenvolvimento da Plataforma da OriginalMy. Essa nova plataforma trará soluções globais para registro de identidade, documentos e assinaturas em ambiente digital, além de dar início ao processo de completa descentralização do Blockchain ID.

Uma vez que a captação da Fase 01 tenha sucesso (vide item 8), será desenhado e iniciado o desenvolvimento de um novo blockchain específico para registros de Autenticidade de forma descentralizada, tendo por base formas de identificação digital, como é o caso de algumas das aplicações já desenvolvidas pela OriginalMy.

Importante frisar que o processo de descentralização de Provas de Autenticidade, além do desafio de desenvolvimento da tecnologia, envolve lidar com tradicionais instituições, públicas e privadas, que existem com o fim único de centralizar Informações. Por conta disso, optamos por um processo paulatino de criação de rede e descentralização gradual, tendo sido a oferta dos ABC tokens, da mesma maneira, sido dividido em duas etapas.

7.1 Internacionalização

A primeira meta a ser alcançada em função da oferta de tokens é o início de internacionalização da Plataforma OriginalMy. Para tanto, serão promovidas alterações substanciais que permitam o registro em Blockchain ID por usuários de outros países, de acordo com o *Roadmap* ora previsto.

7.2 Experiência do usuário

Temos consciência de que soluções em blockchain precisam resolver problemas reais sem causar fricção ou resultar em custos de transação e/ou transição significantes. Assim, uma das principais metas será prover melhorias substanciais na navegabilidade das aplicações já disponibilizadas em ambiente web e aplicativos mobile.

7.3 ABC Token

Com o sucesso do *crowdsale*, todas as funcionalidades disponibilizadas por meio da Plataforma OriginalMy passarão a ser acessíveis apenas por meio do ABC token (vide Roadmap para implantação). Nesse sentido, o ABC token dará direito à utilização de todas as aplicações disponíveis na Plataforma OriginalMy e poderá ser parte de programas específicos de fomento de rede, adquirido dos participantes do *crowdsale* (via mercado secundário) ou diretamente da OriginalMy, por meio de balcão a ser implementado (OTC OriginalMy).

7.4 OTC OriginalMy

A fim de tornar possível a utilização universal da Plataforma OriginalMy, além das políticas para fomento de rede a serem criadas, também criaremos um mercado de balcão próprio por meio do qual realizaremos a venda direta de tokens àqueles que desejem utilizar nossos serviços. O preço para utilização, que para fins de mera referência está atualmente fixado em R$ 5,20 para o varejo, poderá variar de acordo com o volume de utilização e tipo de serviço contratado, bem como em razão dos blockchains utilizados.

Uma vez que o OTC seja disponibilizado, a OriginalMy compromete-se, observando-se o *Roadmap*, a praticar o preço mínimo de venda acima do preço de mercado secundário. A princípio, estimamos que o preço do token vendido via OTC será ao menos 20% (vinte por

cento) superior ao valor médio ponderado de acordo com o volume de tokens negociado nos últimos 30 (trinta) dias em mercado secundário relevante que registre maior volume de negociações do ABC token:

$$OTC\ Sale$$

$$min.\ Price = 1,2 \times \frac{\sum_{i=1}^{n}(pi \times xi)}{\sum_{i=1}^{n} pi}$$

Onde:
p = volume negociado do ABC Token em mercado secundário de maior liquidez nos últimos 30 dias; e
x = preço de negociação do ABC Token em mercado secundário de maior liquidez nos últimos 30 dias

Ademais, de acordo com critérios de oportunidade e conveniência, a OriginalMy poderá disponibilizar programa de recompra de ABC tokens no OTC OriginalMy, que poderá ser utilizado pelo detentor dos ABC tokens a seu exclusivo critério. Sendo este o caso, a OriginalMy compromete-se a praticar o preço máximo inferior ao preço médio do mercado secundário. A princípio, estimamos que o preço do token vendido via OTC será no máximo de 80%(oitenta por cento) superior ao valor médio ponderado de acordo com o volume de tokens negociado nos últimos 30 (trinta) dias em mercado secundário relevante que registre maior volume de negociações do ABC token:

$$OTC\ Purchase$$

$$max.\ Price = 0,8 \times \frac{\sum_{i=1}^{n}(pi \times xi)}{\sum_{i=1}^{n} pi}$$

Onde:
p = volume negociado do ABC Token em mercado secundário de maior liquidez nos últimos 30 dias; e
x = preço de negociação do ABC Token em mercado secundário de maior liquidez nos últimos 30 dias

Nos reservamos ao direito de alterar as regras ora previstas oportunamente caso se verifique necessário para o bom andamento e desenvolvimento dos nossos negócios. Sendo esse o caso, buscaremos, equilibrar eventuais alterações com os interesses dos detentores de ABC token e as divulgaremos amplamente por meio dos canais oficiais de comunicação da OriginalMy.

