

МОНГОЛ УЛСЫН ШИНЖЛЭХ УХААН ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ

МЭДЭЭЛЭЛ, ХОЛБООНЫ ТЕХНОЛОГИЙН СУРГУУЛЬ



Мөнхбаяр МӨНХБЯМБА

**Блокчэйн технологи ашиглан мэдээлэл
дамжуулах нь**

Using Blockchain Technology to information
transmission

Мэргэжил: Компьютерийн Системийн Хамгаалал

Систем хамгааллын Дипломын ажил

Улаанбаатар хот 2017 он

МОНГОЛ УЛСЫН ШИНЖЛЭХ УХААН ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ
МЭДЭЭЛЭЛ, ХОЛБООНЫ ТЕХНОЛОГИЙН СУРГУУЛЬ

Хамгаалалтанд орохыг зөвшөөрөв.

Мэдээллийн сүлжээ, аюулгүй байдлын салбарын
эрхлэгч дэд доктор (Ph.D), проф Я. Дашдорж

Удирдагч:

Компьютерийн ухааны магистр Г.Дашзэвэг

Зөвлөх:

Компьютерийн ухааны магистр Т.Магсаржав

Компьютерийн ухааны доктор (Ph.D) Б.Мөнхбаяр

Гүйцэтгэсэн:

Компьютерийн систем хамгааллын оюутан М.Мөнхбямба

Дипломын ажлыг электрон байдлаар (*.pdf) хураалгасан болно

.

УШСК-ийн нарийн бичгийн дарга/Магистр Г.Дашзэвэг /

Улаанбаатар 2017 он

Шинжлэх Ухаан, Технологийн Их Сургууль

Мэдээлэл, Холбооны Технологийн Сургууль

Мэдээллийн сүлжээ, аюулгүй байдлын салбар

Шуудангийн хайрцаг-29

Улаанбаатар хот-51

Тел: 70156333

*Мэдээллийн сүлжээ, аюулгүй байдлын салбарын КОМПЬЮТЕРИЙН СИСТЕМ ХАМГААЛАЛ
мэргэжлийн төгсөх курсын оюутан Мөнхбаяр овогтой Мөнхбямбын “Блокчэйн технологи
ашиглан мэдээлэл дамжуулах нь” сэдэвт BSc дипломын шүүмж*

1. Төслөөр дэвшүүлсэн асуудал, үүнтэй холбоотой онолын материал уншиж судалсан байдал. Энэ талаар хүмүүсийн хийсэн судалгаа түүний үр дүнг уншиж тусгасан эсэх (0-6 оноо)

.....
.....
.....
.....
.....

2. Төслийн срөнхий агуулга. Шийдсэн зүйлүүд, хүрсэн үр дүн. Өөрийн санааг гарган, харьцуулалт хийн, дүгнэж байгаа чадвар (0-12 оноо)

.....
.....
.....
.....
.....

3. Эмх цэгцтэй, стандарт хангасан өөрөөр хэлбэл диплом бичих шаардлагуудыг биелүүлсэн эсэх. Төсөлд анзарагдсан алдаанууд, зөв бичгийн болон өгүүлбэр зүйн гэх мэт (хуудас дугаарлагдаагүй, зураг хүснэгтний дугаар болон тайлбар байхгүй, шрифт хольсон, хувилсан зүйл ихээр оруулсан) (0-6 оноо)

.....
.....
.....
.....
.....
.....
.....

4. Төслөөр орхигдуулсан болон дутуу болсон зүйлүүд. Цаашид анхаарах хэрэгтэй зүйлүүд (0-6 оноо)

.....
.....
.....
.....
.....
.....
.....
.....

5. Төслийн талаар онцолж тэмдэглэх зүйлүүд

.....
.....
.....
.....
.....
.....
.....
.....

6. Ерөнхий оноо (0-30 оноо)

.....
.....
.....
.....

Шүүмж бичсэн /...../

Ажлын газар

Хаяг (Утас)

Цаг зав гарган дипломтой бүрэн сайн танилцаж үнэтэй шүүмж гаргасан танд баярлалаа. Сургууль дээр мөрдөж байгаа тарифийн дагуу шүүмжилсний хөлсийг олгох болно.

