

МОНГОЛ УЛСЫН ИХ СУРГУУЛЬ
МЭДЭЭЛЛИЙН ТЕХНОЛОГИ, ЭЛЕКТРОНИКИЙН СУРГУУЛЬ
МЭДЭЭЛЭЛ, КОМПЬЮТЕРЫН УХААНЫ ТЭНХИМ

Энхбаярын Жавхлан

Блокчэйн суурьт лиценз баталгаажуулалт
(Licence validation with blockchain)

Программ хангамж
Бакалаврын судалгааны ажил

Улаанбаатар хот

2024 он

МОНГОЛ УЛСЫН ИХ СУРГУУЛЬ
МЭДЭЭЛЛИЙН ТЕХНОЛОГИ, ЭЛЕКТРОНИКИЙН СУРГУУЛЬ
МЭДЭЭЛЭЛ, КОМПЬЮТЕРЫН УХААНЫ ТЭНХИМ

Блокчэйн суурьт лиценз баталгаажуулалт
(Licence validation with blockchain)

Программ хангамж
Бакалаврын судалгааны ажил

Үдирдагч: _____ Дэд профессор Ч.Алтангэрэл

Гүйцэтгэсэн: _____ Э.Жавхлан (20B1NUM0649)

Улаанбаатар хот

2024 он

Зохиогчийн баталгаа

Миний бие Энхбаярын Жавхлан ”Блокчэйн суурьт лиценз баталгаажуулалт” сэдэвтэй судалгааны ажлыг гүйцэтгэсэн болохыг зарлаж дараах зүйлсийг баталж байна:

- Ажил нь бүхэлдээ эсвэл ихэнхдээ Монгол Улсын Их Сургуулийн зэрэг горилохоор дэвшүүлсэн болно.
- Бусдын хийсэн ажлаас хуулбарлаагүй, ашигласан бол ишлэл, зүүлт хийсэн.
- Ажлыг би өөрөө (хамтарч) хийсэн ба миний хийсэн ажил, үзүүлсэн дэмжлэгийг тайлангийн ажилд тодорхой тусгасан.
- Ажилд тусалсан бүх эх сурвалжид талархаж байна.

Гарын үсэг: _____

Огноо: _____

Батлав.

МКҮТ-ийн эрхлэгч/Дэд профессор, Ч.Алтангэрэл/

2024 оны 02 сарын 12 наадам

Монгол нэр: Блокчэйн сурьт лиценз багалгаажуулалт

Англи нэр: Licence validation with blockchain

Сэлзвт бакалаврын судалгааны ажлын 7 хоногийн үучилсэн төлөвлөгөө

Хугацаа: 2024.02.13-ас 2024.05.23 хүргэл 14 долоо хоног

№	Хийх ажлы	Долоо хоног												13 Засаж сайжруулалт	14 Жинхэн хамгаалалт	
		0	1	2	3	Яви I	4	Яви II	5	6	7	8	9	10	11	12
1	Судалгаа	Сэдвийн Технологийн														
2	Системийн шинжилгээ шингилгээ тодорхойлолт зохиомж	Шаардлагын тодорхойлолт														
3	Системийн хэрэгжүүлэлт	Системийн UI/UX дизайн														
4	Түршилт	Үндсэн код НЭМЭЛТҮҮД														
5	Тайлан	Тест Сайжруулалт Явцын Эцсийн														

Тайлбар: Төслийг хэрэгжүүлэх төлөвлөгөөг 7 хоногийн давтамжтайшар хийж тод хараар бүдэж тэмдэглээнэ. Хийх ажлын дүрүүдэд ялгарах хувьдад төлөвлөж болно. Ажлын эхийг төсвэх хугацаа хөгөөндоо давтаж болно. Ажлын түүрээндээх хийх боломжтой байхадар "Хоног" баганыг тусгаснаа.

Зөвшөөрсөн: Удирдагч багш/Дэд профессор Ч.Алтангэрэл/

Боловсруулсан: Оюутан/Программ хантамж-4, Э.Жавхлан/
Оюутны ID: 20b1num0649
Холбогдох утас: 88242310

МУИС-ийн МТЭС-ийн Программ хангамж хотолбөрийн оюутан
Энхбаяр овогтой Жавхлан “Блокчэйн суурьт лиценз баталгаажуулалт” сэдэвт
бакалаврын судалгааны ажлын удирдагчийн тодорхойлолт

2023-05-17

Оюутан Э.Жавхлан нь бакалаврын судалгааны ажлыг “Блокчэйн суурьт лиценз баталгаажуулалт” сэдвээр хийж гүйцэтгэлээ. Энэхүү ажил нь блокчэйн технологиор дамжуулан цахим бүтээлийг хамгаалах, хуваалцах, түүнд хандах зөвшөөрөл олгох цахим бүтээлийн лицензийн төвлөрсөн бус систем хөгжүүлэх зорилготой. Энэ ажлыг гүйцэтгэнээр блокчэйн технологийн төвлөрсөн бус, ил тод, хувиршгүй шинж чанарыг ашиглан цахим бүтээгдэхүүн эзэмших, лиценз олгоход итгэлцэл, ил тод байдлыг бий болгож хуурамч лиценз, хууль бус хуулбарлалтыг бууруулах, зөвшөөрөлгүй түгээлтийг таслан зогсоох ач холбогдолтой юм.

Оюутан Э.Жавхлан нь энэхүү системийг эхнээс нь алхам алхмаар шаардлагаас нь хэрэгжүүлэлт хүртэл хийж гүйцэтгэсэн ба системийн судалгаа, шинжилгээ зохиомжийг зохих дарааллын дагуу гүйцэтгэсэн болно. Хэрэгжүүлэлтийн хувьд Next.js, этереум блокчэйн, ухаалаг гэрээ, IPFS болон Lit протокол технологиудыг ашиглан хийсэн.

Ажлын гүйцэтгэлийн хувьд тавьсан зорилгодоо тодорхой түшинд хүрсэн, баримт бичгийн боловсруулалтын хувьд шаардлагад нийцсэн ажил болсон гэж үзэж оюутан Э.Жавхланг удирдагч багшийн зүгээс жинхэнэ хамгаалалтад орохыг дэмжиж байна.

Удирдагч:  /доктор, дэд профессор Ч. Алтангэрэл/

МУИС, МТЭС-ийн ПХ-ын 4-р ангийн оюутан Э.Жавхлан
“Блокчэйн суурьт лиценз баталгаажуулалт”
сэдэвт төгсөлтийн ажилд өгөх шүүмж

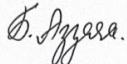
Оюутан Э.Жавхлан нь төгсөлтийн ажлын хүрээнд хэрэглэгчид блокчэйн технологиор дамжуулан цахим бүтээлийг хамгаалах, хуваалцах, түүнд хандах зөвшөөрөл олгох цахим бүтээлийн лицензийн төвлөрсөн бус систем хөгжүүлэх зорилго тавин ажиллажээ.

Ажлыг сайжруулах дараах саналыг өгч байна. Үүнд:

1. Гарчиг хэсгийн удиртгал доор Сэдэв сонгосон үндэслэл, Зорилго, Зорилт бичих шаардлагагүй. Удиртгалыг дэлгэрэнгүй бичихдээ доош цувруулан бичсэн байхад болно.
2. Удиртгал бүлэгт сэдвийн ач холбогдол, сэдвийн судлагдсан байдал, ашигласан технологи/арга зэргийг нэмж оруулах;
3. Онолын судалгаа хэсэгт Блокчэйнтэй холбоотой хэсгүүдийг 1 бүлэг болгожи нэгтгэх;
4. Системийн шинжилгээ, зохиомж бүлгийг салгах;
5. Хавсралтад байгаа үечилсэн төлөвлөгөөг хасах;
6. Хуудаснуудад өгсөн header устгах;
7. Онолын судалгаа хэсэгт ижил төстэй системийн судалгааны ажил дээр өөрийн санал болгож буй системтэй харьцуулан харуулах; Ойлгомжтой, цэгтэй байлгах үүднээс харьцуулалтуудыг хүснэгтлэх;
8. Бүлэг бүрийн эхэнд тухайн бүлэгт хийгдэх ажлын талаар ерөнхий тайлбар оруулах, хэт богино биш байхыг анхаарах; Жишээ нь: Системийн шинжилгээ бүлгийн хүрээнд шинжилгээнүүдийг хийлээ гэх мэт;
9. Шаардлагуудыг хүснэгтлэх, тайлбар оруулах;
10. Диаграммуудад тайлбар бичих;
11. Хүснэгтүүдэд тайлбар бичих, хэт товч биш байх;
12. Судалгааны ажил учраас холбоотой хийгдсэн судалгааны ажлуудаас ишлэл оруулах;
13. Үг сонголтоо анхаарах. Ойлгомжгүй өгүүлбэр, найруулгыг засах.
14. Үг үсгийн алдаа их байгааг засах;

Энэхүү төгсөлтийн ажилд шүүмжлэгчийн зүгээс 5 оноо өгч байна.

Шүүмж бичсэн: Б.Аззаяа /Дадлагажигч багш/



2024 оны 5 дугаар сарын 11

ГАРЧИГ

УДИРТГАЛ	1
БҮЛГҮҮД	2
1. ОНОЛЫН СУДАЛГАА	2
1.1 Блокчэйн технологи	2
1.2 Дижитал эрхийн менежмент (DRM)	7
1.3 DRM систем дэх блокчэйн технологийн боломжууд	8
1.4 Технологийн судалгаа	9
1.5 Ижил төстэй системийн судалгаа	12
2. СИСТЕМИЙН ШИНЖИЛГЭЭ, ЗОХИОМЖ	14
2.1 Системийн шаардлага	14
2.2 Системийн ажлын явцын диаграмм	17
2.3 Дарааллын диаграмм	18
2.4 Архитектур	20
3. СИСТЕМИЙН ХЭРЭГЖҮҮЛЭЛТ	21
3.1 Хөгжүүлэлт	21
3.2 Үр дүн	29
ДҮГНЭЛТ	34
НОМ ЗҮЙ	35
ХАВСРАЛТ	36
A. КОДЫН ХЭРЭГЖҮҮЛЭЛТ	36
A.1 Ухаалаг гэрээ	36

ЗУРГИЙН ЖАГСААЛТ

1.1	Блокчэйний өгөгдлийн бүтэц	3
1.2	”Hello World”, ”Hallo World” гэсэн үгнүүдийн хэшийг бодсон байдал	4
1.3	Цахим гарын үсгийн ажиллах зарчим	5
2.1	Use-case диаграмм	17
2.2	Хэрэглэгч цахим бүтээл оруулах дарааллын диаграмм	18
2.3	Хэрэглэгч цахим бүтээлийг хүсэх дарааллын диаграмм	19
2.4	Системийн ерөнхий архитектур	20
3.1	Хөгжүүлэлтийн орчин	21
3.2	Хэрэглэгчийн үндсэн хуудас	29
3.3	Цахим бүтээл оруулах хуудас	29
3.4	Миний сан хуудас	30
3.5	PDF файл харах	30
3.6	Video файл харах	31
3.7	Marketplace хуудас	31
3.8	Marketplace дэх бүтээлийн хуудас	32
3.9	Лиценз хүсэлтийн хуудас	32
3.10	Лицензийн хуудас	33
3.11	Лицензийн гэрчилгээ харах	33

ХҮСНЭГТИЙН ЖАГСААЛТ

1.1	Системүүдийн харьцуулалт	13
2.1	Функциональ шаардлагууд	15
2.2	Функциональ бус шаардлагууд	16
3.1	Ухаалга гэрээний функцийд	22

Кодын жагсаалт

3.1	Ухаалаг гэрээг блокчэйнд байршуулах	23
3.2	Lit protocol-н файл шифрлэлт болон хандалтын хяналтын нөхцөл	24
3.3	Файлыг IPFS-д хадгалах	26
3.4	Ухаалаг гэрээний өгөгдлийг унших	26
3.5	Ухаалаг гэрээний өгөгдлийг унших	27
A.1	Ухаалаг гэрээ	36

УДИРТГАЛ

Өнөөгийн цахим орчинд зонхилон тохиолдож буй оюуны өмч болон цахим бүтээгдэхүүний хулгай, өмчлөх эрхийн ил тод байдал, зөвшөөрөлгүй түгээлт зэрэг сорилтуудтай тулгарч байна. Блокчэйн технологи нь цахим орчинд аюулгүй байдал, итгэлцлийг хангах, болон төвлөрсөн бус менежментийн боломжийг олгодог онцлог шинж чанартай. Энэ нь зөвхөн криптовалютын салбарт бус, цахим лицензийн баталгаажуулалт, оюуны өмч хамгаалал зэрэг олон салбарт ач холбогдолтой юм. Цахим бүтээгдэхүүний лицензийг баталгаажуулах системд блокчэйн технологийг ашигласнаар хуурамч лиценз, хууль бус хуулбарлалтыг бууруулах, зөвшөөрөлгүй түгээлтийг таслан зогсоох боломжтой.

Блокчэйн технологийн талаар судалгаа анх 2008 онд Сатоши Накамото-гийн “Биткойн: Peer-to-Peer Электрон Мөнгөний Тогтолцоо” нийтлэлээр эхэлсэн. Үүнээс хойш блокчэйн технологийн олон салбар дахь хэрэглээний талаар өргөн хүрээтэй судалгаа хийгдсэн. Гэсэн хэдий ч, цахим лицензийн баталгаажуулалтын тал дээрх судалгаа харьцаангуй шинэ бөгөөд энэхүү судалгаагаар энэ чиглэлд тулгарч буй сорилтууд, боломжуудыг илрүүлэн судлах болно.

Энэхүү судалгааны ажлаар блокчэйн технологиор дамжуулан цахим бүтээлийг хамгаалах, хуваалцах, түүнд хандах зөвшөөрөл олгох цахим бүтээлийн лицензийн төвлөрсөн бус систем хөгжүүлэх зорилготой билээ. Уг зорилгын хүрээнд дараах зорилтуудыг тавьсан болно:

1. Блокчэйн технологийн талаарх ойлголт, хэрэглээний боломжууд болон дижитал эрхийн менежментийн талаар судлах
2. Системийг хэрэгжүүлэх шаардлагатай технологи, арга хэрэгслүүдийг судлах
3. Системийн зохиомж, архитектурыг боловсруулах
4. Блокчэйн дээр сууриссан цахим бүтээлийн лицензийн систем хөгжүүлэх

1. ОНОЛЫН СУДАЛГАА

Онолын судалгаа бүлгийн хүрээнд блокчэйн технологи болон дижитал эрхийн менежментийн талаар судлах мөн цахим бүтээлийн лицензийн төвлөрсөн бус системтэй ижил төстэй системүүд болон, энэхүү сэдвээр судалгааны ажил хийгдсэн эсэхийг судалж хооронд нь харьцуулалт хийх бөгөөд үүний үр дүнд системийн хэрэгцээ шаардлага, давуу тал, өөр ямар нэмэлт боломжууд байж болох талаар мэдэх юм. Мөн системийг хөгжүүлэхэд шаардагдах технологи болон фреймворкуудын талаарх судалгааг хийлээ.