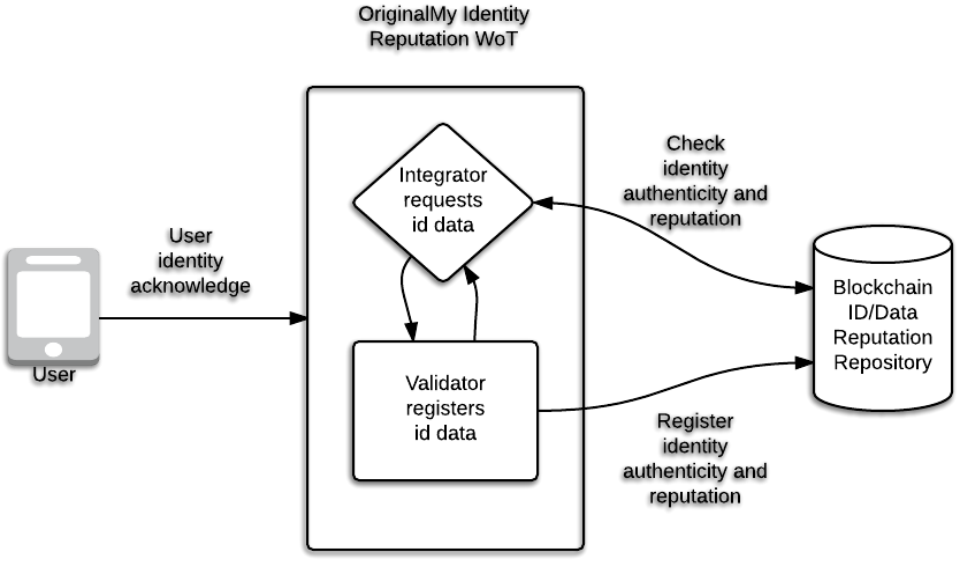
7.5 Descentralização do Blockchain ID

A solução de Blockchain ID poderá trazer benefícios incalculáveis a empresas de diversas indústrias e à sociedade por meio de aplicações, tanto desenvolvidas pela OriginalMy quanto por terceiros. Para que isso seja de fato possível, uma das principais medidas será descentralizar o processo de criação e validação das identidades e atributos em blockchain,

incentivando-se assim a criação de efeito de rede substancial e incentivos para adoção em massa dessa nova plataforma.

Utilizando recursos de *Web-of-Trust* associado à Autenticidade descentralizada promovida pelo blockchain, será possível avaliar a consistência e reputação de cada um dos atributos que compõem a identidade do usuário.

Nesse sentido, a OriginalMy será responsável por prover a arquitetura e design deste novo protocolo, contemplando o passo-a-passo para o processo de descentralização segura do Blockchain ID, de forma a criar e fomentar uma nova rede descentralizada por meio de sistema de incentivos específicos que estimulem o registro de identidades e atributos de usuários, bem como estabeleça forma de recompensa pela validação e revalidação de cada um desses dados pelos nodes (“Proof-of-Authenticity”).



8. Crowdsale: ABC Tokens

O processo de venda de tokens foi dividido em fases, haja vista tratar-se da primeira oferta de tokens utilidade no Brasil e uma das primeiras no mundo que tem por objetivo lastrear a economia inteira de uma plataforma tecnológica já desenvolvida e em produção.

Assim, tendo por princípio a cautela e o respeito àqueles que participarão deste processo, achamos por bem segregar a venda dos tokens em duas etapas distintas, tendo como objetivo o processo gradual de descentralização já descrito e a criação orgânica de uma rede descentralizada.

8.1 Fase 01

A Fase 01 da venda dos ABC tokens tem por objetivo levantar recursos para o início da internacionalização da plataforma, com pesquisa e validação de identidades em bases

públicas de alguns países, e melhorias significativas de experiência do usuário (itens 6.1 e 6.2). Para tanto, a contribuição total mínima deverá atingir o valor de USD 1.000.000,00, quantia estimada para execução dessas etapas.