Мэдээллийн сүлжээ, аюулгүй байдлын салбарын эрхлэгч

..... Доктор (Ph.D), дэд профессор Я.Дашдорж

2018.01.04

ЗОХИОГЧИЙН ЭРХИЙГ ХАМГААЛАХ ХУУДАС

Энэ дипломын төслийн зохиогчийн эрх ШУТИС
зохиогчийн эрхийг хамгаалах заалтын дагуу хамгаалах болно.
Төслийн санаа, агуулга мөн төслийн материалын аль нэг хэсгийг авч ашиглахыг
хориглоно.

МЭДЭГДЭЛ

Энэ төслийг би өөрөө хийсэн ба төслийн аль ч хэсэг өөр ямар нэг их дээд сургууль, коллежид зэрэг хамгаалагдахаар хавсаргагдаагүй, мөн төсөлд өмнө хэвлэгдсэн өгүүллэг, ном сурах бичгээс шууд хуулсан зүйл байхгүйг мэдэгдэж байна.

Мөнхбаяр Мөнхбямба

ТАЛАРХАЛ

Энэхүү дипломын ажлыг хийж гүйцэтгэхэд туслалцаа үзүүлсэн дипломын удирдагч багш Магистр Г.Дашзэвэг багш болон Мэдээллийн сүлжээ Аюулгүй байдлын салбарын багш нарт намайг дэмжсэнд талархал илэрхийлье.

Гарчиг

Зургийн жагсаалт

iii

1 Ерөнхий хэсэг	1
1.1 Удиртгал	1
1.2 Зорилго	2
1.3 Зорилт	2
2 Онол	3
2.1 Блокчэйн технологи	3
2.1.1 Түүх	3
2.1.2 Блокчэйн гэж юу вэ	6
2.1.2.1 Блокчэйн юу хийдэг вэ	7
2.1.2.2 Блокчэйн яагаад хэрэгтэй вэ	8
2.1.2.3 Блокчэйний бүтэц	9
2.1.3 Replicated database	10
2.1.4 Блокчэйнд оролцогчид ба тэдний үүрэг	11
2.1.5 Блокчэйний хөгжлийн үе шат	12
2.1.6 Өнөөгийн блокчэйний хэрэглээ	13
2.1.7 Блокчэйн аппликацийн ирээдүйд	13
2.1.8 Технологи болон хууль, эрх зүй	14
2.1.9 Блокчэйний боломжууд	14
2.2 Төвлөрсөн бус сүлжээ	15
2.2.1 Төвлөрсөн бус сүлжээний архитектур	18
2.2.1.1 Бүтэцлэгдээгүй сүлжээ	18
2.2.1.2 Бүтэцлэгдсэн сүлжээ	19

<i>ГАРЧИГ</i>	<i>ГАРЧИГ</i>
2.2.1.3 Хосолмол загвар	20
2.3 Нууцлал аюулгүй байдал	21
2.3.1 Хаш функц	21
2.3.1.1 Хаш функцийн төрлүүд	22
2.3.1.2 Өөрчлөлтийг илрүүлэх	22
2.3.1.3 Давхцал	22
2.3.1.4 Нэг чиглэлт функц	22
2.3.1.5 Шахалт	23
2.3.1.6 Хаш функц блокчэйнд хэрхэн хэрэглэгддэг вэ	23
2.3.2 RSA алгоритм	23
2.3.3 Цахим гарын үсэг	25
2.4 Тохиролцооны протоколууд	29
2.4.1 PoW(Proof of Work)	29
2.4.2 Эцэслэн шийдэх чанар(finalty)	32
2.4.3 Ухаалаг гэрээ(Smart contract)	34
3 Судалгаа	36
3.1 Блокчэйн хэрхэн ажилладаг вэ	36
3.1.1 Криптограф түлхүүр	37
3.1.2 Тархсан сүлжээ	38
3.1.3 Бичилтийн систем	38
3.1.4 Протокол	39
3.1.5 Блок хэрхэн үүсдэг вэ	41
3.2 Блокийн багтаамж	42
3.2.1 Блок хэмжээний асуудал	43
3.2.2 Давуу тал	44
3.2.3 Сул тал	44
3.3 Блокчэйний хэрэглээ	45
3.3.1 Худалдаа	45
3.3.2 Олон улсын гүйлгээ	45
3.3.3 Даатгал	46
3.3.4 Эмнэлгийн цахим бүртгэл	46