1.1 Блокчэйн технологи

Хамгийн анх блокчэйн технологийн талаар 2008 онд Сатоши Накамото гэдэг этгээдийн нийтэлсэн “Биткойн: Peer-to-Peer Электрон Мөнгөний Тогтолцоо” судалгааны ажлын нийтлэлд дурдагдсан байдаг [1].

Блокчэйн гэдэг нь өгөгдөл буюу дата мэдээллүүдийг хадгалдаг нэгэн төрлийн мэдээллийн бааз гэж хэлж болно. Бааз доторх дата мэдээллийг Блок гэж нэрлэгдэх хэсгүүдэд багцлан хадгалж уг сүлжээнд холбогдсон бүх компьютерт ижил хуулбар болгон тархмал хэлбэрээр хадгална. Тэдгээр блокуудыг өөр хоорондоо гинжин хэлхээ буюу математик тооцоолол, цахим нууцлалын аргаар хэлхэн холбосноор бидний ярьж буй Блокчэйн үүсэх юм.

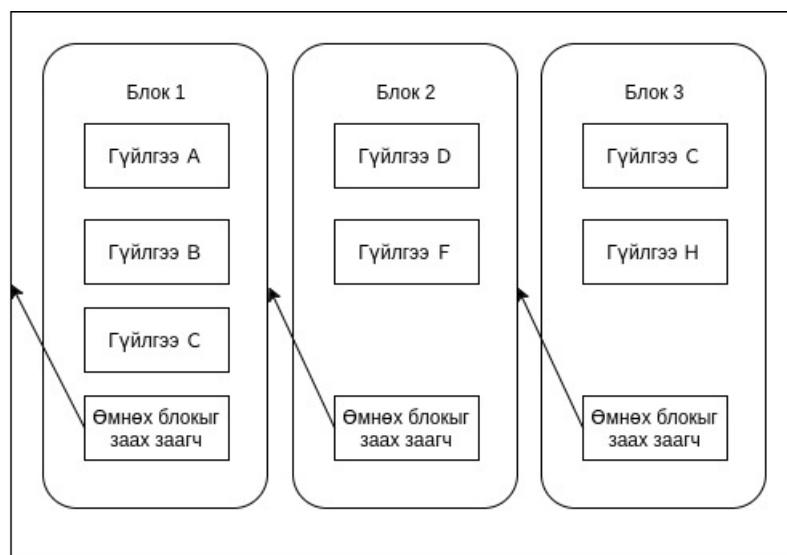
1.1.1 Блокчэйний онцлог

Тархсан Peer-to-Peer (P2P) сүлжээ гэдэг нь сүлжээнд оролцогч буюу зангилаанууд нь газарзүйн хувьд тархсан байдаг ба аль ч хоёр зангилаа хоорондоо байршилаас үл хамааран ямар нэг серверээр дамжилгүйгээр өөр хоорондоо шууд холбогдог сүлжээ юм.

Тархсан бүртгэлийн дэвтэр буюу Distributed ledger technology (DLT) технологи нь мэдээллийг тархсан P2P сүлжээний оролцогч нар дээр хадгалдаг технологи бөгөөд уламжлалт өгөгдлийн сангийн системээс ялгарах гол ялгаа нь төвлөрсөн өгөгдлийн сан болон төвлөрсөн удирдлагын функцийн байхгүйд оршино [2].

Блокчэйн нь DLT технологийн гол төлөөлөгч бөгөөд мэдээллийн гинжин хэлхээ юм. Блокчэйнд тогтсон хэмжээтэй блок үүсгэж, үүн дотроо мэдээллийг хадгалах ба эхний блок дүүрэхэд дараагийн шинэ блок үүсгэдэг. Эдгээр блок нь хэш функцээр кодлогдсон байх ба блокийг цаг хугацааны дагуу жагсааж, блок тус бүр яг өөрийн өмнөх блокийн мэдээллийг өөр дотроо хадгалах байдлаар гинжин бүтцийг үүсгэнэ.

Блокчэйн технологийн хамгийн чухал, онцлох давуу тал нь төвлөрсөн бус тархсан бүтэцтэй бөгөөд сүлжээнд байгаа бүх компьютер блокчэйний халдашгүй чанарыг үргэлж баталгаажуулж байдаг ба хэн нэгэн, эсвэл аль нэг компани үүн доторх өгөгдөл түүний бүрэн бүтэн байдлыг удирдах боломжгүй байдагт байгаа юм. Блокчэйний бүх зангилаа ижил мэдээллийг агуулж байдаг болохоор “A” зангилаан дахь өгөгдөл эвдэрч гэмтвэл блокчэйний хэсэг болж чадахгүй, учир нь өгөгдөл нь бусад “B” болон “C” зангилааны өгөгдөлтэй ижил байж чадахгүй болно.



Зураг 1.1: Блокчэйний өгөгдлийн бүтэц

1.1.2 Блокчэйний нууцлалын технологи

Криптограф хэш

Криптограф хэш функц нь оруулсан өгөгдлийн уртаас үл хамааран тогтсон урттай хэш утгуудыг буцаадаг. Оролтын зөвхөн нэг тэмдэгт өөрчлөгдөхөд гаралтын хэш утгууд нь эрс ялгаатай

байна. Энэ шинж чанарыг ашиглан, гүйлгээний өгөгдөл болон бусад бүх өгөгдлийн хувьд засвар ороогүй болохыг баталгаажуулах боломжийг олгодог. Жишээ нь, та Mac-ын командлайнаар дараах командыг оруулбал, SHA-256 hash функцийн утгыг хялбархан олох болно.

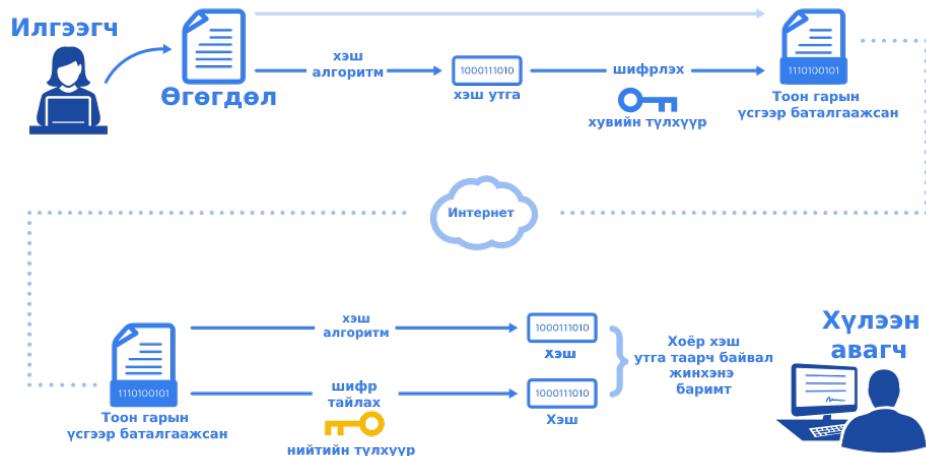
```
> echo "Hello World" | openssl sha256  
SHA2-256(stdin)= d2a84f4b8b650937ec8f73cd8be2c74add5a911ba64df27458ed8229da804a26  
> echo "Hallo World" | openssl sha256  
SHA2-256(stdin)= e6c1396639c0b79bebc94e4448cfe2700b871d45d0d38d98df6ee9da3f09d35c
```

Зураг 1.2: "Hello World", "Hallo World" гэсэн үгнүүдийн хэшийг бодсон байдал

"Hello World", "Hallo World" гэсэн үгнүүдийн sha256 хэшийг бодсон байдал жишээн дээр, "Hello World" гэсэн үний SHA-256 hash утга болон, "е"-г "а"-гээр сольсон үгийн SHA-256 hash утгыг харуулсан байна. Зөвхөн нэг үсгээр ялгаатай боловч, тэдгээрийн hash утгууд нь эрс ялгаатай байна. Энэ мэтчилэн hash функц нь оролт нь 1 байтаар л ялгаатай байхад, эрс өөр үр дүн гаргадаг шинж чанарыг агуулж байдаг. Энэ шинж чанарыг ашиглан, гүйлгээний өгөгдөл болон тэдгээрийг хадгалах блокийн бүх өгөгдлийн хувьд гарах hash утгыг тухайн өгөгдлийн бүтцэд оруулснаар, засвар ороогүй болохыг баталгаажуулах боломжтой болно.

Тоон гарын үсэг

Тоон гарын үсэг нь дижитал мессеж эсвэл баримт бичгийн жинхэнэ эсэхийг шалгах математик аргачлал юм. Энэ нь хос түлхүүр үүсгэх замаар ажилладаг: өргөн тархсан нийтийн түлхүүр, нууцлагдсан хувийн түлхүүр. Гарын үсэг зурахдаа баримт бичгийн өвөрмөц хэшийг үүсгэж, хувийн түлхүүрээр шифрлэж, тоон гарын үсгийг бүрдүүлдэг. Хүлээн авсны дараа хэшийг илгээгчийн нийтийн түлхүүрээр тайлж, хүлээн авсан баримтаас шинэ хэш үүсгэнэ. Хэрэв хоёулаа таарч байвал энэ нь тухайн баримт бичиг нь жинхэнэ бөгөөд ямар нэгэн өөрчлөлт ороогүй гэсэн үг юм.



Зураг 1.3: Цахим гарын үсгийн ажиллах зарчим

Тоон гарын үсэгт хаш функц болон хос түлхүүрийг нийлүүлж ашигласнаар, өгөгдөл илгээгчийг болон агуулгын засагдаагүй гэдгийг баталгаажуулах ажлыг зэрэг гүйцэтгэдэг юм. Блокчэйнд өмнөх хэсгийн хаш функц болон дээр өгүүлсэн цахим гарын үсгийг аль алийг нь ашигладаг бөгөөд гүйлгээ тус бүрийн үнэн зөв байдал, нийцтэй байдлын талаарх мэдээллийн илгээгч, агуулгын бүрэн бүтэн(засагдаагүй) байдлын баталгаа зэрэг төрөл бүрийн зорилгоор ашигладаг.

1.1.3 Ухаалаг гэрээ

Ухаалаг гэрээ гэдэг нь дундын зуучлагч буюу хуульч, нотариатгүйгээр хоёр этгээд гэрээ байгуулсныг баталсан компьютерын код бөгөөд тухайн гэрээний нөхцөл, үүрэг, хариуцлагыг багтаасан байна. Анх этереум нь ухаалаг гэрээг оруулсан блокчэйн гэдгийг гаргаж, түүний дараагаар олон тооны блокчэйнд ухаалаг гэрээг оруулж ирсэн. Ухаалаг гэрээ нь зөвхөн нөхцөл, үүргийг заахаас гадна автоматаар биелэх боломжтой байдаг.

Анх 1996 онд Nick Szabo ухаалаг гэрээний санааг нь гаргаж ирсэн. Гол санаа нь хүнээс хамааралгүйгээр урьдчилан тодорхойлсон ямар нэг нөхцөлийн биелэх үед автоматаар үйлдэл хийгдэнэ.

- Хийгдсэн үйлдэл/гүйлгээ нь олон нийтэд ил байх ч, хэн хийсэн бэ гэдэг нь нууц байж болдог.

2. Блокчэйн сүлжээний бүх зангилаанууд ухаалаг гэрээг ажиллуулдаг.
3. Цаг хугацаа хэмнэхээс гадна гарч болох олон асуудлыг шийдэх боломжтой. (3-дагч этгээдийг оролцоо хэрэггүй)

1.1.4 Блокчэйн зарим хэрэглээ

Олон улсын хэмжээнд стартап компаниуд блокчэйн технологийг ашигласан шинэ системийг эрүүл мэнд, даатгал, татвар зэрэг олон салбарт санал болгож байна.

Жишээлбэл, **Нэгдсэн Үндэстний Байгууллага** 2017 онд блокчэйн технологи ашигласан олон төрлийн санал, санаачилагыг хэрэгжүүлснээс үүний нэг болох тусlamж түгээлтийн бүртгэлийн систем амжилттай хэрэгжсэн байна. НҮБ-аас гаргасан судалгаагаар, нийт тусlamжийн 30 орчим хувь нь очих ёстой хүлээн авагчдаа хүрдэггүй гэж гарсан байна. 2017 оны тавдугаар сараас НҮБ-ын Дэлхийн хүнсний хөтөлбөрт хэрэгжсэн хүрээнд Сирийн дүрвэгчдэд үзүүлж байгаа тусlamжийг этереум блокчэйн ашиглаж түгээжээ. Тодруулбал, Иордан улсын дүрвэгчдийн хуаранд байрлаж байгаа Сири улсын 10500 дүрвэгчид хүнсний бүтээгдэхүүн (1.4 сая ам.доллар) түгээхэд криптовалютад суурилсан ваучер тарааж, уг ваучераа ашиглан хуаранд байрлах дэлгүүрээс хүнсний бүтээгдэхүүн авах боломжийг хангажээ. НҮБ-аас уг төслийг өмнөх тусlamжтай харьцуулахад маш амжилттай хэрэгжсэн гэж үзэж байгаа бөгөөд 2018 оны хоёрдугаар улиралд тусlamжинд хамрагдах хүний тоог 500,000-д хүргэхээр төлөвлөж байна гэж мэдээлж байна.

НҮБ-аас хамгийн сүүлд эхлүүлсэн нэг ажил нь хүүхдийг блокчэйнд бүртгэлжүүлэх систем юм. Хуурамч бичиг баримт үйлдэн хүүхэд хил дамнуулахыг зогсооход хамгийн ээдрээтэй зүйл нь жинхэнэ юм шиг бүрдүүлсэн хуурамч бичиг баримтыг таних ажил байдаг. Хүний наймаа ихээр явагддаг бүс нутагт хүүхдүүдийг шат дараатайгаар албан ёсны бүртгэлтэй болгож, түүнийг нь НҮБ-ын блокчэйн системд хадгална. Энэ төрлийн гэмт хэрэг хамгийн их явагддаг Молдав улсад хэрэгжүүлж эхэлсэн ажээ. НҮБ-ийн судалгаагаар 5-аас доош насны хүүхэд бүртгэлжээгүй байх тохиолдол зарим бүс нутагт их байдаг байна [3].