Ademais, com recursos adicionais disponíveis, será possível expandir a plataforma para mais países, concluir a completa tokenização dos produtos disponíveis na OriginalMy, bem como a implementação do OTC próprio (itens 6.3 e 6.4), tornando este um dos primeiros ambientes cuja economia estará lastreada integralmente pelos tokens disponíveis no mercado. Para que isso ocorra, a contribuição total mínima deverá atingir o valor de USD 3.000.000,00.

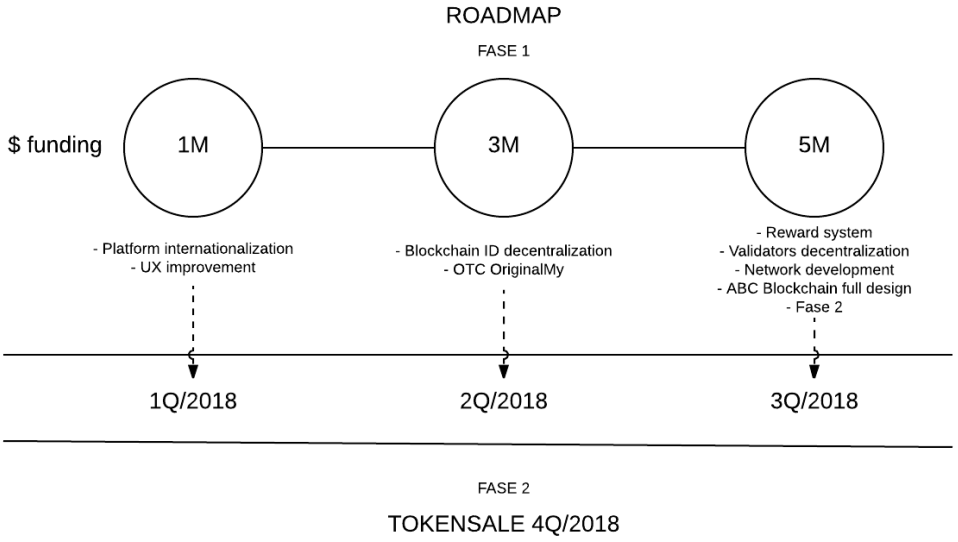
Por fim, caso a oferta atinja o valor do hard cap (USD 5.000.000,00), será possível descentralizar os validadores de dados, criar um sistema de recompensa para validadores e usuários, fomentar a rede global e, ainda, prototipar a arquitetura e design de um novo blockchain, específico para o registro de autenticidade (item 6.5), acelerando o processo de criação do novo protocolo antes do início da Fase 02, descrita adiante.

8.2 Fase 02

A Fase 02 da venda dos ABC tokens está prevista para ocorrer após a conclusão do *roadmap* previsto para a Fase 01 e terá por objetivo arrecadar recursos para o desenvolvimento completo de um novo protocolo para registro e verificação de identidade e atributos de pessoas e organizações, que contemplará novo blockchain específico e regras de mineração próprias.

Um blockchain dedicado ao registro e verificação de autenticidade de identidades, assinaturas de contratos (celebração de negócios jurídicos), documentos e transferências identificadas de ativos poderá promover escala e baixo custo de registro, itens limitantes nos blockchains atuais.

As condições da oferta serão oportunamente divulgadas; sendo que os ABC tokens a serem ofertados em tal fase serão desde já emitidos e ficarão reservados para negociação em tal oportunidade.



8.3 Novo blockchain e token swap

Uma vez que as duas fases do token sale sejam concluídas com sucesso, será dado início ao desenvolvimento de um novo protocolo de código aberto (*open-source*) para processamento descentralizado de registros de autenticidade, que deverá contar com blockchain específico, sistema próprio de mineração e incentivos (vide item 7.5).

Nesse caso, a OriginalMy estabelecerá um programa de substituição dos tokens utilizados para acesso à Plataforma OriginalMy, bem como cronograma razoável e amplamente noticiado para a troca dos ABC tokens já emitidos por tokens emitidos pelo novo protocolo, na proporção 1:1.