	<i>ГАРЧИГ</i>
3.3.5 Зүйлсийн интернет(Internet of Things)	47
3.4 Bitcoin-ий нийтлэг буруу ойлголтууд	48
3.5 Bitcoin ба залилан	49
3.5.1 Хуурамч сайтууд	49
3.5.2 Эхлээд мөнгөө явуул!	50
3.5.3 Хурдан баяжих арга	50
3.6 Bitcoin олборлолт	51
3.6.1 Cloud олборлолт	52
3.7 Bitcoin цаасан түрийвч үүсгэх	52
3.8 Ethereum	55
3.8.1 Тархсан аппликашн	56
3.8.2 Decentralized autonomous organization (DAO)	56
3.8.3 Блокчэйнийг хакдах нь	58
3.8.4 Smart contract	58
3.8.5 Ether криптовалиут	59
3.9 Etehreum дээр ажиллах	59
3.9.1 Ethereum олборлолт	60
3.9.2 Ethereum түрийвч үүсгэх	60
3.10 DAO	61
3.10.1 Test net	62
3.10.2 Засаглан болон санал хураалт	63
3.10.3 DAO -д хөрөнгө оруулах	63
3.10.4 Системд алдаа олох	64
3.11 Нотариат	64
3.11.1 Гэрээний тухай	65
3.11.2 Итгэмжлэлийн тухай	65
3.11.3 Цахим нотариат	66
3.11.4 Нотариатчийн судалгаа	68
3.11.5 Олон улсын чиг хандлага	69
4 Төслийн хэсэг	70
4.1 Системийн танилцуулга	70

<i>ГАРЧИГ</i>	<i>ГАРЧИГ</i>
4.2 Системийн хамрах хүрээ	70
4.3 Багаж хэрэгсэл	71
4.4 Ажиллагаа	72
5 Дүгнэлт	77
6 Хавсралт	78
Ном зүй	86

Зургийн жагсаалт

2.1	Блокчэйн сүлжээний бүтэц	8
2.2	Peer-to-Peer	15
2.3	Unstructured	19
2.4	Structured p2p	20
2.5	MD5 хаш функ	21
2.6	SHA256	22
2.7	Нийтийн түлхүүртэй алгоритм	26
2.8	Цахим гарын үсэг	28
2.9	Гүйлгээний мэдээллийг зассан үед	31
3.1	Блокчэйн бүтэц	36
3.2	Хэрэглэгчид	37
3.3	Хувийн болон нийтийн түлхүүр	37
3.4	Цахим гарын үсэг	37
3.5	Бичилт	38
3.6	Блок	39
3.7	Протокол	40
3.8	Блокын гинж	40
3.9	Хаш хүснэгт	41
3.10	Блокийн загвар	42
3.11	wallet1	53
3.12	wallet2	54
3.13	wallet3	54
3.14	wallet4	55
3.15	wallet5	55

ЗУРГИЙН ЖАГСААЛТ	ЗУРГИЙН ЖАГСААЛТ
3.16 wallet6	55
3.17 Etheria	57
3.18 code box	62
3.19 Маягт	66
3.20 Шивсэн гэрээний маягт	67
4.1 Нотариат	71
4.2 Системийн өрөнхий ажиллагаа	72
4.3 Ethereum блокчэйны ажиллах зарчим	72
4.4 Гэрээний бүтцийн схем	73
4.5 Системийн үндсэн нүүр	74
4.6 Файлаа хуулах талбар	74
4.7 Батлах файлын мэдээлэл	74
4.8 Шинэ гэрээ үүсгэх	75
4.9 Батлагдсан файлын гэрчилгээ	75
4.10 Гэрчилгээний хаяг	76