Швейцарийн Зуг (ZUG) хот нь крипто хот болохоор ажиллаж байгаа бөгөөд ийм уриа

гаргасан бусад хот болох Сан-Франциско, Лондон, Токио, Сингапур, Нью-Йорк, Амстердамаас ялгагдах зүйл нь санхүү болон технологийн гарааны бизнесээ эхэлж буй компаниудад хууль эрх зүйн орчин нь маш тааламжтай юм. Зуг хотын удирдлага крипто хөндий байгуулж, иргэдээ блокчэйнд бүртгэж эхэлсэн ба 2017 оны арваннэгдүгээр сараас иргэддээ зориулж цахим ID авах вебийн үйлчилгээг нээсэн [4] нь этереум блокчэйнд суурилсан ба хэрэглэгч хаанаас ч өөрийн мэдээллийг оруулан цахим ID-гаа авах боломжтой бөгөөд хотын зүгээс уг мэдээллийг зөвхөн шалгаж баталгаажуулах эрхтэй. Энэхүү цахим ID-гаа ашиглаад иргэд зөвхөн хотын үйлчилгээг (хэрэглээний төлбөр, түрээсийн төлбөр) авахаар хязгаарлагдахгүй ба 2018 оны хавар сонгуулийн санал өгөхөд (e-vote) ашиглахаар бэлдэж байна.

1.2 Дижитал эрхийн менежмент (DRM)

Digital Rights Management (DRM) системийг дижитал контентыг хэрэглэх, тараах, хуваалцахад хяналт тавих зорилготой технологиуд гэж ойлгож болно. Энэ нь ном, хөгжим, кино, программ хангамж зэрэг дижитал контентыг хамгаалах, агуулгын эзэмшигч, хэвлэн нийтлэгчдийн оюуны өмчийн эрхийг хамгаалахад чиглэдэг [5].

1.2.1 DRM-ийн үндсэн ойлголт ба бүрэлдэхүүн хэсгүүд:

- Шифрлэлт:** Шифрлэлт нь криптограф алгоритмыг ашиглан цахим контентыг унших боломжгүй формат руу хөрвүүлэх явдал юм. Шифрлэгдсэн контентод зөвхөн шаардлагатай код тайлах түлхүүрийг эзэмсхэн эрх бүхий хэрэглэгчид хандах буюу тайлж болно.
- Хандалтын хяналт:** DRM систем нь дижитал контент руу хэн хандах, үзэх, өөрчлөх, түгээх боломжтойг зохицуулах хандалтын хяналтын механизмыг хэрэгжүүлдэг. Хандалтын эрхийг ихэвчлэн хэрэглэгчийн үүрэг, лиценз эсвэл контент эзэмшигчээс олгосон зөвшөөрөл дээр үндэслэн тодорхойлдог.
- Лицензийн менежмент:** DRM шийдлүүд нь хэрэглэгчдэд дижитал контент руу нэвтрэх, ашиглах зөвшөөрөл олгохын тулд лицензэд суурилсан загваруудыг ашигладаг. Лицензүүд

нь ашиглалтын хугацаа, зөвшөөрөгдсөн төхөөрөмж, нэгэн зэрэг хэрэглэгчдийн тоо зэрэг ашиглалтын нөхцөл, нөхцөлийг тодорхойлдог.

- **Тоон усан тэмдэг:** Тоон усан тэмдэг нь үл үзэгдэх танигч эсвэл гарын үсгийг цахим контентод оруулахад ашигладаг техник юм. Усан тэмдэглэгээг контентын зөвшөөрөлгүй хуулбарыг эх сурвалж руу нь буцаах эсвэл контентын жинхэнэ эсэхийг шалгахад ашиглаж болно.
- **Хуулбарлах хамгаалалт:** DRM системүүд нь цахим контентыг зөвшөөрөлгүй хуулбарлах, хуулбарлахаас сэргийлэхийн тулд хуулбарлах хамгаалалтын механизмыг хэрэгжүүлдэг. Хулгайлах, зөвшөөрөлгүй түгээхээс урьдчилан сэргийлэхийн тулд хуулбарлахаас урьдчилан сэргийлэх, хуулбарлах хяналт, хуулбар илрүүлэх зэрэг арга техникийг ашигладаг.

1.3 DRM систем дэх блокчэйн технологийн боломжууд

Блокчейн технологи нь төвлөрсөн бус, ил тод, өөрчлөх боломжгүй шинж чанартай бөгөөд уламжлалт дижитал эрхийн менежментийн (DRM) системийн тулгардаг олон асуудлыг шийдвэрлэх боломжтой. Үүнд:

1. **Төвлөрсөн бус өмчлөлийн болон гарал үүслийн бүртгэл:** Блокчейн технологи нь дижитал хөрөнгийн өмчлөл болон гарал үүслийг өөрчлөх боломжгүй, төвлөрсөн бус бүртгэлийг хангаж чадна. Ингэснээр зохиогч болон эзэмшигч нар зохих хулээн зөвшөөрөл, нөхөн төлбөрийг авах боломжтой бөгөөд хөрөнгийн өмчлөл болон шилжүүлгийн түүхийг ил тод байдлаар хянах боломжтой болно. Энэ нь уламжлалт DRM системд тулгардаг өмчлөлийн эргэлзээ болон ил тод бус байдлын асуудлыг шийдвэрлэнэ.
2. **Ухаалаг гэрээгээр дамжуулан эрхийн автоматжуулсан менежмент:** Блокчейн дээр суурилсан ухаалаг гэрээнүүд нь дижитал хөрөнгийн хэрэглээ, роялти төлбөр тооцоо болон бусад холбогдох нөхцөлүүдийг автоматаар хэрэгжүүлэх боломжтой. Эдгээр нь өөрөө гүйцэтгэгддэг гэрээнүүд нь зөвхөн ил тод, үнэн зөв байдлыг хангаад зогсохгүй

тохиролцсон нөхцөлүүдийг автоматаар хэрэгжүүлж, оролцогч талуудын итгэлцлийг нэмэгдүүлнэ.

3. **Хэрэглэгчийн хяналт ба эрх мэдэл:** Блокчейн технологид суурилсан дижитал хөрөнгийн менежментийн систем нь хэрэглэгчдэд хөрөнгийн хандах эрхийн зөвшөөрөл, өмчлөх эрхийг шилжүүлэх, дахин зarah зэрэг хяналтыг олгож, шинэ бизнес загваруудыг хэрэгжүүлэх боломжийг олгоно. Энэ нь хэрэглэгчийн эрх мэдэл, хяналтын дутагдлыг шийдвэрлэж, уламжлалт DRM системд тулгардаг асуудлыг арилгана.
4. **Төлбөр тооцоо ба мөнгө олох шинэ загварууд:** Блокчейн нь төлбөр тооцоог хөнгөвчлөх чадвар нь ашиглалтын төлбөр эсвэл захиалгад суурилсан хандалт зэрэг дижитал контентоор мөнгө олох шинэ загваруудыг бий болгож чадна. Энэ нь уламжлалт DRM загвартай харьцуулахад илүү уян хатан, хэрэглэгчдэд ээлтэй сонголтуудыг өгөх боломжтой.

1.4 Технологийн судалгаа

1.4.1 React & Next.js

Declarative

React нь хэрэглэгчийн интерактив интерфейс бүтээхийг хялбарчилдаг. Аппликашны state бүрд зориулсан энгийн бүтэц зохион байгуулахаас гадна, React нь өгөгдөл өөрчлөгдөхөд яг зөв компонентоо өөрчлөн рендер хийдэг. Declarative бүтэц нь кодыг тань debug хийхэд хялбар болгохоос гадна, ажиллагаа нь илүү тодорхой болдог.

Next.js

Netflix, TikTok, Hulu, Twitch, Nike гэсэн орчин үеийн аваргууд ашигладаг энэхүү орчин үеийн фрэймворк нь React технологи дээр үндэслэгдсэн бөгөөд Frontend, Backend хоёр талд хоёуланд нь ажилладаг веб аппуудыг хийх чадвартайгаараа бусдаасаа давуу юм. Next.js-ийн үндсэн дизайн нь клиент болон сервер талын аль алиных давуу талыг ашиглаж чаддаг, ямар нэг

дутагдалгүй веб сайтыг яаж хамгийн хурдан хялбар бүтээх вэ гэдгийг бодож тусгасан байдаг. Next.js нь сервер талд react компонентуудыг рендерлэн энгийн html, css, json файл болгон хувиргах замаар ажилладаг бөгөөд 2020 оноос олон нийтэд танигdsan JAMStack технологи болон статик сайт, автоматаар статик хуудас үүсгэх, CDN deployment, сервергүй функц, тэг тохиргоо, файлын системийн рүүтинг (PHP-ээс санаа авсан), SWR (stale while revalidate), сервер талд рендерлэх зэрэг асар олон орчин үеийн шинэхэн технологиудыг бүгдийг хийж чаддаг анхны бүрэн веб фрэймворк гэж хэлж болно.

1.4.2 Ethereum блокчэйн

Төвлөрсөн бус, блокчэйн дээр суурилсан програмуудыг хангамжийн платформ анх Ethereum-ийг 2013 онд программист Vitalik Buterin бичсэн бөгөөд 2015 онд олон нийтэд анх танилцуулагдсан юм. Ethereum нь бусад койныг бодвол зөвхөн арилжааны бус тус платформыг ашиглан smart contract буюу ухаалаг гэрээ үүсгэх боломжтой. Энэ нь энгийнээр хөгжүүлэгчдэд төвлөрсөн бус хэрэглээний програмуудыг бүтээх, ажиллуулах боломжийг олгодог.

1.4.3 Hardhat

Hardhat нь ухаалаг гэрээг хөгжүүлэх орчин юм. Энэ нь Ethereum ухаалаг гэрээг бичих, туршихаас эхлээд байршуулах, дигитал хийх хүртэлх бүх амьдралын мөчлөгийг хөнгөвчлөх зорилготой юм. Hardhat нь Ethereum Virtual Machine (EVM) дээр бүтээгдсэн бөгөөд Ethereum, Polygon, Avalanche болон бусад EVM-тэй нийцтэй блокчэйнүүдийг дэмждэг.

1.4.4 Wagmi

Wagmi нь блокчэйнтэй ажиллахад шаардлагатай бүх зүйлийг агуулсан React Hook-ийн цуглуулга юм. Wagmi нь крифто түрийвч холбох, мэдээллийг авах, ухаалаг гэрээтэй харилцах гэх мэт үйлдлүүдийг хөнгөвчлөх боломжийг олгодог.

1.4.5 IPFS & Pinata

IPFS буюу Interplanetary File System нь peer-to-peer сүлжээн дэх файлуудыг хадгалах, хуваалцахад зориулагдсан төвлөрсөн бус протокол юм. Үндсэндээ IPFS нь файлуудыг жижиг хэсгүүдэд хувааж, сүлжээний олон зангилаанд хадгалдаг. Энэ нь файлуудыг нэг байршилд хадгалдаггүй, харин сүлжээгээр тарааж байршуулдаг. Pinata нь төвлөрсөн бус бичиг баримт хадгалалтын сүлжээ болох Interplanetary File System (IPFS) дээр бүтээгдсэн үйлчилгээ юм. Pinata нь хөгжүүлэгчид болон хэрэглэгчдэд IPFS сүлжээнд өгөгдөл хадгалах, уншихад хялбар болгодог. Энэ нь IPFS дээр хадгалагдсан файлуудыг байршуулах, удирдах, хандахад зориулсан API болон бусад хэрэгслээр хангаснаар IPFS-тэй харилцах үйл явцыг хялбаршуулдаг.

1.4.6 Lit Protocol

Lit Protocol нь хэрэглэгчдэд өгөгдөл шифрлэх, түүнд хандах хандалтыг хянах боломжийг олгодог төвлөрсөн бус түлхүүр удирдлагын систем юм. Lit Protocol-ийн хандалтын хяналтын систем нь хэрэглэгчид өөрсдийн өгөгдөлд хэн хандаж, ашиглах боломжтойг нарийн хянах боломжийг олгодог. Lit Protocol-г дараах зорилгоор ашиглаж болно.

- Lit сүлжээнд өгөгдлийг шифрлэх түлхүүр үүсгэх, удирдах
- Lit сүлжээнээс өгөгдлийн шифрлэлтийг тайлах түлхүүрийг авах эрхийг нарийвчилсан нөхцөлтэйгөөр тодорхойлох
- Lit сүлжээнээс түлхүүрийг авч өгөгдлийн шифрлэлтийг тайлах

Lit Protocol бол төвлөрсөн бус сүлжээ бөгөөд үйл ажиллагааны хувьд програмчлагдах түлхүүр хэлбэрээр ажилладаг. "threshold криптографи" гэж нэрлэгддэг процессоор Lit нь хувийн түлхүүрийг төвлөрсөн бус болгож, уг түлхүүр нь Lit зангилаанууд дээр тархсан байдлаар хадгалдаг. Lit сүлжээ нь өгөгдөл шифрлэхэд BLS тоон гарын үсэг ашиглан тодорхой нөхцөл хангасан хүмүүст л шифрлэлтийг тайлахыг зөвшөөрдөг таних тэмдэгт (ID) суурилсан шифрлэлтийн схемийг ашигладаг. BLS (Boneh-Lynn-Shacham) тоон гарын үсэг нь нийтийн түлхүүрт суурилсан

криптографийн нэг төрөл бөгөөд өгөгдлийг нууцлах, баталгаажуулахад өргөн ашиглагддаг. Энэ нь тодорхой нөхцөл хангасан хүмүүст л нууцлалыг тайлах эрх олгодог тул зөвхөн зөвшөөрөгдсөн хүмүүс л өгөгдлийг үзэх боломжтой болдог.

Өгөгдөл шифрлэхийн тулд дараах алхмуудыг хийх хэрэгтэй.

1. Крипто хэтэвчний гарын үсгийг авах, өөрөөр хэлбэл хэтэвчийг эзэмшдэг эсэхийг нотлох
2. Хэн таны өгөгдлийн шифрлэлтийг тайлах түлхүүрийг авч чадах талаар хандалтын хяналтын нөхцөлийг тодорхойлох
3. Lit сүлжээнд холбогдож, өгөгдлийг шифрлүүлэх түлхүүр үүсгэн өгөгдлийг шифрлэх

1.5 Ижил төстэй системийн судалгаа

Блокчэйн технологийг ашиглан цахим лицензийн баталгаажуулалт хийж буй хэд хэдэн системүүдийг судаллаа. Эдгээр системүүдийн ихэнх нь төвлөрсөн бус архитектур дээр суурилж, цахим бүтээгдэхүүний лицензийг баталгаажуулах, хянахад чиглэгдсэн байна.