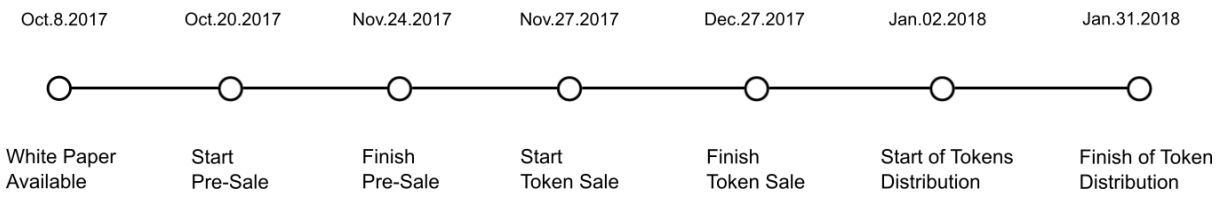
A substituição dos tokens emitidos em plataforma Ethereum pelo token do novo blockchain, será efetuada utilizando tecnologia Atomic Swap[24] ou similar.

8.4 Cronograma da Venda dos Tokens

A venda dos tokens (Token Sale) da Fase 01 seguirá cronograma pré estabelecido com datas chaves (Key Dates) que guiarão todo o processo.

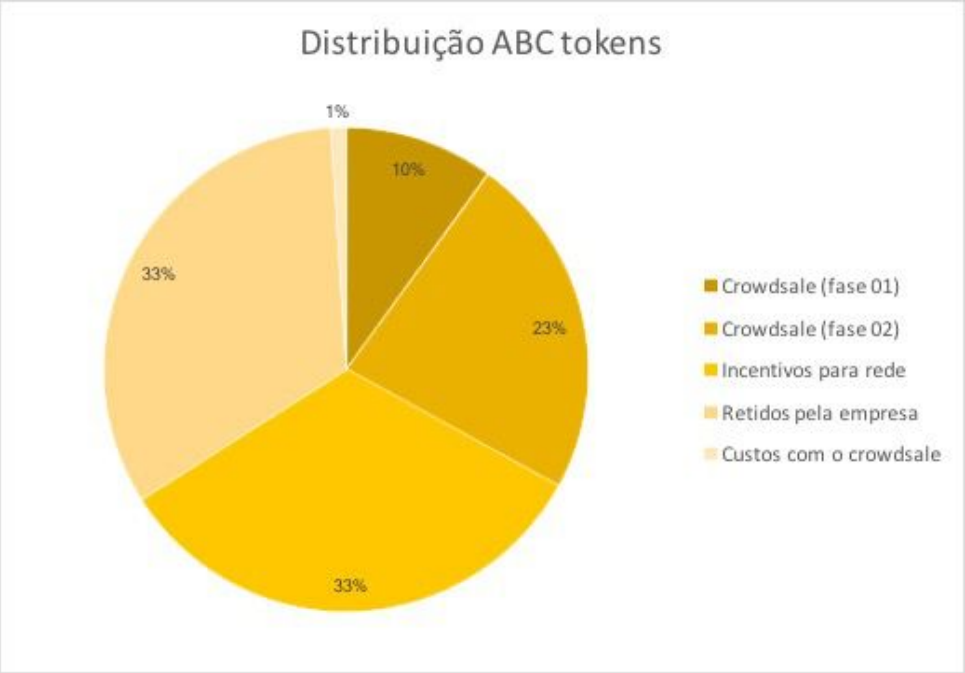
O encerramento acontecerá quando todos os tokens ofertados nesta Fase 01 forem vendidos ou quando atingir a data limite para venda dos tokens, o que ocorrer primeiro.

As Key Dates para a Fase 01 do Token Sale são as seguintes:



8.5 Emissão de tokens e prazos

- Total de Tokens: Serão emitidos 200.000.000 (duzentos milhões) de tokens, que serão distribuídos da seguinte maneira:
    - 33% serão disponibilizados para o Token Sale (Fase 01: 10%, Fase 02: 23%);
    - 33% permanecerão em posse da empresa;
    - 33% serão utilizados para fomento de rede;
    - 1% será utilizado para despesas com o crowdsale.



