Novas características do token RDGCoin

1. Nomenclatura

O projeto Rotas do Garimpo possui uma enorme quantidade de diferentes áreas de atuação. Atualmente a maior parte das atividades do projeto estão voltadas para a negociação direta de pedras, jóias e minerais, podendo envolver outros ativos como carros, casas, apartamentos, terrenos, outras criptomoedas, e etc. Porém logo outras iniciativas vão surgir no sentido de atender todo o setor garimpeiro, tanto nas atividades diretas como nas indiretas.

Os participantes do projeto Rotas do Garimpo logo poderão usufruir de muitas outras funcionalidades dentro desse ecossistema, como por exemplo:

- Investir em participações futuras em projetos
- Recrutar financiamento coletivo para iniciativas de mineração
- Emitir participações fracionadas de bens e ativos
- Gerir suas informações, dados, cadastros e licenças dentro da blockchain
- Gerir contratos de maneira automatizada
- Se conectar com clientes e fornecedores dentro da mesma rede utilizando a blockchain
- Adquirir treinamentos, certificações e licenças validadas em blockchain
- e muito mais…

Por conta dessa imensidão de projetos, se torna necessário adotar uma nomenclatura mais específica para cada token, aplicação e rede dentro desse ecossistema. Por isso, a moeda que até então conhecíamos como RDG, agora se chamará RDGCoin, com o intuito de evidenciar sua funcionalidade como “ficha de troca” a ser utilizada dentro do ecossistema Rotas do Garimpo para expressar os valores negociados dentre seus participantes.

Como infelizmente a blockchain do Ethereum não permite a simples atualização do nome do token, a nova moeda RDGCoin será emitida novamente, como se fosse um lançamento inicial. Todos os atuais detentores de RDG poderão trocar seus tokens por RDGCoin sem grandes dificuldades através da ferramenta de “Swap” que será disponibilizada dentro da aplicação “Carteira RDGCoin”.

Juntamente com a atualização do nome, a moeda RDGCoin também terá várias melhorias em comparação com o atual token RDG.

2. Segurança e usabilidade

Com o desenvolvimento do projeto e o aumento da quantidade de funcionalidades e usuários, o token RDG começou a ser explorado muito além do que foi planejado inicialmente. Por isso, com o lançamento do token RDGCoin se faz necessário implementar alguns cuidados a mais quanto à segurança e a usabilidade da moeda.

2.1. Divisibilidade

Atualmente o token RDG pode ser dividido apenas até a sua oitava casa decimal. Isso significa que não é possível transacionar menos do que 0.00000001 unidade de RDG na blockchain do Ethereum.
Inicialmente quando o token RDG era negociado a menos de 1 centavo de real, isso não era nenhum problema, pois não se havia necessidade alguma de transacionar valores tão baixos da moeda. Porém atualmente (Outubro de 2020) com o valor do token se aproximando dos 10 dólares, havendo a possibilidade de alcançar 100 dólares ou mais no próximo ano, esse problema começa a se tornar mais evidente.

Evidenciando o problema: Na hipótese de 1 RDG valer 100 dólares, o valor mínimo a ser transitado de 0.00000001 unidade de RDG significaria um montante de 0.00001 dólares, ou um milésimo de centavo de dólar, que é atualmente cerca de dois centésimos de centavos de real. Aparentemente ainda é um valor pequeno o suficiente para ser desconsiderado, pois geralmente as transações são feitas em centavos, raramente passando dos décimos de centavos em alguns casos. Porém esse problema começa a se tornar evidente quando se é necessário aplicar valores proporcionais sobre números pequenos.

Exemplificando: 3 pessoas possuem saldos em RDG aplicados em “poupança”. Uma com 100 reais, outra com 10 e outra com 1. Essa poupança rende 1% ao mês, portanto ao final do mês essas pessoas teriam respectivamente 101, 10.1 e 1.01 RDG. Caso esse mesmo 1% seja aplicado dia a dia, significaria 0.03333% ao dia - nesse caso ao final do dia essas pessoas teriam respectivamente 100.03, 10.003 e 1.0003 RDG. Como na blockchain do Ethereum os processamentos são feitos bloco a bloco, e que num mês geralmente são gerados 172800 blocos (média de 1 bloco a cada 15 minutos), esse mesmo rendimento de 1% ao mês quando computado bloco a bloco pode resultar em valores infinitesimais de rendimento. Nesse exemplo proposto o rendimento seria de 0.0000057583% por bloco, o que significa que após o primeiro bloco os saldos dessas pessoas seriam de 100.00057583 10.000057583 e 1.0000057583. Como o RDG só possui 8 casas decimais, os valores dos saldos seriam de 100.00057583 10.00005758 e 1.00000575, onde fica evidente que apenas a pessoa que possui 100 RDG obteve o rendimento completo, enquanto as outras duas perderam parte do rendimento por conta do efeito de “truncamento” por conta da falta de casas decimais. No caso de uma pessoa com apenas 1 real aplicado na poupança, seu saldo seria de aproximadamente 0.0018 RDG,

portanto receberia apenas 0.0000000001036494 de rendimento por bloco, equivalente a 0.00000000 RDG. Nesse caso, os usuários dessa poupança precisam de no mínimo 100 reais de aplicação para não perderem por completo seus rendimentos por conta do truncamento, e no mínimo 55000 reais em aplicação para não sofrerem nada com os efeitos de truncamento bloco a bloco.
Esse efeito se agrava mais e mais conforme a moeda obtém mais valor de mercado.