1.5.1 Системүүдийн тайлбар

Audius: Audius нь хөгжим дамжуулах үйлчилгээ бөгөөд Ethereum болон Solana блокчэйнүүдэд суурилсан. Энэ систем нь төвлөрсөн бус байдлыг хангаж, ухаалаг гэрээг ашиглан хөгжмийн бүтээлийг баталгаажуулдаг. Хэрэглэгчид үнэгүй болон төлбөртэй контентуудыг ашиглах боломжтой.

OpenSea: OpenSea нь дижитал бүтээл, NFT (Non-Fungible Token) худалдааны хамгийн том зах зээл бөгөөд Ethereum блокчэйнд суурилсан. Энэ систем нь ухаалаг гэрээг ашиглан дижитал өмчийг худалдах, худалдан авах боломжийг олгодог боловч төвлөрсөн хадгалалттай.

Үзүүлэлтүүд	Audius	OpenSea	Манай систем
Технологи	Ethereum, Solana	Ethereum	Ethereum, IPFS
Ухаалаг гэрээ	Тийм	Тийм	Тийм
Хандалтын хяналт	Тийм	Тийм	Тийм (Lit protocol)
Төвлөрсөн бус хадгалалт	Тийм	Үгүй	Тийм (IPFS)
Лицензийн төрөл	Үнэгүй болон төлбөртэй	Төлбөртэй	Үнэгүй болон төлбөртэй
Ашиглалтын төвөгтэй байдал	Хялбар	Хялбар	Хялбар
Төвлөрсөн бус хадгалалт	Тийм	Үгүй	Тийм

Table 1.1: Системүүдийн харьцуулалт

1.5.2 Манай системийн давуу тал

Манай систем нь Ethereum блокчэйн дээр сууринсан бөгөөд IPFS-ийг ашиглан төвлөрсөн бус хадгалалт хийх боломжтой. Ухаалаг гэрээгээр дамжуулан лицензийн нөхцөл, хандалтын эрхийг тодорхойлох боломжтой. Мөн Lit протоколыг ашиглан хандалтын хяналтын нөхцөлийг хэрэгжүүлэх боломжтой. Энэ нь хэрэглэгчид болон бүтээлийн эзэд хоорондын итгэлцлийг нэмэгдүүлж, цахим бүтээгдэхүүний лицензийг илүү найдвартай, аюулгүй байлгадаг.

2. СИСТЕМИЙН ШИНЖИЛГЭЭ, ЗОХИОМЖ

Системийн шинжилгээ, зохиомж бүлгийн хүрээнд өмнөх бүлгээс олж авсан мэдээллийн дагуу системийн функциональ ба функциональ бус шаардлагыг боловсруулж түүнээс системийн статик болон динамик загварыг боловсруулан системийн ерөнхий архитектурыг гаргасан болно.

2.1 Системийн шаардлага

2.1.1 Функциональ шаардлагуудыг дараах хүснэгтэд тодорхойлов

ФШ 10	Систем нь цахим бүтээл болон лицензийн талаарх мэдээллийн найдвартай байдлыг хадгалахын тулд блокчэйнтэй харилцах ёстай.
ФШ 20	Системд хэрэглэгчид крипто хэтэвчээ ашиглан өөрийгөө баталгаажуулах боломжтой байх ёстай (жишээ нь, MetaMask).
ФШ 30	Системд зөвхөн холбогдсон түрийвчтэй, баталгаажуулсан хэрэглэгчид системийн функцэд хандах эрхтэй байх ёстай.
ФШ 40	Систем нь хэрэглэгчдэд янз бүрийн төрлийн цахим бүтээлийг (жишээ нь, видео, аудио, PDF, зураг) аюулгүйгээр байршуулах боломжтой байх ёстай.
ФШ 50	Систем нь цахим бүтээлийг байршуулахдаа бүтээлийн мэдээллийг бүртгэх мөн үнийг тогтоох боломжтой байх ёстай.
ФШ 60	Систем нь өгөгдлийн нууцлал, аюулгүй байдлыг хангах үүднээс байршуулахаас өмнө файлуудыг шифрлэн IPFS (InterPlanetary File System) дээр найдвартай хадгалах ёстай.
ФШ 70	Систем нь шифрлэгдсэн файлуудыг зохих зөвшөөрөлтэй эрх бүхий хэрэглэгчдэд зориулан тайлах ёстай.

ФШ 80	Системд хэрэглэгчдэд цахим бүтээлийн үнэд тохирсон шаардлагатай төлбөрийг төлж эзэмшигчдээс тухайн цахим бүтээлд хандах лиценз буюу хандах зөвшөөрөл авах хүсэлт илгээх боломжтой байх ёстай.
ФШ 90	Системд цахим бүтээл эзэмшигчид лицензийн хүсэлтийг зөвшөөрөх эсвэл татгалзах боломжтой байх ёстай. Зөвшөөрөгдсөн үед худалдан авагчид бүтээлийн лицензийг өгөх мөн зохих төлбөрийг эзэмшигчид шилжүүлэх ёстай.
ФШ 100	Системд цахим бүтээл эзэмшигчид мөн хэрэглэгчдийн лицензийн хүсэлтээс татгалзах сонголттой байх ёстай. Ийм тохиолдолд төлбөрийг хэрэглэгчдэд буцааж өгөх ёстай.
ФШ 110	Систем нь цахим бүтээл эзэмших, түүнд лиценз олгох асуудлыг зохицуулахын тулд ухаалаг гэрээг блокчэйн дээр байршуулж, удирдах ёстай.
ФШ 120	Системд хэрэглэгчид хүссэн үедээ системээс цахим бүтээлийн орлогоо өөрийн крипто хэтэвч рүү татах боломжтой байх ёстай.
ФШ 130	Систем нь бүтээл байршуулах, удирдах, өмчлөлийг баталгаажуулахын тулд ухаалаг гэрээтэй харилцах ёстай.
ФШ 140	Хэрэглэгчид систем дээр байршуулсан цахим бүтээлийн дэлгэрэнгүй мэдээллийг үзэх боломжтой байх ёстай.
ФШ 150	Цахим бүтээлийн лиценз авахад лицензэд өвөрмөц дугаар олгож, блокчэйн дээр хадгалах ёстай.
ФШ 160	Систем нь хэрэглэгчид лиценз авсны дараа лицензийн дугаар, файлын мэдээлэл зэрэг лицензийнхээ дэлгэрэнгүй мэдээллийг агуулсан цахим гэрчилгээ олгох ёстай.

Table 2.1: Функциональ шаардлагууд

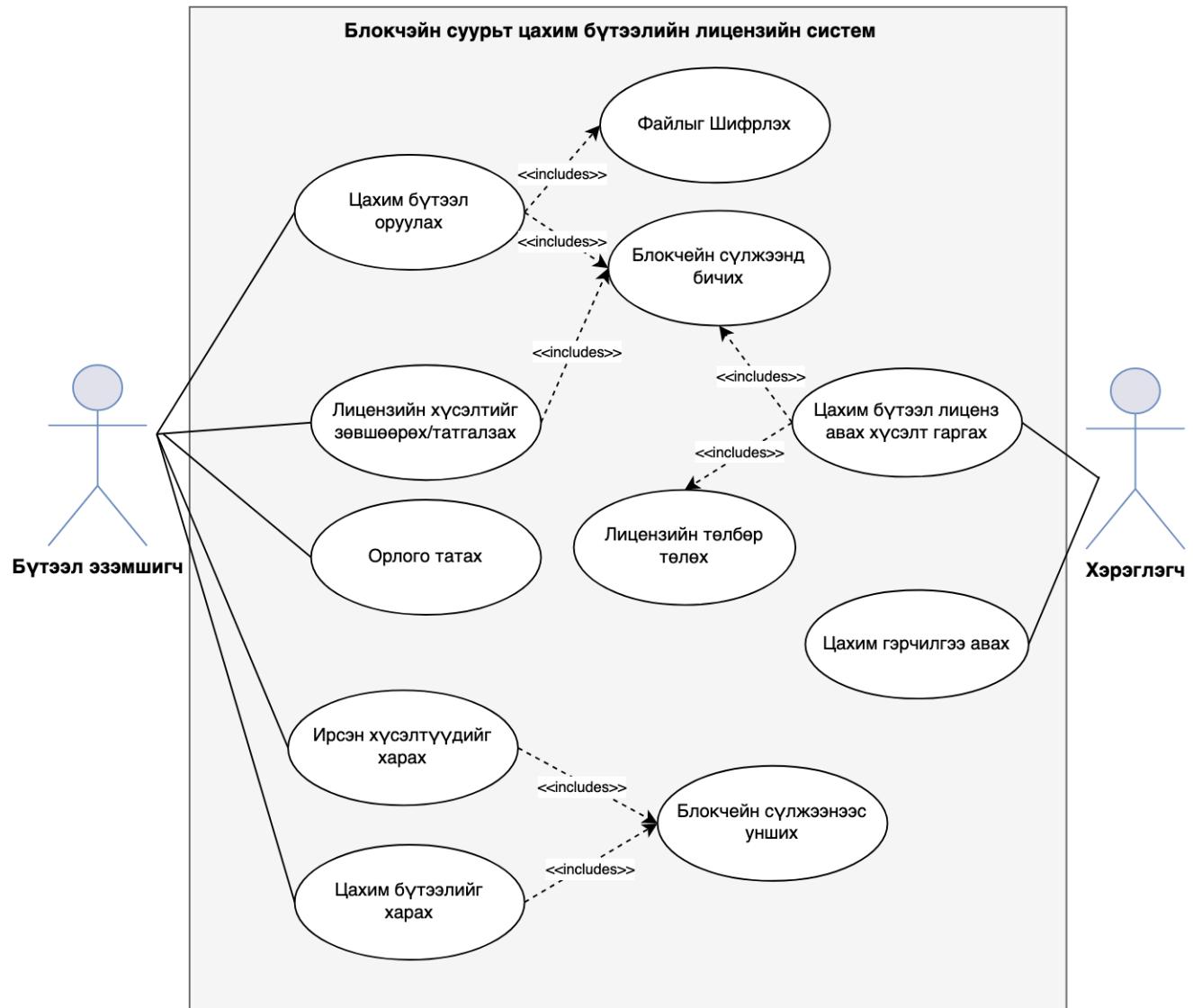
2.1.2 Функциональ бус шаардлагуудыг дараах хүснэгтэд тодорхойлов

ФБШ 10	Блокчэйн технологи нь өгөгдлийн бүрэн бүтэн байдлыг хангаж, лицензийн мэдээллийг зөвшөөрөлгүй өөрчлөхөөс сэргийлнэ.
ФБШ 20	Систем нь гүйцэтгэлийн бууралтгүйгээр олон тооны хэрэглэгчид болон лицензүүдийг зохицуулах чадвартай байх ёстай.
ФБШ 30	Ухаалаг гэрээ нь модульчлагдсан байх ёстай бөгөөд шинэчлэгдэхэд хялбар байх ёстай.
ФБШ 40	Систем нь хүлээн зөвшөөрөгдсөн тодорхой хугацааны дотор баталгаажуулах хүсэлтийг хурдан боловсруулах чадвартай байх ёстай.
ФБШ 50	Систем нь янз бүрийн техникийн чадвартай хэрэглэгчдэд үүнийг үр дүнтэй ашиглах боломжийг олгодог хэрэглэгчдэд ээлтэй интерфейстэй байх ёстай.
ФБШ 50	Систем нь янз бүрийн үйлдлийн систем, хөтөч, төхөөрөмжтэй нийцтэй байх ёстай.
ФБШ 60	Систем нь лиценз олгох, дижитал гүйлгээ, блокчэйн технологитой холбоотой аливаа зохицуулалтын шаардлагад нийцэж байх ёстай.
ФБШ 70	Энэ систем нь гамшгийн үед өгөгдөл алдагдахгүй байхын тулд найдвартай нөөцлөх, сэргээх механизмтай байх ёстай.

Table 2.2: Функциональ бус шаардлагууд

2.2 Системийн ажлын явцын диаграмм

Цахим бүтээлийн ажлын явцыг дараах байдлаар тодорхойлов. Системийн оролцогч талуудыг цахим бүтээлийн лиценз буюу хандах зөвшөөрөл авах гэж буй хэрэглэгч. Нөгөө талаас цахим бүтээл оруулах, түүнд лиценз буюу хандах зөвшөөрөл олгож буй бүтээл эзэмшигч гэж тодорхойлсон.