- Outorga de tokens para equipe (com ou sem vesting): não haverá na fase 1, podendo ser revisto para a fase 2.
- Lançamento do ICO: em 07 de outubro de 2017 será lançado o site exclusivo no qual serão divulgados o whitepaper e demais documentos do projeto. Aqueles que desejarem participar do crowdsale poderão registrar a partir desta data seus dados e intenção de participar do token sale.
- Pré Venda: será realizada a pré venda dos Tokens entre 20 de Outubro de 2017 e 24 de Novembrode 2017. A aquisição de tokens nesse período possibilitará ao comprador a aquisição de um número maior de tokens em relação ao número máximo possível após a abertura do token sale.
- Token Sale: o período pretendido para o Token Sale acontecerá entre 27 de Novembro de 2017 e 27 de Dezembro de 2017.

- Entrega dos Tokens: A distribuição dos tokens para os compradores será efetuada em até, aproximadamente, um mês após o encerramento do Token Sale, estando prevista para ter início em 2 de Janeiro de 2018 e finalizar até 31 de Janeiro de 2018.

8.6 Regras e condições do ABC Token sale - Fase 01

Para que a venda dos Tokens aconteça de maneira organizada e ofereça oportunidade de participação ao maior número de interessados possível, algumas regras deverão ser observadas, conforme definido a seguir:

- Canal oficial: o Token Sale ocorrerá **exclusivamente** através do site https://originalmy.com/ico, onde poderão ser adquiridos os ABC tokens desde que respeitadas as regras do crowdsale. A OriginalMy não se responsabiliza por qualquer oferta, compra e/ou venda ocorrida ou de qualquer forma negociada fora do ambiente do site ora mencionado.

- ABC Tokens: os tokens serão emitidos utilizando a plataforma Ethereum, no formato ERC20. O total de tokens a serem emitidos será de 200 milhões.

- Tokens ofertados: o total de tokens a ser ofertado em fases de crowdsale corresponderá a 33% da totalidade dos tokens ABC emitidos, sendo que destes 20 milhões, correspondentes a 10% do total de ABC tokens, estarão disponíveis para venda nesta oportunidade, ao valor de $0.25 cada token.

- Venda em lotes: Os tokens disponibilizados para venda na Fase 01 serão separados em lotes, a serem anunciados quando da abertura das vendas.

- Limite de participação: somente será permitida a aquisição de 01 (um) lote de tokens por participante. Assim, uma vez finalizada a compra, não será possível efetuar uma nova aquisição de tokens ou quaisquer dados da aquisição já concluída.

- Forma de pagamento: o pagamento pelos ABC tokens poderá ser feito por meio de Bitcoin (BTC) ou Ether (ETH), não sendo aceitas outras formas de pagamento.

- Endereços para pagamento: os endereços das carteiras digitais de Bitcoin e Ethereum apenas serão fornecidas ao comprador no momento do pagamento, exclusivamente pelo site no qual ocorrerá o crowdsale. A OriginalMy não disponibilizará o endereço de carteiras digitais para pagamentos decorrentes do token sale por nenhum outro meio, nem autorizará que outros façam em seu nome. Assim, não se responsabilizará por quaisquer pagamentos realizados em endereços de carteiras distintos daqueles disponibilizados no site oficial do crowdsale.

- Confirmação do pagamento: o pagamento pelos ABC Tokens somente será considerado confirmado, após o mínimo de 6 confirmações pela rede Bitcoin ou 30 confirmações pela rede Ethereum. Uma vez que a transação seja confirmada, a OriginalMy enviará uma notificação por e-mail informando sobre o sucesso da participação no crowdsale.

- Divergências no valor pago: pagamentos recebidos em valor diverso ao custo para aquisição dos ABC Tokens pretendidos, serão devolvidos ao endereço informado pelo participante, sendo o pedido de compra cancelado.

- Prazo para pagamento: uma vez feita a ordem de compra dos ABC Tokens, o pagamento deverá ser realizado em até 30 minutos para o endereço divulgado naquele momento. Caso isso não se verifique,o comprador terá seu pedido de compra de tokens cancelado.

- Valor Mínimo de Contribuição: o *crowdsale* será cancelado e serão reembolsadas todas as compras realizadas caso a venda de tokens não atinja o mínimo de US$ 1.000.000,00;

- Reembolsos: caso ocorra qualquer evento que resulte em reembolso dos valores depositados ao compradores, nos termos já dispostos, a taxa cobrada pelos mineradores para processar tal reembolso será abatido do valor originalmente depositado, sendo-lhe, nesse caso, devolvido o valor líquido.