Solução proposta: Seguindo o padrão de todos os grandes projetos de tokens na rede do ethereum, o token RDGCoin possui 18 casas decimais, significando que o mesmo pode valorizar cerca de cem milhões vezes antes que o problema de truncamento comece a ser notado como existe hoje no token RDG.

2.2. Controle do token

Atualmente o token RDG não implementa nenhuma função que indique quem tem a posse sobre o contrato ou sobre o projeto. Em alguns casos isso é desejável, em outros isso pode ser prejudicial. No caso do projeto Rotas do Garimpo, é desejável que as entidades reguladoras possam expressar sua posse sobre o contrato.

Evidenciando o problema: caso seja necessário assinar alguma transação ou mensagem na rede do ethereum para indicar a posse do contrato, não existe nenhuma carteira na rede que seja remetida pelo contrato como “dono” do mesmo.

Exemplificando: Na hipótese de que seja necessário validar uma comunicação feita à comunidade, por exemplo em meio à divulgação de fake news, o “dono” do contrato poderia assinar uma mensagem com sua chave privada (portanto provando sua identidade) para garantir à comunidade a veracidade de algum comunicado. Atualmente isso não é possível.

Solução proposta: Implementar uma propriedade de “Owner” (padrão para a indicação de “dono” de um smart contract) que remete a algum endereço específico da rede. Caso o projeto seja reestruturado com novas entidades reguladoras, é possível fazer a transferência desse título de owner para outra carteira, ou até mesmo para um contrato de multi-assinatura.

2.3. Proteção contra ataques

Atualmente o token RDG possui a função de “aprovar” saldos para uma outra carteira gastar. É uma funcionalidade atualmente pouco explorada dentre seus usuários, porém pode ser de grande utilidade em aplicações mais complexas para o token. Essa função “aprovar” possui uma vulnerabilidade conhecida chamada “front running attack”, que pode ser facilmente explorada por usuários avançados. Por conta disso, se recomenda que não se use a função “aprovar” no token RDG com terceiros que não sejam de confiança.

Evidenciando o problema: Ao aprovar um endereço A para gastar X do seu saldo, a qualquer momento o detentor da chave desse endereço A pode remover até X tokens da sua conta e enviar para qualquer outro endereço, que é justamente a funcionalidade prevista para a função “aprovar”. O problema ocorre quando se emite uma nova aprovação para A no valor de Y. Nesse momento, caso o detentor dessa carteira A seja um atacante, ele pode explorar essa vulnerabilidade. A transação de alteração da aprovação de X para Y pode demorar algum tempo para ser confirmada na rede, geralmente alguns segundos ou minutos, dependendo da taxa escolhida. Nesse cenário o atacante pode enviar uma transação com taxa altíssima para gastar o saldo X antes que a transação de alteração seja processada. Assim, após um tempo de ter gastado X, ele estará permitido a gastar novamente Y, podendo usufruir de X + Y do saldo permitido, enquanto a intenção original era que esse endereço pudesse gastar apenas X ou Y.

Exemplificando: Eu aprovei uma pessoa para remover 500 tokens RDG da minha conta, pois ao fazer isso essa pessoa iria me enviar um ativo que me interessa. Antes que ela fizesse, eu me interessei em outro ativo dessa mesma pessoa no valor de 100 tokens RDG, então alterei minha aprovação de 500 para 600, no intuito que essa pessoa me mandasse tanto o ativo no valor de 500 tokens quanto o ativo de valor 100 tokens. Porém antes que essa transação completasse, essa pessoa removeu 500 tokens da minha carteira, e alguns minutos depois removeu mais 600 tokens, totalizando 1100 tokens aprovados para serem movimentados.

Solução proposta: Implementar as funcionalidades de “aumentar permissão” e “reduzir permissão”, de tal forma que esse comando não reinicia o valor aprovado, mas apenas altera. No exemplo acima, caso o comando fosse de “aumentar a permissão” no valor de 100 tokens, o ataque seria impedido, pois no momento em que fosse executado, a permissão estaria em zero tokens.

3. Mecanismos de recuperação de moedas

Durante a fase de “Swap” (troca de RDG por RDGCoin), usuários que comprovarem terem sido vítimas de fraudes, furtos ou acontecimentos similares poderão ser restituídos de suas perdas com o novo token RDGCoin. Através da funcionalidade de cunhar tokens presente na aplicação de “Swap”, esses tokens podem ser restituídos aos originais donos, com base em provas e evidências objetivas, aceitas e incontestáveis por ao menos 50% da comunidade de usuários do projeto Rotas do Garimpo. Os tokens RDG objetos desses acontecimentos são serão aceitos na aplicação, sendo assim permanecerão na blockchain como tokens RDG, e seus donos não poderão adquirir RDGCoins com as mesmas.