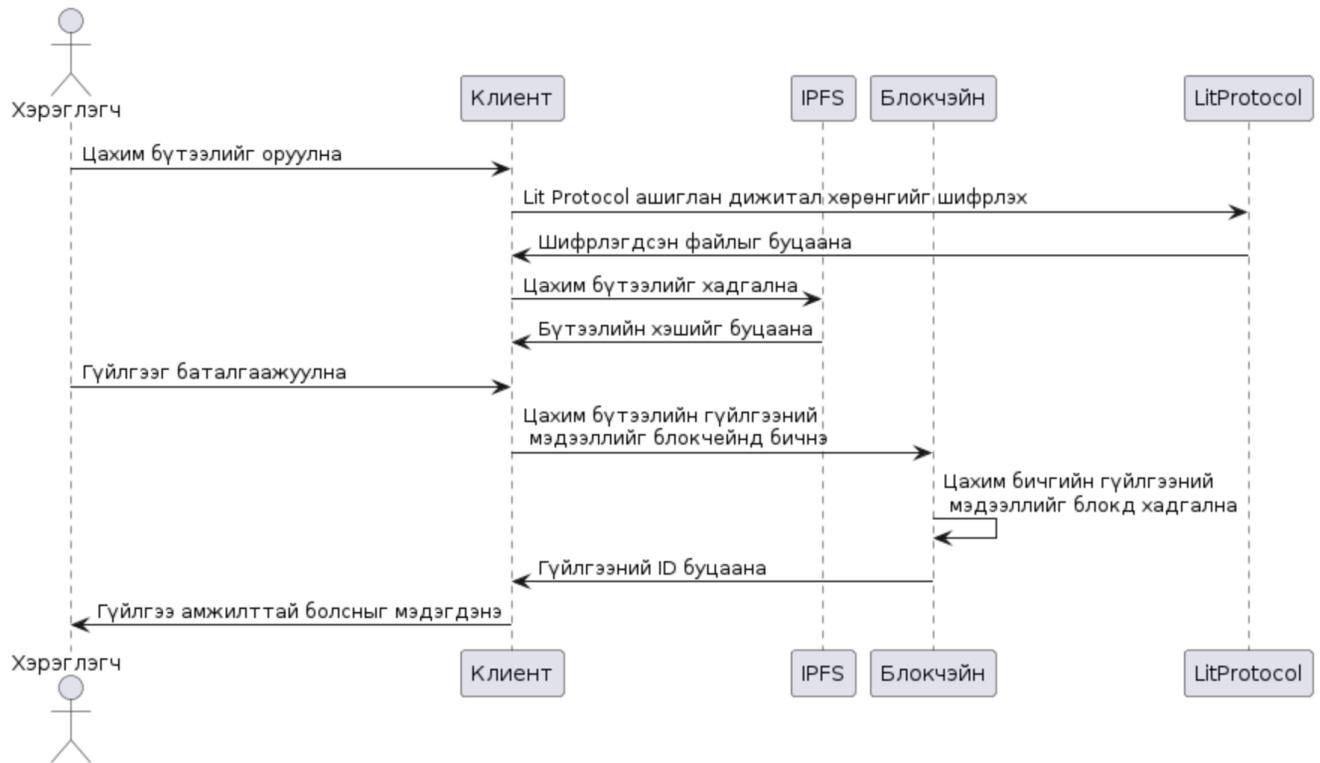


Зураг 2.1: Use-case диаграмм

2.3 Дарааллын диаграмм

2.3.1 Хэрэглэгч цахим бүтээл оруулах дарааллын диаграмм

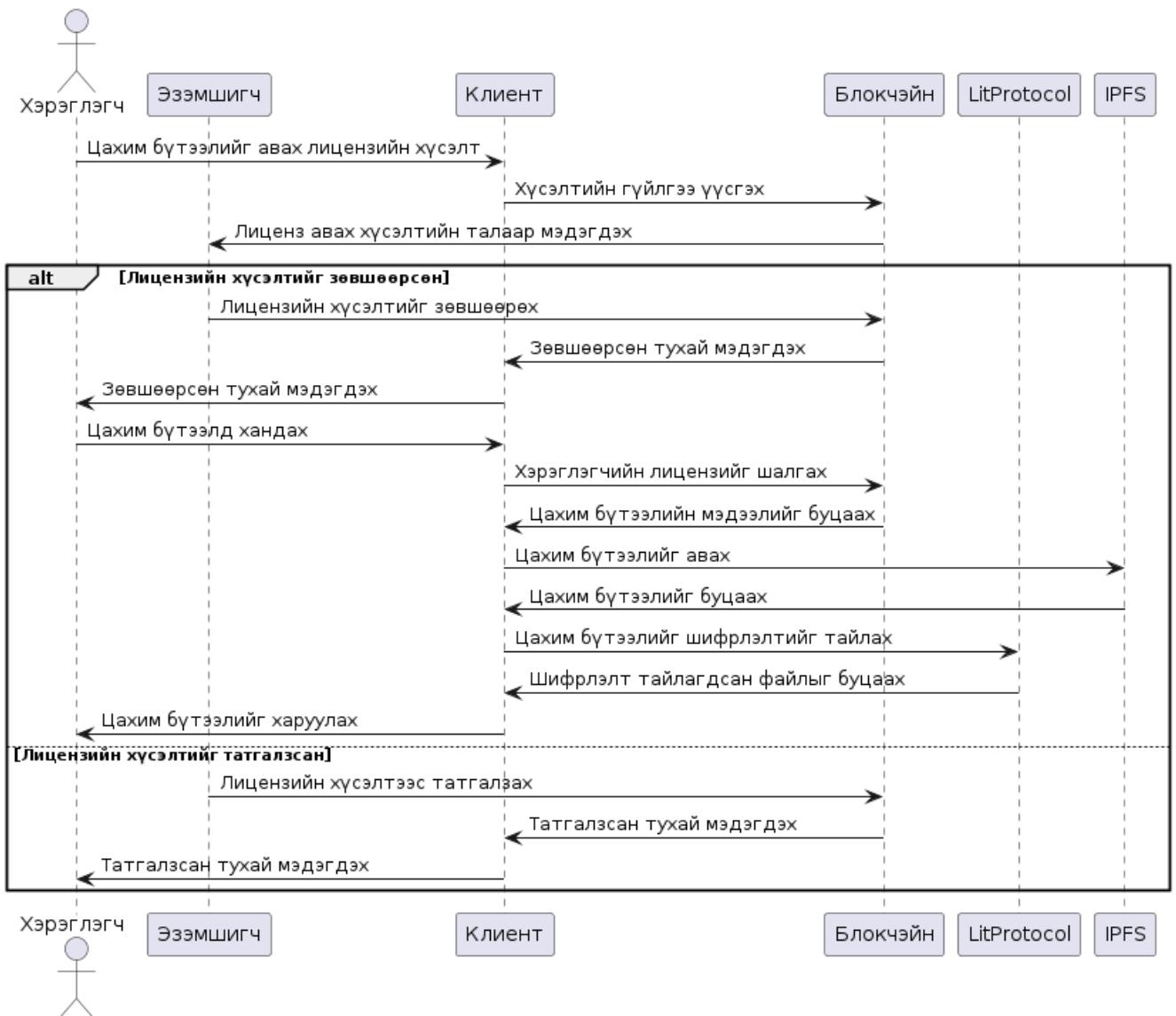
Энэхүү дарааллын диаграмм нь цахим бүтээлийг төвлөрсөн бус системд байршуулах, Lit протокол ашиглан шифрлэх, IPFS сүлжээнд хадгалах, блокчэйн дээр бүртгэх үйл явцыг дүрсэлсэн болно.



Зураг 2.2: Хэрэглэгч цахим бүтээл оруулах дарааллын диаграмм

2.3.2 Хэрэглэгч цахим бүтээлд хандах эрх хүсэх дарааллын диаграмм

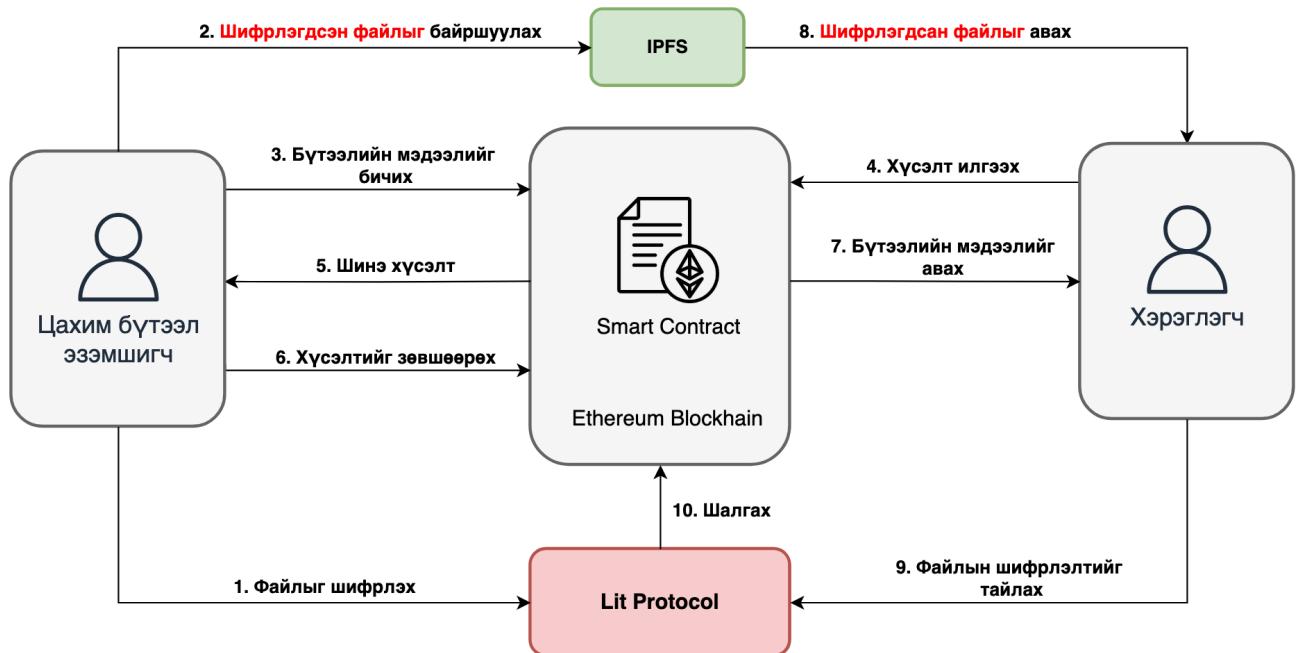
Энэхүү дарааллын диаграмм нь эзэмшигчээс цахим бүтээлийн лиценз авах хүсэлт гаргасан хэрэглэгч, дараа нь хүсэлтийг зөвшөөрөх эсвэл татгалзах үйл явцыг дүрсэлсэн болно.



Зураг 2.3: Хэрэглэгч цахим бүтээлийг хүсэх дарааллын диаграмм

2.4 Архитектур

Энэхүү төслийн фронтэнд хэсэг нь NextJS-н ашигласан тул сервер талын рендер хийж байгаа ба хэрэглэгчийн оруулсан цахим бүтээл болон лицензийн мэдээллийг этереум блокчэйн сүлжээнд байршсан ухаалаг гэрээнд бичих болон унших үйлдлийг хийх юм. Мөн хэрэглэгчийн оруулсан цахим бүтээлийн файлыг IPFS сүлжээнд шифрлэн байршуулж, шифрлэлтийн түлхүүрийг Lit сүлжээнд хадгална. Шифрлэлтийн түлхүүрийг хандалтын хяналтын нөхцөлд тодорхойлсны дагуу ухаалаг гэрээгээр зөвшөөрөлтэй эсэхийг шалган авч файлын шифрлэлтийг тайлна.



Зураг 2.4: Системийн ерөнхий архитектур

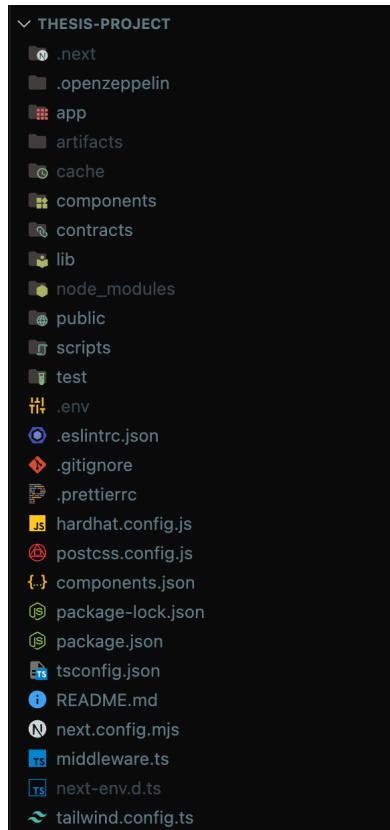
3. СИСТЕМИЙН ХЭРЭГЖҮҮЛЭЛТ

Системийн хэрэгжүүлэлт бүлгийн хүрээнд системийн хөгжүүлэлтийг дээрх бүлэг сэдвүүд дээр тодорхойлсон шинжилгээ ба зохиомжийн дагуу хийлээ.

3.1 Хөгжүүлэлт

3.1.1 Хөгжүүлэлтийн орчныг бэлдэх

Энэхүү судалгааны ажлын практик хэсэгт би NextJS, Hardhat, Pinata IPFS, Lit Protocol, Wagmi, Tailwind CSS зэргийг ашиглан хөгжүүлэлт хийх билээ. NextJS нь монолитик төсөл хийхэд тохиромжтой ба төслийн ухаалаг гэрээн хөгжүүлэлт, клайнт талуудыг нэг repository-д хадгалж байгаа. Version Control System-ээр Github-г сонгосон юм. Кодын фолдер бүтэц нь дараах байдлаар байна.



- **components** - React компонентууд
- **lib** - Хэрэглэгчийн талын шаардлагатай код туслах функцууд
- **app** - NextJS дээрх хуудаснууд
- **public** - Статик зураг, файлууд
- **scripts** - Ухаалаг гэрээний хөгжүүлэлттэй холбоотой файлууд
- **contracts** - Ухаалаг гэрээний файлууд

Зураг 3.1: Хөгжүүлэлтийн орчин

3.1.2 Ухаалаг гэрээн хөгжүүлэлт

Миний төсөл нэг ухаалаг гэрээнээс бүтнэ. Ухаалаг гэрээг Solidity хэл дээр бичсэн бөгөөд Ethereum блокчэйн дээр байршуулсан. Уг ухаалаг гэрээ нь цахим файлууд болон тэдгээртэй холбоотой лицензүүдийг төлөөлдөг Файл, Лиценз ба Хүсэлт гэсэн гурван бүтцийг тодорхойлсон. Файл бүтэц нь id, эзэмшигчийн хаяг, файлаын нэр, дэлгэрэнгүй, ангилал, шифрлэсэн файлаын хэш, файлаын хэмжээ, бүтээлийн үнэ, үүсгэсэн хугацаа зэрэг атрибутуудыг агуулна. Лиценз бүтэц нь лицензийн дугаар, бүтээл эзэмшигчийн хаяг, лиценз эзэмшигчийн хаяг, файлаын нэр, дэлгэрэнгүй, ангилал, шифрлэсэн файлаын хэш, файлаын хэмжээ, лиценз үүсгэсэн хугацаа зэрэг атрибутуудыг агуулна. Мөн дараах функцүүдтэй:

createFile	Цахим бүтээлийн мэдээллийг бичих
getAllPublicFiles	Оруулсан бүх цахим бүтээлийн мэдээллийг авах
getAllUserFiles	Хэрэглэгчийн оруулсан цахим бүтээлийн мэдээллийг авах
getAllUserLicenses	Хэрэглэгчийн эзэмшиж буй цахим бүтээлийн лицензүүдийг авах
getPublicFileById	Цахим бүтээлийн мэдээллийг дугаараар нь авах
requestLicense	Цахим бүтээлийг авах бүтээлийн эзэмшигч рүү лицензийн хүсэлт илгээх
approveLicenseRequest	Өөрийн цахим бүтээлд ирсэн хүсэлтийг зөвшөөрөх
rejectLicenseRequest	Өөрийн цахим бүтээлд ирсэн хүсэлтээс татгалзах
getFileOwnerLicenseRequests	Бүтээлийн эзэмшигчид ирсэн хүсэлтүүдийг авах
isFileOwnedOrLicensed	Цахим бүтээлийн эзэмшигч эсэх эсвэл түүний лицензийг авсан эсэхийг шалгах
generateUniqueLicense	Лицензэд өвөрмөц дугаар бий болгох

Table 3.1: Ухаалга гэрээний функцүүд

3.1.3 Ухаалаг гэрээг этереум блокчэйн сүлжээнд байршуулах

```
1 const { ethers } = require('hardhat');
2
3 async function deployContract() {
4   let contract;
5
6   try {
7     contract = await ethers.deployContract('LicenseMarketplace');
8     await contract.waitForDeployment();
9
10    console.log('Contracts deployed successfully.');
11    return contract;
12  } catch (error) {
13    console.error('Error deploying contracts:', error);
14    throw error;
15  }
16}
17
18 async function main() {
19   let contract;
20
21   try {
22     contract = await deployContract();
23     await saveContractAddress(contract);
24
25     console.log('Contract deployment completed successfully.');
26   } catch (error) {
27     console.error('Unhandled error:', error);
28   }
29}
30
31 main().catch((error) => {
32   console.error('Unhandled error:', error);
33   process.exitCode = 1;
34});
```

Код 3.1: Ухаалаг гэрээг блокчэйнд байршуулах

3.1.4 Lit protocol-н файл шифрлэлт болон хандалтын хяналтын нөхцөл

Lit Protocol-оор дамжуулан блокчэйнд байршуулсан ухаалаг гэрээнд бичсэн isFileOwnerOrLicensed функц хэрэглэгчийн крипто хэтэвчийн хаяг, файлын дугаараар файлыг зөвхөн бүтээл эзэмшигч эсвэл тухайн бүтээлд лиценз буюу хандах зөвшөөрөлтэй хэрэглэгч эсэхийг баталгаажуулан файлын шифрлэлтийг тайлах боломжтойгоор хандалтын хяналтын нөхцөлийг тодорхойлж клиент талд файлыг шифрлэнэ.