8.7 Disposições legais

a) Panorama legal das Aplicações da OriginalMy

As aplicações da oferecidas através da Plataforma OriginalMy foram desenvolvidas em consonância com o Princípio da Legalidade aplicável aos particulares e tendo por premissa os ditames das legislações brasileira (em especial, Lei de Registros Públicos [Lei 6.015/73], Lei do Processo Digital [Lei 11.419/06] e demais legislações sobre assinaturas em ambiente digital [Medida Provisória 2200-2/01 e Lei 12.682/12], políticas anti lavagem de dinheiro de KYC emanadas pelo COAF, BACEN e CVM) e estrangeiras (especialmente no que tange a Diretiva UE 2015/849, Financial Action Task Force (FATF) e regulações de KYC/AML/CTF esparsas).

b) Panorama legal dos ABC Tokens

Os ABC Tokens representam uma licença de uso de produtos e/ou aplicações a serem oportunamente disponibilizados na Plataforma OriginalMy, de acordo com termos e condições a serem oportunamente divulgado.

Desta forma, referidos tokens não têm, por definição nem por finalidade, o escopo de representar investimento financeiro com expectativa de retorno. Assim, não possuem natureza de valores mobiliários e/ou *securities*, não conferem a seus possuidores expectativas de ganhos mediantes distribuição de quaisquer valores e/ou dividendos nem conferem direitos, políticos e/ou econômicos, atuais ou futuros, sobre a OriginalMy.

9. Time

O time do OriginalMy é formado por pessoas experientes e com feitos relevantes nas respectivas áreas de expertise.

Edilson Osório Junior - Founder e CEO

Cientista computacional, técnico em processamento de dados, professor e especialista em segurança da informação e infraestrutura, com experiência de 25 anos de mercado. Graduado em Copyright pela Harvard Law School. É referência em Blockchain no Brasil e na América Latina, formou centenas de desenvolvedores e introduziu o assunto para todo o mercado brasileiro, sendo convidado a palestrar em eventos públicos e privados, inclusive internacionais, para falar sobre Blockchain e sobre a disrupção causada pelo OriginalMy.
https://www.linkedin.com/in/osoriojr

Miriam Tomie Oshiro - Co-founder e CFO

Química e Engenheira química especialista em engenharia de processos, iniciando a carreira em 2002 no Departamento de Engenharia Química da USP na área de pesquisa científica voltada para o meio ambiente e depois passando por multinacionais nos segmentos de meio ambiente, plásticos, metais preciosos e máquinas pesadas. Foi diretora de operações da Daruni Healthcare por 4 anos.
https://www.linkedin.com/in/miriam-tomie-oshiro-6a4b9223

Renato Martins da Silva - CTO

Desenvolvedor formado pela FIAP e atuando na área de desenvolvimento desde 2001. Atuou em grandes empresas de GED nacionais e grandes projetos governamentais de processamento e classificação de documentos.
https://www.linkedin.com/in/renatomartinsdev

Helena Suarez Margarido - Legal & Compliance

Advogada formada pela PUC-SP, estudou LLM nos EUA (University of Illinois) e Europa (Universidade Católica Portuguesa). Especialista em Blockchain & moedas digitais há 5 anos, professora e palestrante, no Brasil e no exterior, tem mais de 15 anos de experiência (GP Investments, PwC, Banco Itaú). Sócia fundadora do escritório SuM Law, escritora da Inversa Publicações e co-fundadora do Instituto Bitcoin Brasil.
https://www.linkedin.com/in/helenamargarido

Rafael Matos Araújo - Desenvolvedor

Engenheiro Mecânico formado pela PUC Minas. Trabalhou durante 5 anos no setor de Engenharia Industrial executando projetos de grande porte para grandes companhias brasileiras como Vale e Petrobrás.
https://www.linkedin.com/in/rafamatosaraujo

Renato Novaes de Abreu Neto - Desenvolvedor

Autodidata e apaixonado por tecnologia. Escolheu a programação Web como seu principal foco. Experiência com Chatbots e Processamentos de Web Crawler.
https://www.linkedin.com/in/rnato-neto/

Fernando Henrique Corrêa - Desenvolvedor

Iniciou a carreira desenvolvendo com software livre em 2004. Trabalhou no desenvolvimento do software de sistema para casas noturnas, bares e restaurantes que é referência no segmento. Atuou na Mandic, pioneira no fornecimento de Internet brasileira. Foi integrante da equipe de desenvolvimento do UOL, maior portal de notícias do Brasil, utilizando DevOps com foco em infraestrutura de ambiente de desenvolvimento.
https://www.linkedin.com/in/fernando-henrique-corrêa-98b55920