БҮЛЭГ 1

Ерөнхий хэсэг

1.1 Удиртгал

Ардчилсан нийгмийг төлөвшүүлэн хөгжүүлэхэд хууль хамгаалах байгууллагуудын эрх зүйн зохицуулалт, үйл ажиллагааг боловсронгуй болгох шаардлага зүй ёсоор тавигдаж байна. Нийгэмд хүний эрх, эрх чөлөөг дээдэлж түүнийг хэрэгжүүлэх эрх зүйн орчныг бүрдүүлэхэд аливаа үйл явдал, бичиг баримт гэрчилж түүнийг хууль ёсны болгох үндсэн үүргийг нотариатч хэрэгжүүлж байна. Нөгөө талаас зах зээлийн эдийн засгийн харилцаанд шилжсэнээр нотариатчаар үйлчлүүлэх үйлчлүүлэгчдийн тоо нэмэгдсээр байгаа. Мөн түүнчлэн мэдээллийн технологийн хурдацтай хөгжлийн нөлөөгөөр бидний амьдралын хэв маяг, хэрэглээ улам бүр цахим тогтолцоонд шилжиж байна. Гэвч монгол улсын нотариатын систем хараахан цахим тогтолцоонд шилжиж амжаагүй байгаа. Тиймээс нотариатын үйл ажиллагааг цахим системд шилжүүлэх зайлшгүй шаардлага гарч байна.

Мэдээлэл технологийн салбарын халуун сэдвийн нэг болох биткойн цахим мөнгөн тэмдэгт, түүний суурь технологи болох блокчэйн нь технологи нь мэдээлэл технологийн салбарт өмнө нь байгаагүй том итгэлцлийг өгч байгаа билээ.

Миний бие энэхүү төгсөлтийн ажлын хүрээнд блокчэйн технологийг ашиглан нотариатын системийг бүтээхийг зорьсон бөгөөд блокчэйн технологийг бусдад таниулан мэдүүлэх, нотариатын үйл ажиллагаа олон нийтэд ил тод байлгах боломжийг олгох явдал юм.

1.2 Зорилго

Энэхүү төслийн ажлын зорилго нь блокчейн технологийн талаар судлан, судалгаан дээрээ үндэслэн мэдээлэл дамжуулах буюу блокчэйн технологид суурилсан нотариатын систем бүтээхэд оршино.

1.3 Зорилт

Дээрх зорилгыг хэрэгжүүлэхийн тулд дараах зорилтуудыг дэвшүүлж байна.

- Блокчейн технологи
- Төвлөрсөн бус сүлжээний загвар
- Криптографийн алгоритмууд
- Блокчейн протоколууд
- Нотариатын баталгаажуулах систем
- Цахим нотариатын систем
- Блокчэйн технологиор мэдээлэл дамжуулж турших
- Нотариатын системийг туршиж ажиллуулах

БҮЛЭГ 2

ОНОЛ

2.1 БЛОКЧЭЙН ТЕХНОЛОГИ

2.1.1 ТҮҮХ

Интернетийн хөгжлийн эхэн үед бид и-мэйл, World Wide Web, dot-com, нийгмийн сүлжээ, хөдөлгөөнт Веб, big data, үүлэн тооцоолол болон зүйлсийн интернет зэрэгтэй танилцсан. Энэ үе нь бидэнд хайлт, хамтран ажиллагаа болон мэдээлэл солилцооны зардлыг багасгахад маш их тус болсон. Түүнчлэн шинэ төрлийн медиа, байгууллагын зохион байгуулалт болон жижиглэн худалдааны шинэ хэв маягийг нэвтрүүлсэн. Мэдрэгч технологийг нэмснээр бидний турийвч, хувцас, тээврийн хэрэгсэл, байшин барилга, хот, түүнчлэн бидний биологид хүртэл ухаалаг системийг ашиглах болсон.

Нэгтгэн дүгнэхэд сүүлийн хориодхон жилд Интернет өөрт хандсан хэрэглэгч, зүйл бүрд эерэг өөрчлөлт авчирсан. Гэвч эдийн засгийн болон бизнесийн орчинд нэлээд хязгаарлагдмал байсаар байна. Петер Штэйнэр(Peter Steiner)-ийн 1993 онд бүтээсэн хүүхэлдэйн кинонд нэг нохой нөгөөдөө "Интернетэд чамайг хэн ч нохой гэдгийг мэдэж чадахгүй" гэж хэлдэг бөгөөд энэ үг өнөөдөр ч утга зүйн хувьд алдаагүй ашиглагдаж болохоор байна. Интернет орчинд бид хэн нэгний нэрийг баталгаатай олж авах боломжгүй, эсвэл банк юм уу засгийн газар гэх мэт баталгаат гуравдагч этгээдгүйгээр хэн нэгэнд итгэн мөнгө шилжүүлэх боломжгүй байна. Тэдгээр дундын баталгаажуулан зуучлагч байгууллагууд бидний мэдээллийг цуглуулан, бидний хувийн мэдээлэлд арилжааны ашиг олох болон үндэсний аюулгүй байдал зэрэгт ашиглахаар халддаг. Технологи хувийн мэдээллийг үнэгүйдүүлэхээсээ илүү ашиг орлого авчирдаггүй. Цахим эрин үед, технологи нь бараг л бүх л сайн болон муу зүйлсийн үндсэн цөм болж