Файлыг шифрлэсний дараа Lit сүлжээ нь хандалтын хяналтын нөхцөлд тодорхойлсноор хэн шифрлэлтийг тайлах эсэхийг зөвшөөрнө.

```

1  const client = new LitJsSdk.LitNodeClient({});
2  const chain = "sepolia";
3
4  const createAccessControlCondition = (id: string) => {
5      return [
6          {
7              contractAddress: licenseValidationContract.
8                  contractAddress,
9                  chain: "sepolia",
10                 functionName: "isFileOwnedOrLicensed",
11                 functionParams: [":userAddress", id],
12                 functionAbi: {
13                     inputs: [
14                         {
15                             internalType: "address",
16                             name: "user",
17                             type: "address",
18                         },
19                         {
20                             internalType: "uint256",
21                             name: "fileId",
22                             type: "uint256",
23                         },
24                     ],
25                     name: "isFileOwnedOrLicensed",
26                     outputs: [
27                         {
28                             internalType: "bool",
29                             name: "isOwned",
30                             type: "bool",
31                         },
32                     ],
33                     stateMutability: "view",
34                     type: "function",
35                 },
36                 returnValueTest: {
37                     key: "isOwned",
38                     comparator: "=",
39                     value: "true",
40                 },
41             },
42         ];
43     };
44     class Lit {
45         litNodeClient: any;
46
47         async connect() {
48             await client.connect();
49             this.litNodeClient = client;
50         }
51
52         async encryptFile(id: string, file: any) {
53             if (!this.litNodeClient) await this.connect();
54             const authSig = await LitJsSdk.checkAndSignAuthMessage({
55                 chain: "sepolia",
56                 nonce: this.litNodeClient.getLatestBlockhash() as string
57             });
58         }
59     }
60 }

```

```

58
59     const encryptedZip = await LitJsSdk.
60         encryptFileAndZipWithMetadata({
61             evmContractConditions: createAccessControlCondition(
62                 String(id)),
63             authSig,
64             chain: "sepolia",
65             file: file,
66             litNodeClient: this.litNodeClient,
67             readme: "Encrypted\u2022file",
68         });
69
70     const encryptedBlob = new Blob([encryptedZip], {
71         type: "text/plain",
72     });
73     const encryptedFile = new File([encryptedBlob], file.name);
74
75     return encryptedFile;
76 }
77
78 async decryptFile(file: any) {
79     if (!this.litNodeClient) await this.connect();
80     const authSig = await LitJsSdk.checkAndSignAuthMessage({
81         chain: "sepolia",
82         nonce: this.litNodeClient.getLatestBlockhash() as string
83     });
84
85     const { decryptedFile } = await LitJsSdk.
86         decryptZipFileWithMetadata(
87             {
88                 file: file,
89                 litNodeClient: this.litNodeClient,
90                 authSig: authSig,
91             },
92         );
93
94     return decryptedFile;
95 }
96 const lit = new Lit();
97 export default lit;

```

Код 3.2: Lit protocol-н файл шифрлэлт болон хандалтын хяналтын нөхцөл

3.1.5 Pinata API-ээр дамжуулан файлыг IPFS-д хадгалах

Pinata нь IPFS дээрх үйлдлүүдийг хийх боломжийг олгодог бөгөөд Pinata API-г ашиглан хэрэглэгч контент хадгалах боломжтой болно. Pinata API-г ашиглахын тулд хэрэглэгч Pinata дээр бүртгүүлж, API түлхүүр үүсгэх шаардлагатай.

Pinata API ашиглан файлыг IPFS-д байршуулах функцийг тодорхойлсон. Энэ нь POST

хүсэлтийг файлын өгөгдөл болон шаардлагатай аюулгүй байдлын header мэдээллийн хамт илгээж, серверээс хариу хүлээн авсны дараа өгөгдлийг JSON форматаар буцаана.

```
1 | async function pinFileToIPFS(file: File): Promise<any> {
2 |   const formData = new FormData();
3 |   formData.append('file', file);
4 |
5 |   const res = await fetch('https://api.pinata.cloud/pinning/
6 |     pinFileToIPFS', {
7 |       method: 'POST',
8 |       headers: {
9 |         pinata_api_key: process.env.NEXT_PUBLIC_PINATA_API_KEY!,
10 |         pinata_secret_api_key: process.env.
11 |           NEXT_PUBLIC_PINATA_API_SECRET!,
12 |       },
13 |       body: formData,
14 |     });
15 |   return res.json();
16 }
```

Код 3.3: Файлыг IPFS-д хадгалах

3.1.6 Ухаалаг гэрээнээс өгөгдлийг унших

Хэрэглэгчийн ethereum хэтэвчний хаяг, ухаалаг гэрээний хаяг болон ухаалаг гэрээний ABI (ухаалаг гэрээ ба ухаалаг гэрээнүүдтэй харилцах программуудын хоорондын харилцааг тодорхойлдог интерфейс) авч, Wagmi сангийн ухаалаг гэрээнээс өгөгдөл авахад зориулагдсан useReadContract hook-г ашиглана. Ethereum блокчэйн дээр байрласан ухаалаг гэрээнээс өгөгдөл авах бөгөөд гэрээ нь 'getAllUserFiles' гэсэн нэртэй функцтэй байх ёстой. Энэ функц нь тухайн хэрэглэгчийн эзэмшдэг цахим бүтээлүүдийг буцаана.

```
1 | const { address } = useAccount();
2 | const {
3 |   data: userFiles,
4 |   isLoading,
5 |   error,
6 | } = useReadContract({
7 |   address: licenseValidationContract.contractAddress as `0x${
8 |     string}`,
9 |   abi: licenseValidationAbi.abi,
10 |   functionName: 'getAllUserFiles',
11 |   account: address,
12 | } as { data: UploadedFile[]; isLoading: boolean; error: any };
13 }
```

Код 3.4: Ухаалаг гэрээний өгөгдлийг унших

3.1.7 Ухаалаг гэрээнд цахим бүтээлийн өгөгдлийг бичих

Wagmi-н тодорхойлсон React Hook-г ашиглан цахим бүтээл эзэмшигчийн оруулсан бүтээлийн өгөгдлийг ухаалаг гэрээнд бичнэ. Товчхондоо, файл байршуулж, нууцлал, Ethereum ухаалаг гэрээтэй харилцах үйл ажиллагааг React компонент дотор хийнэ. Энэ нь хэрэглэгч Ethereum түрийвчтэй холбогдсон эсэхийг баталгаажуулж, Lit Protocol ашиглан файлыг шифрлэж, шифрлэгдсэн файлыг IPFS-д байршуулж, ухаалаг гэрээнд өгөгдлийг бичнэ. Уг үйл явцын туршид төлөвлүүдийн мэдээллийг хэрэглэгчдэд шинэчлэн мэдэгдэнэ.

```
1 const { writeContract, isPending, data: hash } = useWriteContract
2   ();
3 const { isLoading, isSuccess, isError } =
4   useWaitForTransactionReceipt({
5     hash,
6   });
7 const { isConnected, address } = useAccount();
8
9 async function onSubmit(data: z.infer<typeof formSchema>) {
10   if (!isConnected) {
11     connect({ connector: injected() });
12   }
13   if (!file) {
14     toast({
15       variant: "destructive",
16       description: "Please select a file to upload.",
17     });
18   return;
19 }
20 setUploading(true);
21
22 try {
23   if (!thumbnail) {
24     if (data.category === "Video") {
25       const fileUrl = URL.createObjectURL(file);
26       const thumbnailVideo = await getThumbnailForVideo(
27         fileUrl,
28         file.name,
29       );
30       setThumbnail(thumbnailVideo as File);
31     }
32   }
33   let thumbnailRes = null;
34
35   if (thumbnail) {
36     thumbnailRes = await pinFileToIPFS(thumbnail);
37   }
38
39   const encryptedFile = await lit.encryptFile(String(fileId),
40     file);
41   const res = await pinFileToIPFS(encryptedFile);
```

```

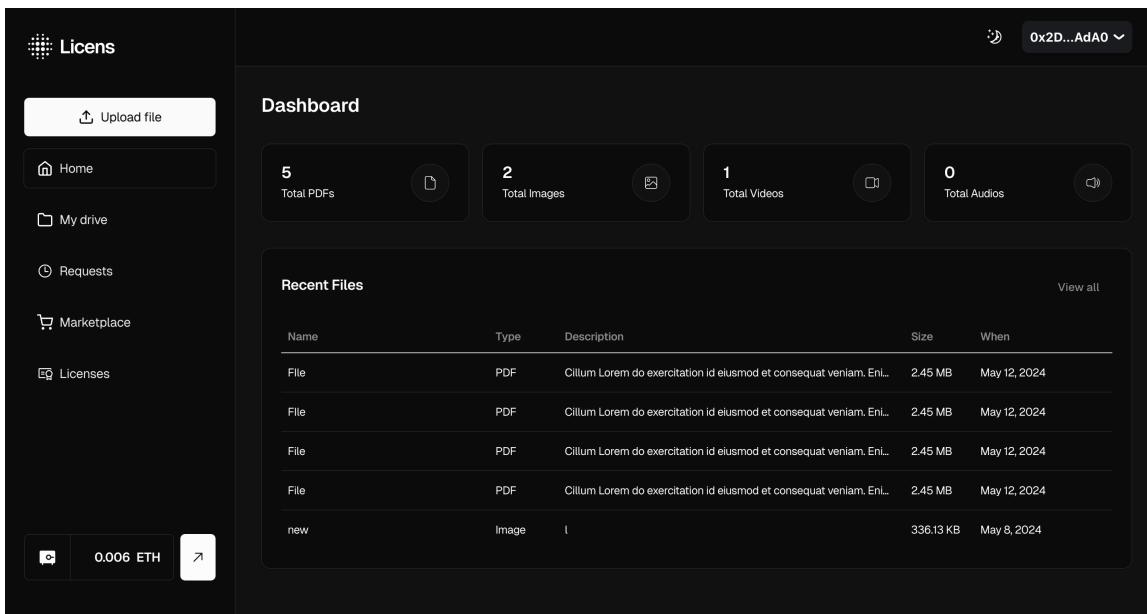
42 |     if (res.isDuplicate) {
43 |         if (fileInputRef.current) {
44 |             fileInputRef.current.value = "";
45 |         }
46 |         toast({
47 |             variant: "destructive",
48 |             description: "This file has already been uploaded.",
49 |         });
50 |     } else {
51 |         writeContract({
52 |             abi: licenseValidationAbi.abi,
53 |             address:
54 |                 licenseValidationContract.contractAddress as `0x${
55 |                     string}`,
56 |             functionName: "createFile",
57 |             args: [
58 |                 data.fileName,
59 |                 data.description,
60 |                 data.category,
61 |                 res.IpfsHash,
62 |                 file.size,
63 |                 thumbnailRes?.IpfsHash || "",
64 |                 parseEther(String(data.price)),
65 |             ],
66 |         });
67 |     }
68 | } catch (error) {
69 |     console.error("Error uploading file:", error);
70 |     toast({
71 |         variant: "destructive",
72 |         description:
73 |             "An error occurred while uploading the file. Please try again.",
74 |     });
75 | } finally {
76 |     setUploading(false);
77 |     refetch();
78 | }

```

Код 3.5: Ухаалаг гэрээний өгөгдлийг унших

3.2 Үр дүн

Хөгжүүлэлтийг дээрх бүлэг сэдвүүд дээр тодорхойлсон шинжилгээ, зохиомжийн дагуу хийсэн болно. Системийн интерфейс дараах байдлаар харагдана.