Caso seja de comum acordo pela comunidade, esse efeito pode ser aplicado mesmo após a fase de swap, desde que hajam mecanismos de governança que impeçam o abuso dessa funcionalidade pelas instituições que regulam o projeto Rotas do Garimpo.

4. Conformidade com as normas brasileiras

A Instrução normativa RFB nº 1.888, de 3 de maio de 2019, instaura obrigações a entidades registradas no brasil que transitam valores em criptoativos. Complementada pela Instrução normativa RFB nº 1.899, de 10 de Julho de 2019, a mesma indica informações que devam ser coletadas, processadas e enviadas para a Receita Federal do Brasil.

Com a finalidade de oferecer utilidades diversas ("**Novas aplicações**") para os detentores do token RDGCoin, os solicitantes da aplicação de "Swap" deverão informar algumas informações obrigatórias para cumprimento desta instrução normativa.

Ao receber a aprovação da documentação enviada, todos os usuários do token RDGCoin poderão utilizar suas identidades validadas para futuramente realizar os cadastros nas aplicações de maneira muito mais ágil e segura.

Em conformidade com a Lei Geral de Proteção de Dados (LGPD), todos os usuários terão todos os direitos, deveres e coberturas da lei quanto aos seus dados enviados. Pessoas expostas politicamente (peps) precisam notificar de sua situação ao enviar a documentação a fim de que as medidas legais sejam tomadas quanto às exigências acerca da gestão e retenção de dados.

5. Novas aplicações

Com todas essas melhorias, o token RDGCoin está preparado para dar suporte a diversas aplicações novas para o ecossistema do projeto Rotas do Garimpo.

5.1. Carteira nativa

Com a "Carteira RDGCoin" é possível guardar e utilizar seus tokens sem a necessidade de ferramentas de terceiros. Essa carteira oferece todas as integrações com as demais aplicações, trazendo segurança e facilidade de uso.

Os participantes do projeto poderão utilizar essa aplicação tanto do computador, quanto de celulares, tablets e até mesmo relógios inteligentes.

A "Carteira RDGCoin" é uma aplicação **não custodial**, o que significa que todos os seus ativos estão sobre a sua gestão apenas, de forma completamente segura e protegida contra ataques de terceiros. Nesse tipo de aplicação, é sempre muito importante **guardar a chave de recuperação** da sua carteira, pois sem essa chave é impossível recuperar a sua conta caso seja necessário.

5.2. Compatibilidade com outras carteiras

Mesmo com a aplicação “Carteira RDGCoin”, ainda assim é possível adicionar o token RDGCoin na sua aplicação carteira favorita. Basta seguir as instruções da sua carteira e adicionar o endereço do smart contact do token RDGCoin, que você poderá usufruir de todas as funcionalidades hoje presentes no token RDG.

Algumas funcionalidades presentes no token RDGCoin só podem ser exploradas em carteiras específicas, portanto sempre consulte as informações técnicas para se assegurar de todos os passos necessários para interagir com as aplicações do token RDGCoin a partir de carteiras de terceiros.

5.3. Ferramenta de e-commerce

Com o token RDGCoin será possível realizar a compra de itens a venda no e-commerce do Rotas do Garimpo, que serão negociados **exclusivamente em RDGCoin**.

A aplicação de e-commerce do Rotas do Garimpo é uma aplicação **custodial centralizada**, o que significa que o saldo depositado na mesma estará sob posse de terceiros, e portanto exige uma relação contratual de custódia e de operação entre as partes, na qual é inevitavelmente aplicável a IN RFB nº 1.888 e a IN RFB nº 1.899.

5.4. Ferramenta de leilão

Com o token RDGCoin será possível realizar lances sobre itens em exposição no leilão do Rotas do Garimpo, que serão negociados **exclusivamente em RDGCoin**.

A aplicação de leilão do Rotas do Garimpo é uma aplicação **custodial centralizada**, o que significa que o saldo depositado na mesma estará sob posse de terceiros, e portanto exige uma relação contratual de custódia e de operação entre as partes, na qual é inevitavelmente aplicável a IN RFB nº 1.888 e a IN RFB nº 1.899.

5.5. Exchange dedicada

O token RDGCoin poderá ser negociado com diversos outros ativos digitais tanto na modalidade de corretagem quanto de intermediação. **Corretagem**: conversão de um ativo por outro mediante a um câmbio flutuante; **Intermediação**: livro público de ofertas com compradores e vendedores de ambos os lados dos pares de negociação, no qual as trocas ocorrem de acordo com os encontros das ofertas de ambos os lados.

O token RDGCoin continuará listado em exchanges de terceiros para serem negociados em outros mercados, de acordo com a própria adoção nas comunidades externas.

A aplicação de exchange do Rotas do Garimpo é uma aplicação **custodial centralizada**, o que significa que o saldo depositado na mesma estará sob posse de terceiros, e portanto exige uma relação contratual de custódia e de operação entre as partes, na qual é inevitavelmente aplicável a IN RFB nº 1.888 e a IN RFB nº 1.899.