DOCUMENTO PARA REGISTRO DE IDEIA,SOFTWARE E MARCA NO INPI

1. **Título do Projeto**

PayByt – ***Plataforma de Marketplace Descentralizada com Escrow Multisig e Lightning Network***

Comércio Seguro e Privado Impulsionado por Bitcoin

1.2 - Domínio Plataforma

www.paybyt.com (*Em construção)*

---

2. Titular da Ideia

Nome: Daniel Clayton dos Santos Cardoso Lobo
Endereço: Alameda Itapecuru, 149, Apto 1201, Alphaville, Barueri-SP
CPF: 060.834.536-90
E-mail: cardosolobo@protonmail.com
Telefone : 31-998292222
Co-titulares:
1 - **Eduardo Ruan Ribas Marinho**, CPF 117.348.999-13, Rua Trajano Araújo lejanoski,125, Bairro Araucária, Candoi-PR, Cep: 85140000;
2 - **Alexon José Umbelino da Conceição**, CPF 030.448.335-40, Rua Rubens Pinheiro, Amaralina, Salvador – BA;
3 - **Paulo Alexandre Reducino**, CPF 378.713.928-16, endereço Alameda 6, Bloco L, Apartamento 304, Bairro Bequimão, Condomínio Buena Vista, São Luis – MA, CEP 65.061-550;
4 - **Breno Roberto da Silva**, CPF 500.568.878-17, Endereço Rua Adelmo Arkanjo Bissi, 314, Cachoeira, Curitiba – PR;
5 - **Rodolfo Romão de Oliveira**, CPF 005.502.351-75, endereço Av. Rabelo, lote 2, Vila Planalto, Brasília, DF.

6 - Nome: Rafael Meira De Oliveira, CPF: 374.968.458-84, endereço Rua Mário Bassani, 43, Campinas - SP

---

3. Resumo da Ideia

O ***PayByt*** é uma plataforma descentralizada que conecta compradores e vendedores para transações seguras de produtos e serviços exclusivamente utilizado o Bitcoin como forma de pagamento. Utilizando *escrow multisig*, suporte nativo à *Lightning Network* e inteligência artificial para detecção de fraudes. O ***PayByt*** garante privacidade total sem KYC, oferecendo uma solução inovadora, irrastreável e imbloqueável para o comércio global. Seu diferencial é a integração de transações rápidas e baratas com um sistema de mediação automatizado e inovador baseado em blockchain.

---

4. Descrição prévia do Projeto

O ***PayByt*** é um marketplace digital que opera exclusivamente com Bitcoin, aproveitando carteiras multisig para escrow, IA para segurança e tecnologias descentralizadas para privacidade. A plataforma será construída em Node.js, garantindo desempenho e escalabilidade.

Destaque o diferencial competitivo, pois será a primeira plataforma a integrar Lightning Network com escrow automatizado.

4.1 Funcionalidades Principais

- Cadastro anônimo via e-mails criptografados (ex.: ProtonMail).
- Escrow seguro com carteiras multisig (2 de 3 chaves: comprador, vendedor e plataforma como julgada), implementada com *bitcoinjs-lib* .
    - **Funcionamento do Escrow** :

- **Recebimento do Pagamento** : Quando o comprador realiza o pagamento em Bitcoin, a plataforma gerará um endereço Bitcoin temporário, onde o pagamento será depositado.
- **Impossibilidade de transferência** : O pagamento em Bitcoin será **retido** em uma **conta de depósito imbloqueável e intransferível** até a notificação da retirada do produto. Isso significa que o comprador não poderá transferir o pagamento de volta até a liberação da plataforma.
- **Implementação com Multisig** : Para garantir que o Bitcoin seja imbloqueável, utilizemos **endereços multisig** . O pagamento será enviado para uma carteira multisig, que exigirá várias assinaturas para ser transferida. As assinaturas podem ser divididas entre:
  - **Uma assinatura do comprador** (confirmando que o produto foi entregue).
  - **Uma assinatura do vendedor** (confirmando que o pagamento foi recebido).
  - **Uma assinatura da plataforma** (garantindo que todas as condições foram atendidas).
- **Seguro** : Em caso de disputa (por exemplo, se o comprador não confirmar a coleta), a plataforma pode funcionar como intermediária, decidindo sobre o depósito após uma análise de evidências.