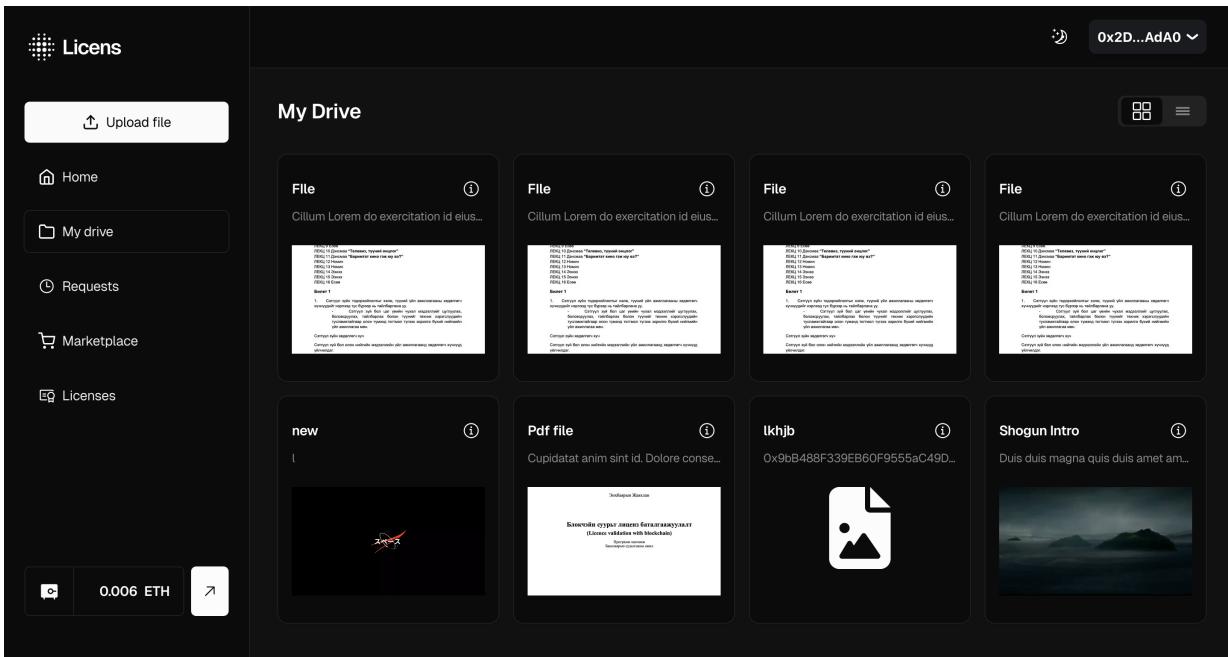


Зураг 3.2: Хэрэглэгчийн үндсэн хуудас

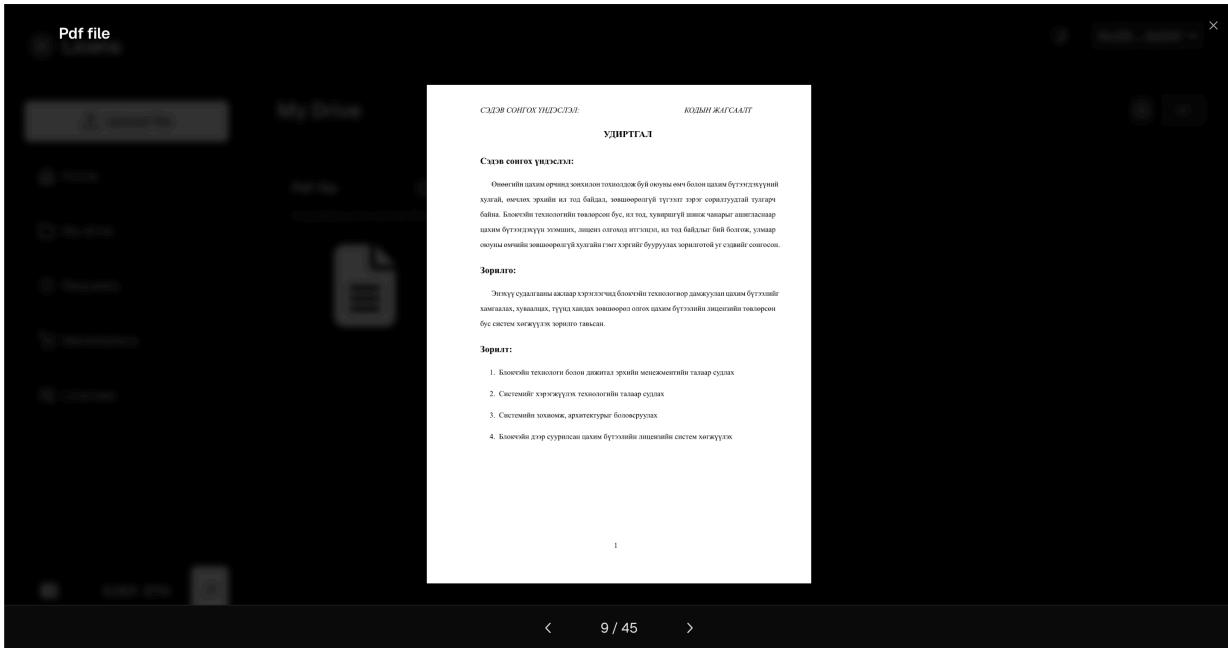
The screenshot shows the Licens application's form for creating a new file listing. The left sidebar is identical to the dashboard. The main form fields include:

- Description: A text input field.
- Price: A text input field containing '0'.
- Thumbnail image: A file selection input field with the placeholder 'Browse... No file selected.'
- Type: A dropdown menu currently set to 'Select'.
- Upload file: A file selection input field with the placeholder 'Browse... No file selected.'
- An 'Upload' button at the bottom right of the form.

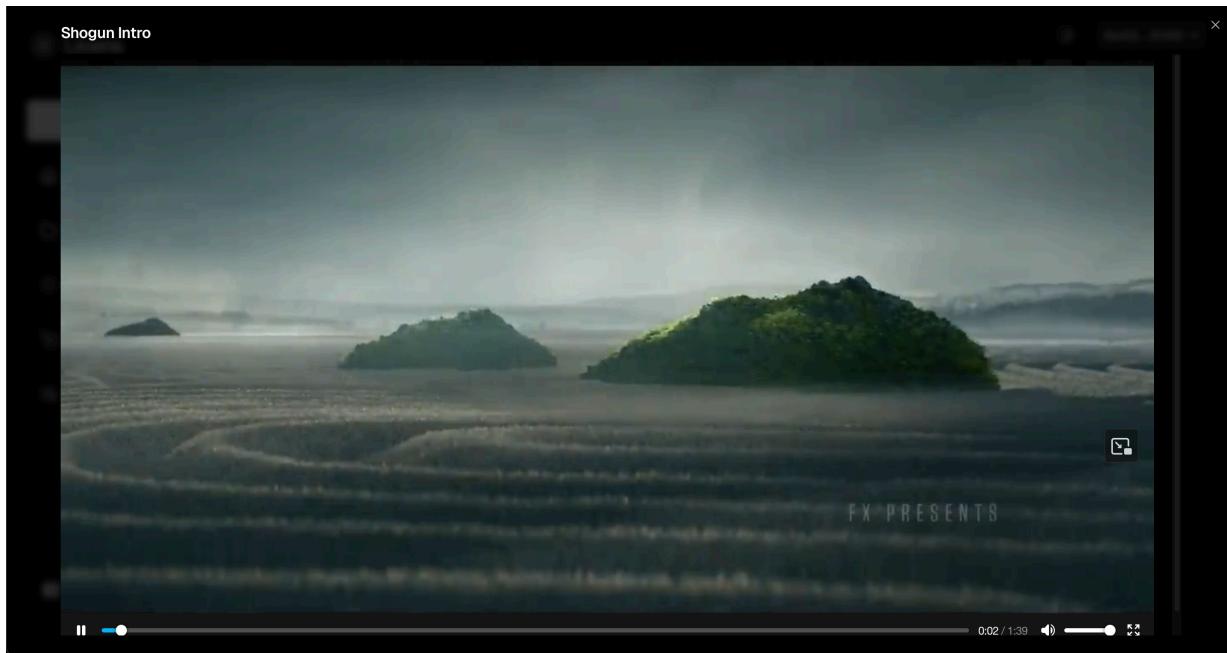
Зураг 3.3: Цахим бүтээл оруулах хуудас



Зураг 3.4: Миний сан хуудас



Зураг 3.5: PDF файл харах



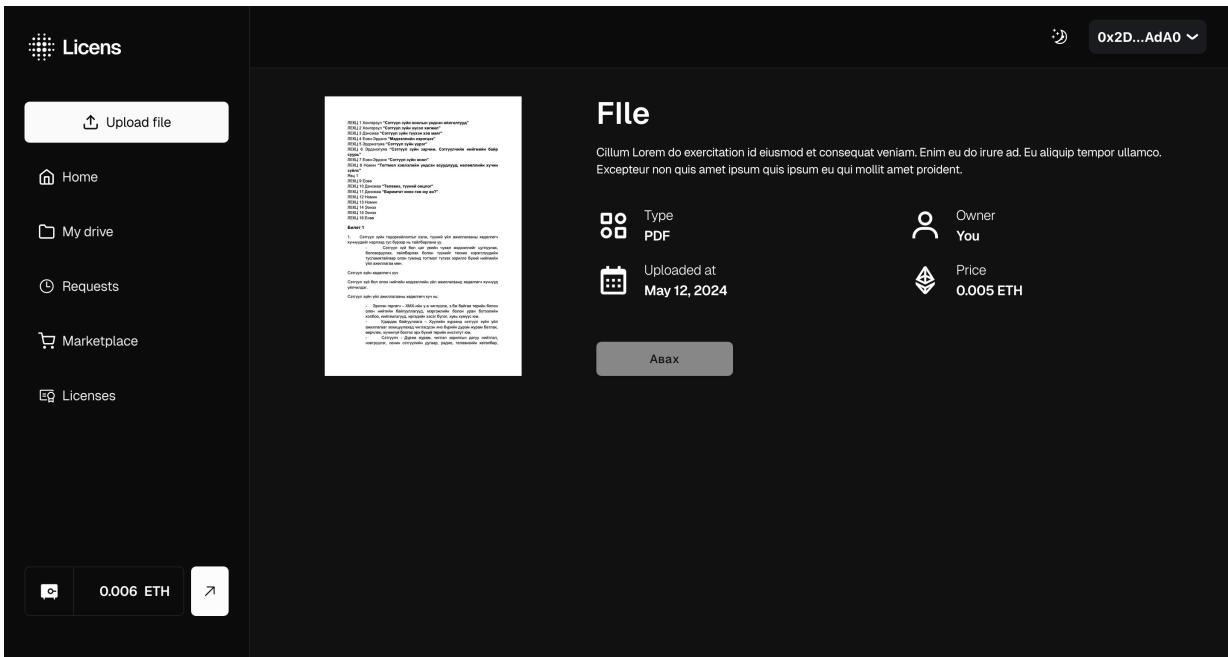
Зураг 3.6: Video файл харах

The screenshot shows the Licens application's marketplace section. On the left sidebar, there are links for Home, My drive, Requests, Marketplace (which is currently selected), and Licenses. The main area has a search bar with the placeholder "Хайх" and a dropdown menu showing "All", "PDF", "Image", "Video", and "Audio". Three file items are listed:

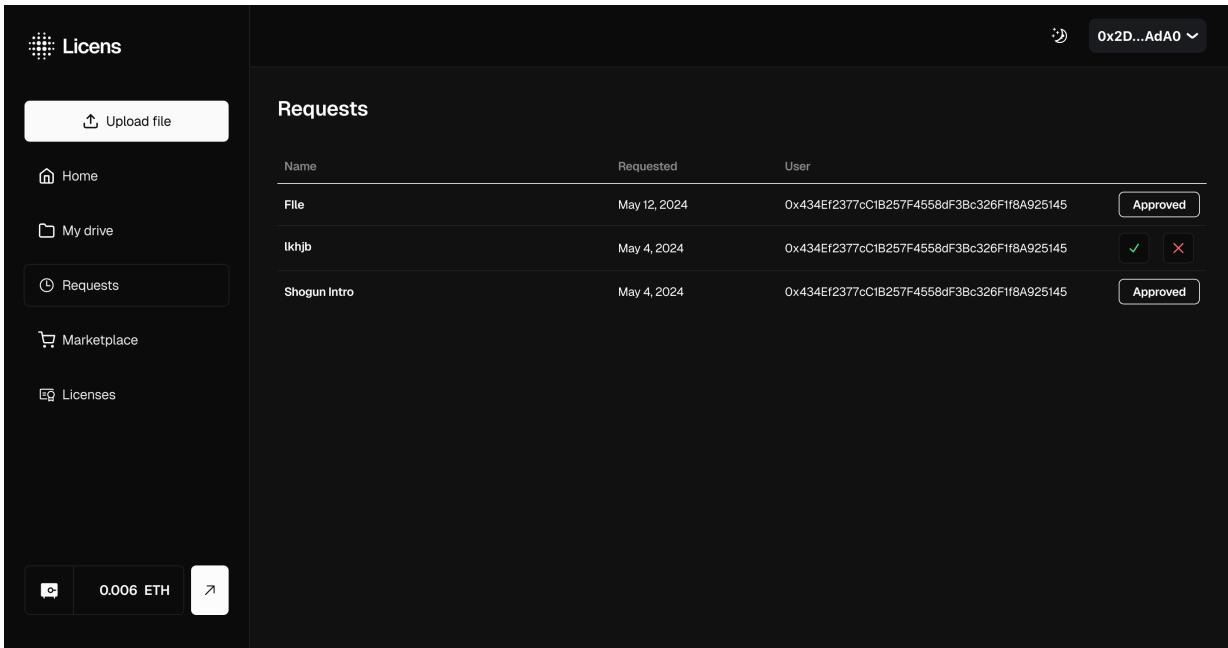
- File**
Owner: 0x434Ef..5145
Price: 0.005 ETH
Cillum Lorem do exercitation id eiusmod et consequat veniam. Enim eu do irure ad. Eu aliquip tempor ullamco. Excepteur non quis amet ipsum qui s ipsum eu qui mollit amet proident.
- File**
Owner: You
Price: 0.005 ETH
Cillum Lorem do exercitation id eiusmod et consequat veniam. Enim eu do irure ad. Eu aliquip tempor ullamco. Excepteur non quis amet ipsum qui s ipsum eu qui mollit amet proident.
- File**
Owner: You
Price: 0.005 ETH
Cillum Lorem do exercitation id eiusmod et consequat veniam. Enim eu do irure ad. Eu aliquip tempor ullamco. Excepteur non quis amet ipsum qui s ipsum eu qui mollit amet proident.

The bottom of the screen shows a summary for the last file: "0.006 ETH" and a download icon.