байна. Онлайн харилцаа холбоо болон худалдаа зэрэг нь кибер гэмт хэрэгт шинэ боломжийг нээсэн. Moorын хуулиар өнөө цагт процессорын хүчин чадал тодорхой хугацаанд хоёр дахин өсөх нь мөн гэмт хэрэгтнүүд болон хулгайчдын чадлын мөн хоёр дахин өсгөж байна. Гэмт хэрэгтэн болон хулгайчид гэдэгт спам тараагч, хувийн мэдээлэл хулгайлалгч, phisher, тагнуулч, zombie farmers, хакер, кибер дарамтлагч болон ransomware тараагч зэрэг орно.

1981 оны эхээр зохион бүтээгчид хувийн мэдээлэл, аюулгүй байдал зэрэг Интернет дэх асуудлуудыг криптографын тусламжтай шийдэл гарцыг хайж эхэлсэн. Тэд үйл ажиллагааг яаж ч инженерчилсэн байсан гуравдагч этгээдийн оролцсон мэдээллийн алдагдал үүссээр байсан. Интернетээр кредит карт ашиглан төлбөр тооцоо хийх нь хэрэглэгч хэтэрхий их хувийн мэдээлэл оруулах шаардлагатайгаас шалтгаалан найдвартай бус, мөн гүйлгээний зардал нь бага хэмжээний төлбөр төлөхөд хэтэрхий их байсан.

1993 онд агуу суут математикч Дэвид Чаум(David Chaum) eCash гэх тоон төлбөр тооцооны системийг танилцуулсан. Энэ систем нь тухайн цаг үедээ интернетээр аюулгүй бөгөөд нэрээ нууцлан төлбөр тооцоо хийх боломжтой бараг л тэгс систем болсон. Энэ систем үнэхээр төгс байсан тул Microsoft болон бусад компаниуд eCash - г сонирхож өөрсдийн програмдаа нэвтрүүлсэн. Гэвч асуудал нь тухайн үед интернет худалдан авагчид интернет нууцлал болон аюулгүй байдалдаа төдийлөн анхаардаггүй байсан тул Чаумын герман компани DigiCash 1998 онд дамжуурсан.

Энэ явдлаас 10-аад жилийн дараа буюу 2008 онд дэлхийн эдийн засаг хямралд өртсөн. Харин энэ үед Satoshi Nakamoto гэх хуурамч нэртэй хүн эсвэл бүлэг хүмүүс bitcoin гэж нэрлэгдэх криптовалиут ашиглах peer-to-peer электрон төлбөрийн системийн протокол үүсгэсэн. Криптовалиут (дижитал мөнгө) нь аль нэг улсаас үүсгэгдэж, хянаагддаггүй гэдгээрээ уламжлалт мөнгөн тэмдэгтээс өөр байсан. Энэ протокол нь сая сая төхөөрөмжүүдийн хооронд итгэмжлэгдсэн гуравдагч талын шаардлагагүйгээр өгөгдөл дамжуулах байдлыг хангаж ажиллах тархсан тооцооллын хэлбэрт тогтсон дурмийн багц юм. Энэ технологи компьютер тооцооллын ертөнцөд маш сонирхолтой, мөн айдас дагуулсан эсвэл төсөөллийг бодит болгосон мэтээр бизнес, засгийн газар, нийгмийн хөгжлийн хөдөлгөөнүүд, медиа террорист, сэтгүүлчид зэрэг олон салбарт яг л ойн түймэр мэт хурдацтай тархсан.