- Sistema de avaliação na blockchain para avaliar compradores e vendedores, com base em transações concluídas.
- Interface intuitiva e acessível, otimizada para desktop e mobile.
- Detecção de fraudes e produtos ilícitos por IA (ex.: análise de texto com PNL, visão computacional para imagens).
- Suporte a transações *Bitcoin on-chain, Liquid e Lightning Network*, com escolha pelo usuário.
- Integração com gateways como *BTCPay Server, OpenNode e CoinGate.*
- Carteira Bitcoin integrada, funcionando como "saldo" para compras instantâneas.
- Contratos inteligentes via *Rootstock (RSK*) para automação de transações.
- Suporte a transações *off-chain* com liquidação *on-chain* sob demanda.
- Notificações em Tempo Real: Atualizações sobre pagamentos, disputas e mensagens via WebSockets,
- Dashboard: Histórico de transações, estatísticas e acompanhamento de pagamentos.

- **Chat Seguro**: Comunicação criptografada entre comprador e vendedor com suporte a anexos.

4.1.1 Política de Proteção de Dados

- Dados criptografados com provas de conhecimento zero (ZKPs) para validação anônima.
- Sem KYC, apenas e-mails criptografados para cadastro.
- Transações registradas diretamente na blockchain, sem armazenamento centralizado sensível.
- Conformidade com a LGPD (Brasil) via anonimização e consentimento explícito opcional.
- Monitoramento de atividades suspeitas sem comprometer a privacidade.
-

4.1.2 Segurança

- Criptografia AES-256 de ponta a ponta para dados sensíveis.
- Autenticação 2FA obrigatória (ex.: Google Authenticator ou YubiKey).
- IA para monitoramento proativo de fraudes. A plataforma utilizará **algoritmos de IA** para detectar e bloquear produtos que envolvam conteúdo ilícito, como drogas, pornografia, pedofilia, violência e outros.
- **IA de Texto** : Algoritmos de processamento de linguagem natural (PNL) serão usados para analisar a investigação dos produtos e identificar palavras-chave associadas a atividades ilegais.
- **IA de Imagem** : Implementação de modelos de **análise de imagem** para verificar se as imagens dos produtos são adequadas e não contêm conteúdo ilícito.
- Armazenamento refrigerado para fundos de garantia em carteiras offline.
- Auditorias trimestrais por empresas especializadas (ex.: Chaincode Labs).

4.1.3 Experiência do Usuário

- Interface simplificada com suporte multilíngue (inglês, português, espanhol).

- Visualização de produtos em realidade aumentada (AR) no mobile via WebAR.
- Suporte 24 horas por dia, 7 dias por semana via chat com IA e opção de escalonamento humano.
-

4.1.4 Escalabilidade e Infraestrutura

- Hospedagem híbrida: IPFS para descentralização e AWS/Google Cloud para redundância.
- Escalabilidade com Node.js e clusters gerenciados por PM2 e Nginx para balanceamento de carga.

4.1.5 Estratégia de Lançamento

- **Comunidade:** Engajamento em fóruns (Reddit r/Bitcoin, Bitcointalk) e X (#PayByt).
- **Incentivos:** Taxas zero nos primeiros 3 meses para os primeiros adotantes.
- **Parcerias:** Colaboração com influenciadores de criptografia e lojas que aceitam Bitcoin.
- **Beta:** Teste fechado com 100 usuários selecionados no terceiro trimestre de 2025.
- **Educação:** Tutoriais em vídeo e blog sobre Bitcoin e Lightning Network.

4.1.6 Manutenção e Expansão

- Atualizações mensais com base em feedback.
- Roteiro: Integração com Ethereum/Solana em 2027; marketplace P2P completo em 2028.
-

4.2 Tecnologias Utilizadas

- **Front-end:** React.js (v18), Tailwind CSS.
- **Back-end:** Node.js (v20), Express.js, MongoDB (com Mongoose).

- **Blockchain:** bitcoinjs-lib (multisig), lnd (Lightning Network), Rootstock (contratos inteligentes).
- **Infraestrutura:** Docker, PM2 (gestão de processos), Nginx (balanceamento).
- **Segurança:** criptografia (Node.js nativo), ZKPs via zk-snarkjs .
- **Uso de VPN e Proxy** : A arquitetura do servidor utilizará técnicas como VPN e proxies para adicionar camadas de anonimato.
- **Criptografia de ponta a ponta** : Todas as comunicações serão criptografadas com **SSL/TLS**

4.3. Envio Efetivo da Mercadoria

O processo de envio da mercadoria pode ser estruturado de maneira clara para garantir segurança e rastreabilidade. Aqui estão algumas opções:

4.3.1. Confirmar o Envio da Mercadoria

Para que o comprador tenha confiança de que o pagamento em Bitcoin será liberado apenas após a retirada do produto, podemos criar um sistema de **rastreabilidade de envio** .

Opções para rastrear o envio:

- **Integração com Serviços de Correios** : Uma plataforma pode integrar um serviço de rastreamento com os correios ou transportadores para que o comprador possa acompanhar o status do envio.
- **Código de Rastreamento** : O vendedor poderá fornecer um **código de rastreamento** do envio, que será compartilhado com o comprador através da plataforma.
    - O comprador será notificado assim que o código for atualizado, garantindo maior transparência.