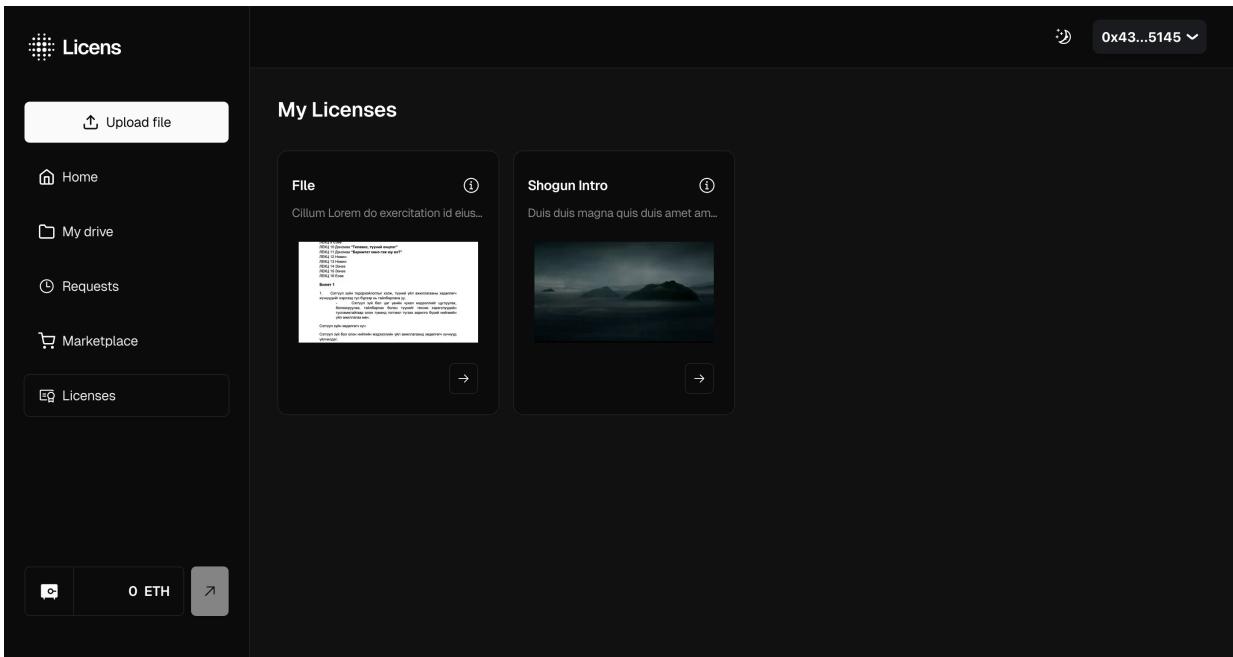
Зураг 3.7: Marketplace хүудас



Зураг 3.8: Marketplace дэх бүтээлийн хуудас



Зураг 3.9: Лиценз хүсэлтийн хуудас



Зураг 3.10: Лицензийн хуудас



Зураг 3.11: Лицензийн гэрчилгээ харах

ДҮГНЭЛТ

Бакалаврын судалгааны ажлын хүрээнд блокчэйн технологи болон дижитал эрхийн менежментийн талаар судалсан. Энэхүү судалж суралцсан мэдлэгээ ашиглан практикт цахим бүтээлийн лицензийн системийг бүтээхээр зорьсон. Уг системийн гол зорилго нь хэрэглэгчид блокчэйн технологиор дамжуулан цахим бүтээлийг хамгаалах, хуваалцах, түүнд хандах зөвшөөрөл олгох төвлөрсөн бус, ил тод систем юм.

Энэхүү системийг эхнээс нь алхам алхмаар шаардлагаас нь хэрэгжүүлэлт хүртэл хийж гүйцэтгэсэн ба системийн функциональ ба функциональ бус шаардлагыг боловсруулж түүнээс системийн статик болон динамик загварыг гаргасан билээ. Үр дүнд нь блокчэйн, ухаалаг гэрээ болон IPFS технологиудыг ашиглан найдвартай, ил тод, төвлөрсөн бус системийг бүтээлээ. Түүнчлэн Lit протоколыг ашиглан файлын нууцлалыг сайжруулсан нь платформын аюулгүй байдал, нууцлалыг улам бэхжүүлсэн.

Гэсэн хэдий ч, судалгааны явцад тулгарсан сорилтууд байсан. Нэг том бэрхшээл нь ухаалаг гэрээ боловсруулах болон системд Lit протоколыг нэгтгэхэд шаардлагатай байсан бөгөөд үүний тулд блокчэйн хөгжүүлэлт, криптографын талаар гүнзгий ойлголт шаардлагатай байв. Түүнчлэн, системийн хэмжээнд аюулгүй байдлыг хангахын зэрэгцээ үр ашиг, хурдыг хадгалахад тогтмол сорилт тулгарч байв.

Цаашид ухаалаг гэрээний функцуудийг оновчтой болгох, гүйлгээний шимтгэлийг буруулах талаар нарийвчилсан судалгаа хийх нь зүйтэй гэж үзэж байна. Түүнчлэн блокчэйний өөр өөр сүлжээ болон шифрлэлтийн аргуудыг судлах нь системийн цар хүрээ, үр ашгийг дээшлүүлэхэд тустай байж болох юм.

Bibliography

- [1] Adam Hayes, Blockchain Facts: What Is It, How It Works, and How It Can Be Used. (December 15, 2023) <https://www.investopedia.com/terms/b/blockchain.asp>
- [2] Scott Nevil, Distributed Ledger Technology (DLT): Definition and How It Works. (May 31, 2023) <https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp>
- [3] Sundararajan S. UN Agencies Turn to Blockchain In Fight Against Child Trafficking. (Nov 13, 2017) <https://www.coindesk.com/markets/2017/11/13/un-agencies-turn-to-blockchain-in-fight-against-child-trafficking/>
- [4] Zug Digital ID: Blockchain Case Study for Government Issued Identity. <https://www.investopedia.com/terms/b/blockchain.asp>
- [5] What is digital rights management (DRM)?. <https://business.adobe.com/blog/basics/digital-rights-management>

A. КОДЫН ХЭРЭГЖҮҮЛЭЛТ

A.1 Ухаалаг гэрээ

```
1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.0;
3
4 contract LicenseMarketplace {
5     address public owner;
6
7     struct File {
8         uint256 id;
9         address fileOwner;
10        string fileName;
11        string description;
12        string category;
13        string fileCid;
14        string imgUrl;
15        uint256 fileSize;
16        uint256 createdAt;
17        uint256 price;
18    }
19
20    struct License {
21        uint256 licenseNumber;
22        uint256 fileId;
23        address fileOwner;
24        address buyer;
25        string fileName;
26        string description;
27        string category;
28        string fileCid;
29        string imgUrl;
30        uint256 fileSize;
31        uint256 createdAt;
32        uint256 price;
33    }
34
35    struct LicenseRequest {
36        uint256 requestId;
37        uint256 fileId;
38        string fileName;
39        address requester;
40        address fileOwner;
41        uint256 requestedAt;
42        bool isApproved;
43        uint256 assetPrice;
44    }
45
46    mapping(address => File[]) private userFiles;
47    mapping (address => License[]) private fileLicenses;
48    mapping (uint256 => LicenseRequest) private licenseRequests;
49
50    mapping(uint256 => bool) public usedLicenses;
51
52    mapping(address => uint256) private userFund;
53    mapping(address => uint256) private userFundWithdrawable;
```

```

55     File[] public publicFiles;
56
57     uint256 public fileId;
58     uint256 public requestId;
59
60     event FileShared(address indexed owner, string fileName);
61     event FileLicense(address indexed owner, address indexed
62         buyer, string fileName);
63     event LicenseRequestCreated(uint256 indexed requestId,
64         uint256 fileId, address requester, address fileOwner);
65     event LicenseRequestApproved(uint256 indexed requestId,
66         uint256 fileId, address requester, address fileOwner);
67     event LicenseRequestRejected(uint256 indexed requestId,
68         uint256 fileId, address requester, address fileOwner);
69
70     modifier onlyOwner(){
71         require(msg.sender == owner, "Only the owner can call this function");
72         -
73     }
74
75     constructor() {
76         owner = msg.sender;
77     }
78
79     function createFile(string memory _fileName, string memory
80         _description, string memory _category, string memory
81         _fileCid, uint256 _fileSize, string memory _imgUrl,
82         uint256 _price) public {
83         fileId++;
84
85         File memory newFile = File({
86             id: fileId,
87             fileOwner: msg.sender,
88             fileName: _fileName,
89             description: _description,
90             category: _category,
91             fileCid: _fileCid,
92             imgUrl: _imgUrl,
93             fileSize: _fileSize,
94             createdAt: block.timestamp,
95             price: _price
96         });
97
98         userFiles[msg.sender].push(newFile);
99         publicFiles.push(newFile);
100
101         emit FileShared(msg.sender, _fileName);
102     }
103
104     function requestLicense(uint256 _fileId, address fileOwner
105         , string memory _fileName, uint256 _assetPrice) public
106         payable {
107         require(!isFileOwnedOrLicensed(msg.sender, _fileId), "
108             User already owns or has a license for this file");
109         require(msg.value == _assetPrice, "Price not met");
110
111         requestId++;
112         LicenseRequest memory newRequest = LicenseRequest({
113             requestId: requestId,
114             fileId: _fileId,

```

```

105     fileName: _fileName,
106     requester: msg.sender,
107     fileOwner: _fileOwner,
108     requestedAt: block.timestamp,
109     isApproved: false,
110     assetPrice: _assetPrice
111   );
112
113   licenseRequests[_requestId] = newRequest;
114   userFund[_fileOwner] += msg.value;
115
116   emit LicenseRequestCreated(_requestId, _fileId, msg.
117     sender, _fileOwner);
118
119
120   function approveLicenseRequest(uint256 _requestId) public {
121     LicenseRequest storage request = licenseRequests[
122       _requestId];
123     require(request.fileOwner == msg.sender, "Only the file owner can approve the request");
124     require(!request.isApproved, "Request already approved");
125
126     request.isApproved = true;
127
128     File memory file = getPublicFileById(request.fileId);
129     uint256 licNum = generateUniqueLicense();
130
131     License memory newLicense = License({
132       licenseNumber: licNum,
133       fileId: file.id,
134       fileOwner: file.fileOwner,
135       buyer: request.requester,
136       fileName: file.fileName,
137       description: file.description,
138       category: file.category,
139       fileCid: file.fileCid,
140       imgUrl: file.imgUrl,
141       fileSize: file.fileSize,
142       createdAt: block.timestamp,
143       price: file.price
144     });
145
146     fileLicenses[request.requester].push(newLicense);
147
148     userFund[msg.sender] -= file.price;
149     userFundDrawable[msg.sender] += file.price;
150
151     emit FileLicense(file.fileOwner, request.requester, file
152       .fileName);
153     emit LicenseRequestApproved(_requestId, request.fileId,
154       request.requester, request.fileOwner);
155
156   function rejectLicenseRequest(uint256 _requestId) public {
157     LicenseRequest storage request = licenseRequests[
158       _requestId];
159     require(request.fileOwner == msg.sender, "Only the file owner can reject the request");

```

```

157     require(!request.isApproved, "Request\u2014already\u2014approved");
158     ,
159     userFundDrawable[request.requester] += request.
160     assetPrice;
161     userFund[msg.sender] -= request.assetPrice;
162
163     delete licenseRequests[_requestId];
164     emit LicenseRequestRejected(_requestId, request.fileId,
165     request.requester, request.fileOwner);
166   }
167
168   function getAllUserFiles() public view returns(File[] memory) {
169     return userFiles[msg.sender];
170   }
171
172   function getAllUserLicenses() public view returns(License[] memory) {
173     return fileLicenses[msg.sender];
174   }
175
176   function getPublicFiles() public view returns (File[] memory)
177   {
178     return publicFiles;
179   }
180
181   function generateUniqueLicense() internal returns (uint256) {
182     uint256 randomNumber = uint256(keccak256(abi.
183     encodePacked(block.timestamp, blockhash(block.number)
184     , msg.sender)));
185     uint256 license = randomNumber % 10000000000;
186
187     while (usedLicenses[license]) {
188       randomNumber = uint256(keccak256(abi.encodePacked(
189         randomNumber, block.timestamp)));
190       license = randomNumber % 10000000000;
191     }
192
193     usedLicenses[license] = true;
194
195     return license;
196   }
197
198   function validateLicense(uint256 licenseNumber) external view
199   returns (bool) {
200     return usedLicenses[licenseNumber];
201   }
202
203   function getPublicFileById(uint256 _id) public view returns (
204     File memory) {
205     for (uint256 i = 0; i < publicFiles.length; i++) {
206       if (publicFiles[i].id == _id) {
207         return publicFiles[i];
208       }
209     }
210     revert("Public\u2014file\u2014not\u2014found");
211   }

```

```

206 |     function getUserLicenseRequests() public view returns (
207 |       LicenseRequest[] memory) {
208 |       uint256 count = 0;
209 |       for (uint256 i = 1; i <= requestId; i++) {
210 |         if (licenseRequests[i].requester == msg.sender) {
211 |             count++;
212 |         }
213 |       }
214 |       LicenseRequest[] memory userRequests = new
215 |         LicenseRequest[](count);
216 |       uint256 index = 0;
217 |       for (uint256 i = 1; i <= requestId; i++) {
218 |         if (licenseRequests[i].requester == msg.sender) {
219 |             userRequests[index] = licenseRequests[i];
220 |             index++;
221 |         }
222 |       }
223 |       return userRequests;
224 |     }
225 |
226 |     function getFileOwnerLicenseRequests() public view returns (
227 |       LicenseRequest[] memory) {
228 |       uint256 count = 0;
229 |       for (uint256 i = 1; i <= requestId; i++) {
230 |         if (licenseRequests[i].fileOwner == msg.sender) {
231 |             count++;
232 |         }
233 |       }
234 |       LicenseRequest[] memory ownerRequests = new
235 |         LicenseRequest[](count);
236 |       uint256 index = 0;
237 |       for (uint256 i = 1; i <= requestId; i++) {
238 |         if (licenseRequests[i].fileOwner == msg.sender) {
239 |             ownerRequests[index] = licenseRequests[i];
240 |             index++;
241 |         }
242 |       }
243 |       return ownerRequests;
244 |     }
245 |
246 |     function isFileOwnedOrLicensed(address _user, uint256 _ fileId)
247 |       public view returns (bool) {
248 |         for (uint256 i = 0; i < userFiles[_user].length; i++) {
249 |           if (userFiles[_user][i].id == _ fileId) {
250 |             return true;
251 |           }
252 |         }
253 |         for (uint256 j = 0; j < fileLicenses[_user].length; j++)
254 |         {
255 |           if (fileLicenses[_user][j].fileId == _ fileId) {
256 |             return true;
257 |           }
258 |         }
259 |       return false;

```

```

260 }
261
262
263     function getFileId() public view returns (uint256) {
264         return fileId + 1;
265     }
266
267     function payTo(address to, uint256 amount) internal {
268         (bool success, ) = payable(to).call{ value: amount }('');
269         require(success, "Transfer\u00d7fund\u00d7failed");
270     }
271
272     function withdrawFund() public {
273         uint256 amountToWithdraw = userFundWithdrawable[msg.
274             sender];
275         require(amountToWithdraw > 0, "No\u00d7funds\u00d7to\u00d7withdraw");
276         userFundWithdrawable[msg.sender] = 0;
277         payTo(msg.sender, amountToWithdraw);
278     }
279
280     function getDrawableFund() public view returns (uint256)
281     {
282         return userFundWithdrawable[msg.sender];
283     }
284
285     function getFund() public view returns (uint256) {
286         return userFund[msg.sender];
287     }

```

Код А.1: Ухаалаг гэрээ