Энэ протокол нь блокчэйний тархсан данснуудыг нэмэгдэх гол суурь бөгөөд bitcoin-

2.1. БЛОКЧЭЙН ТЕХНОЛОГИ

БҮЛЭГ 2. ОНОЛ

ий блокчэйн нь хамгийн томд тооцогдож байна. Хэдий технологи нь ойлгоход төвөгтэй боловч үндсэн санаа нь маш энгийн. Блокчэйн нь биднийг бие биедээ шууд бөгөөд аюулгүй мөн банк, кредит картын компани, эсвэл PayPal гэх зэрэг дундын зуучлагчгүй мөнгө дамжуулах боломж олгодог. Энэ технологи нь энгийнээр нээлттэй эхийн програм бөгөөд хэн ч төлбөргүйгээр татаж авч онлайн гүйлгээ хийх шинэ хэрэгсэл хөгжүүлэхэд ашиглаж болох юм.

Анхандаа блокчэйн нь компьютерын шинжлэх ухаанд мэдээллийг хэрхэн зохион байгуулах болон дамжуулах талаарх нэр томьёо төдий байсан. Харин өнөөдөр блокчэйн нь компьютерын хөгжлийн "5 дахь хувьсал" хэмээн өргөмжлөгдж байна.

Анхны криптографын шифрлэлтээр хамгаалагдсан блокуудын служээг 1991 онд Стюарт Хабер(Stuart Haber) В. Скотт Сторнетта(W. Scott Scornetta) нар танилцуулсан. 1992 онд Баер, Хабер, Сторнетта нар блокчэйнд Merkle trees - г холбосноор нэг блокт хэд хэдэн мэдээллийг цуглуулах боломжтой болж ажлын чадамж нь нэмэгдсэн.

Анхны төвлөрсөн бус блокчэйний концепцыг 2008 онд Сатоши Накамото(Satoshi Nakamoto) гаргаж, дараа жил нь цахим мөнгөн тэмдэгт болох bitcoin - ны цөм хэсэгтэй холбож өгснөөр цахим гүйлгээ бурд нийтийн данс(ledger) маягаар ашиглах боломжтой болгосон. Peer-to-peer служээ болон төвлөрсөн бус цаг бүртгэлийн серверүүдээр блокчэйний мэдээллийн сан автоматаар зохицуулагдаж байдаг. Bitcoin - д блокчэйнийг ашигласан нь давхар төлөлт буюу цахим гүйлгээнд нэг тоон токен нэгээс илүү ашиглагдах асуудлыг итгэмжлэгдсэн зохион байгуулагчийн шаардлагагүйгээр шийдсэн анхны тоон мөнгөн тэмдэгт болсон.

Блок болон чэйн гэх үгүүд нь Сатоши Накамото - ийн 2008 оны 10-р сарын анхны эрдэм шинжилгээний нийтлэлд салангид бичигдэн хэрэглэгдсэн байсан бөгөөд олон нийтэд алдаршиж блокчэйн гэх нэг үг болтлоо 2016 оныг хүртэл блок чэйн гэх салангид үг байдлаар ашиглагдаж байсан.

2014 онд "Блокчэйн 2.0" нь төвлөрсөн бус өгөгдлийн сангийн блокчэйн програмуудыг илтгэсэн нэршил болж гарч ирсэн. Блокчэйн 2.0 технологи ашигласнаар цахим гүйлгээнд утга солилцоход мөнгө болон мэдээллийн арбитрын үүрэгтэй зуучлагчийн шаардлагагүй болгосон. Хоёрдугаар үеийн блокчэйн технологи хувь хэрэглэгчдийн цахим тодорхойлолт болон хувийн мэдээллийг хадгалах боломжтой болсон.

2016 онд Оросын холбооны сангийн аюулгүй байдлын төв Nxt Блокчэйн 2.0 платформд суурилсан автомат санал хураалтын системийн хэрэглээг судлах туршилтын

2.1. БЛОКЧЭЙН ТЕХНОЛОГИ

БҮЛЭГ 2. ОНОЛ

төслийг зарласан. Хөгжмийн зах зээлийн төлөөлөл болсон байгууллагууд олноор блокчэйн технологи ашиглан оюуны өмчийн эрхийн шимтгэлийг цуцлуулах, зохиогчийн эрхийг удирдан хянах ажлыг дэлхий нийтээр хэрэгжүүлэх туршилтын загваруудыг туршиаар байна. IMB 2016 оны 7-р сард Сингапур улсад блокчэйний шинэчлэлт болон судалгааны төвөө нээсэн.

2017 оны эхээр Харвард бизнес шүүмж (Harvard Business Review) сэтгүүлд блокчэйн бол өнөөгийн эдийн засгийн болон нийгмийн системд шинэ үндэслэл бий болгох чадамж бүхий суурь технологи юм гэсэн санал илэрхийлсэн нийтлэл бичжээ.