4.3.2. Confirmação de Recebimento

- **Envio de fotos/provas** : Além do código de rastreamento, o comprador poderá solicitar o envio **de fotos** ou **provas de coleta** (como uma foto do

pacote e do produto), caso necessário, para confirmar que o item foi entregue em boas condições.

- **Sistemas de Feedback** : O comprador também poderá deixar um feedback de coleta, como uma **nota de 1 a 5 estrelas** , para que a plataforma saiba que a transação foi concluída corretamente.

4.3.3. Tempo de Espera e Prazo de Confirmação

- **Prazo para Confirmação** : Após o envio do produto, o comprador terá um prazo (por exemplo, **7 dias**) para confirmar que o produto foi recebido em boas condições. Caso não haja confirmação dentro desse prazo, o pagamento será devolvido automaticamente ao comprador.
- **Disputa** : Se houver desacordo (por exemplo, o comprador alega não ter recebido o produto), a plataforma pode agir como mediadora, resolvendo o problema com base nas entregas fornecidas, como o código de rastreamento ou fotos.

4.4. Remuneração do *PayByt*, dos Mineradores e da Rede da Blockchain

4.4.1. Taxas de Transação para Mineradores

A blockchain do Bitcoin possui um sistema de **taxas de mineração** para validar as transações. O valor pago aos mineradores é cobrado a partir da transação feita entre comprador e vendedor.

Como gerenciar essas taxas:

- **Responsabilidade do Comprador** : Nas transações na ***PayByt***, o comprador geralmente paga a taxa de mineração para garantir que a transação seja confirmada na blockchain. No entanto, a plataforma pode permitir que o comprador escolha a **taxa** (maior taxa para maior prioridade de confirmação).
- **Taxa Variável** : As taxas de transação podem variar dependendo do congestionamento da rede. A plataforma pode gerar automaticamente uma taxa média estimada para que o comprador tenha uma transação confirmada de forma rápida.

4.4.2. Remuneração da Plataforma

- A plataforma terá uma comissão, por exemplo, de **10% a 11,5%** sobre cada negócio concluído, como já foi planejado.
    - Esta comissão será cobrada do **vendedor**, mas o valor da comissão será deduzido diretamente no momento da liberação do pagamento do depósito para o vendedor, após a confirmação do comprador.

4.4.3. Taxa para a Rede Blockchain (Plataforma)

- Além das taxas de transferência pagas aos mineradores, pode ser necessário cobrar uma taxa adicional para a **manutenção da rede da plataforma** (como parte da estrutura de custos de operação da plataforma).
- **Taxa de Rede da Plataforma** : Essa taxa pode ser uma pequena porcentagem ou valor fixo cobrado em cada transação para suportar as atividades da plataforma, como servidores, APIs de blockchain, monitoramento e segurança.
    - Por exemplo, uma **taxa de manutenção de 1%** sobre o valor total da transação pode ser deduzida do valor antes de ser repassada ao vendedor.

4.4.2. Integração com a Rede Blockchain para Escrow

- **Blockchain Imbloqueável** : Para garantir que os Bitcoins se tornem **imbloqueáveis** até a liberação do pagamento, uma plataforma pode usar a funcionalidade de **multisig** . Uma carteira **multisig** exige múltiplas assinaturas (comprador, vendedor e plataforma) para liberar a transação.
    - O Bitcoin poderá ser transferido de volta ou liberado para o vendedor depois que todas as partes envolvidas confirmarem as condições da transação.
    - Isso garante a segurança para ambas as partes, pois a plataforma tem controle sobre o fluxo de dinheiro até que as condições sejam atendidas.

---

5. Protótipo e Referências

Protótipo: https://daniellobo989.github.io/paybyt/

*(***Referências:** OpenBazaar (P2P), Bitcart (cripto-commerce) – diferenciais: Lightning nativa e blockchain.

---

6. Duração da Proteção e Condições

Proteção solicitada por **10 anos** (conforme padrões de patente de software, sujeito a consulta jurídica). Multa por violação: **R$ 1.500.000,00** , proporcional ao impacto estimado.

---

7. Dados locais

São Paulo, 16 de março de 2025

---

8. Código-Fonte Desenvolvido.

HASH SHA256

dda24e9eec557b241dce3162cbc1f0c446954876d00b59e574351640e472af26

---

9. Assinatura do Titular
Daniel Clayton dos Santos Cardoso Lobo
Revisado em: 16 de Março de 2025

---

10. Testemunhas

1. **Nome:** [A ser preenchido]
   CPF: [A ser preenchido]
   Assinatura: _____
2. **Nome:** [A ser preenchido]
   CPF: [A ser preenchido]
   Assinatura: _____