10. Referências e bibliografia

10.1 Referências bibliográficas

[1] 2017 Index of Economic Freedon: http://www.heritage.org/index/country/brazil (acessado em Out/2017)
[2] Ministério Público Federal: http://www.mpf.mp.br/para-o-cidadao/caso-lava-jato/atuacao-na-1a-instancia/parana/resultado (acessado em 04/10/2017)
[3] G1: http://g1.globo.com/pr/parana/noticia/2015/11/pf-estima-que-prejuizo-da-petrobras-com-corrupcao-pode-ser-de-r-42-bi.html (acessado em 04/10/2017)
[4] Banco Central do Brasil: http://www4.bcb.gov.br/pec/taxas/port/ptaxnpesq.asp?id=txcotacao (acessado em 04/10/2017)
[5] RIBEIRO, Mario Sergio - Pós Graduação Lato-Sensu em Gestão de Segurança da Informação no Instituto de Pesquisas Elétricas e Nucleares da USP (IPEN) - 2003
[6] Orange Book, cap. 5 e 6. - Padrões de Segurança do Departamento da Defesa dos EUA: Critérios para a avaliação de sistemas computacionais confiáveis.
[7] WEBER, Max. “O que é a Burocracia?”, ed. Conselho Federal de Administração, p. 37
[8] OLIVEIRA, Gercina Alves de; “A Burocracia Weberiana e a Administração Federal Brasileira”, 1970, R.A.P, Rio de Janeiro, p. 54
[9] YouTube: https://www.youtube.com/watch?v=gHK9HhzaPog
[10] Bitcoin: A Peer-to-Peer Electronic Cash System. Nakamoto, Satoshi, cap 6: Incentives https://bitcoin.org/bitcoin.pdf (acessado em 02/10/2017)

[11] Ethereum Homestead:
http://ethdocs.org/en/latest/contracts-and-transactions/developer-tools.html (acessado em 21/07/2017)
[12] Caracterizada pelo “empréstimo” de Informação ou qualquer dado próprio para utilização por terceiro, geralmente pessoa com vínculo familiar ou de confiança. Ex: utilização de cartão de crédito de um pai por seu filho, sem conhecimento ou consentimento do primeiro.
[13] Câmara dos Deputados: http://www2.camara.leg.br/participacao/sugira-um-projeto (acessado em 04/10/2017)
[14] Google Impact Challenge | Brazil:
https://desafiosocial.withgoogle.com/brazil2016/charity/its-rio
[15] Mudamos: http://mudamos.org
[16] Hashcash: http://www.hashcash.org
[17] Github: https://github.com/OriginalMy/OrigMyID
[18] Github: https://github.com/bitid/bitid
[19] Ethereum Blog: https://blog.ethereum.org/2014/10/21/scalability-part-2-hypercubes/
[20] Github: https://github.com/decred/dcrtime
[21] Open Timestamps: https://opentimestamps.org
[22] Wikipedia: https://en.wikipedia.org/wiki/SHA-2 (acessado em 21/07/2017)
[23] Bitcoinwiki: https://en.bitcoin.it/wiki/OP_RETURN (acessado em 21/07/2017)
[24] Github: https://github.com/decred/atomicswap

10.2 Bibliografia

[A] Anti-Sybil Mechanism against Bogus Identities in Social Networks:
http://ijartet.com/papers/issue2/V01I020925.pdf (acessado em 04/10/2017)

[B] Verifying Program Executions Succinctly and in Zero Knowledge:
https://eprint.iacr.org/2013/507.pdf (acessado em 06/10/2017)

[C] Enigma: Decentralized Computation Platform with Guaranteed Privacy
https://www.enigma.co/enigma_full.pdf (acessado em 06/10/2017)

[D] Hawk: The Blockchain Model of Cryptography and Privacy-Preserving ...
https://eprint.iacr.org/2015/675.pdf (acessado em 06/10/2017)

[E] Pseudonym Parties:
An Offline Foundation for Online Accountability:
http://www.brynosaurus.com/log/2007/0327-PseudonymParties.pdf (acessado em 06/10/2017)