2.1.2 Блокчэйн гэж юу вэ

Блокчэйн гэдэг нь бие даасан хэрэглэгчдийн сүлжээ хооронд цахим мэдээллийн сан үүсгэх болон хуваалцах боломжтой болгох мэдээллийн зохион байгуулалт юм. Блокчэйн нь төвлөрсөн бус өгөгдлийн сангийн технологид шинэ шийдэл болж өгсөн. Энэ шинэчлэлт нь хуучин технологийг шинэ арга замтай холбосноор илүү сайжирч хөгжиж байна. Одоо блокчэйнийг бие даасан хэрэглэгчдийн нэгдэл мэдээллийн санг хадгалж, мэдээллийг хуваалцаж мөн удирдаж ажиллах төвлөрсөн бус өгөгдлийн сан гэж ойлгож болно. Олон төрлийн блокчэйн байдаг:

Нийтийн блокчэйн нь давтагдашгүй токенуудаар ажиллах томоохон төвлөрсөн бус сүлжээ юм. Тэдгээр нь аль түвшний хэрэглэгчдэд нээлттэй ба тэдэнд дэмжлэг үзүүлэх нээлттэй эхийн кодууд байдаг.

Хувийн блокчэйн нь ихэвчлэн жижиг хэмжээний сүлжээ байхаас гадна токен ашигладаггүй. Хэрэглэгчид нь нарийн хяналт дор үйл ажиллагаа явуулдаг. Энэ төрлийн блокчэйнүүд итгэмжлэгдсэн гишүүд болон нууцлагдсан дамжуулалттай холбоогор баталгааждаг.

Зөвшөөрөгдсөн блокчэйн нь нийтийн болон хувийн блокчэйнүүдийн хосолмол шинжтэй, хувийн блокчэйнтэй ижил хяналттай боловч хянах нь сүлжээний хэрэглэгч дотроосоо байдаг. Нийтийн блокчэйнтэй ижлээр томоохон төвлөрсөн бус систем байх ба тэдгээр нь давтагдашгүй токен ашиглана. Код нь зарим нь нээлттэй эхийн, зарим нь нээлттэй эхийн бус байдаг.

Дээрх гурван төрлийн блокчэйнууд гурвуулаа криптограф ашиглан аль ч өгөгдсөн сүлжээнээс хэрэглэгч бүрийг төвлөрсөн хянахчийн шаардлагагүйгээр сүлжээнд хэрэгжиж буй дүрмүүдийг хэрэгжүүлэх, данс бүрийг хянах боломжийг олгодог. Төвлөрсөн

хянаагчийг өгөгдлийн сангийн бүтцээс халсан нь блокчэйн технологийн хамгийн ашигтай бөгөөд чухал шинж болсон юм.

Блокчэйн хэдий гүйлгээний байнгын бичилт болон түүхийг үүсгэж байдаг ч мөнхийн зүйл гэж байдаггүй. Гүйлгээний бичилтийн байнгын ажиллагаа нь сүлжээний тогтвортой байдлаас хамаардаг. Блокчэйний хувьд энэ нь том хэмжээний блокчэйний нэгдлийн гишүүн нэг бүр мэдээлэлд өөрчлөлт орсныг зөвшөөрөх болон зөвшөөрөхгүй байхыг шийдэж байж эцсийн өөрчлөлт хийгдэнэ гэсэн үг юм.

Мэдээлэл блокчэйнд нэгэнт бичигдсэн тохиолдолд үүнийг өөрчлөх эсвэл устгах нь бараг боломжгүй зүйл юм. Хэрэв хэн нэгэн блокчэйнд бичилт хийх буюу өөрөөр хэлбэл гүйлгээ хийх эсвэл дансны харилцаа хийхийг хүсвэл сүлжээн дэх батлах эрхтэй хэрэглэгчид тухайн захиалсан гүйлгээг баталгаажуулна. Үүнд л блокчэйний хамгийн төвөгтэй хэсэг оршдог учир нь блокчэйн бүр хэн хэрхэн ажиллах, хэн гүйлгээг баталгаажуулах зэргээр бие биеэсээ бага зэрэг өөр үүрэгтэй ажилладаг.

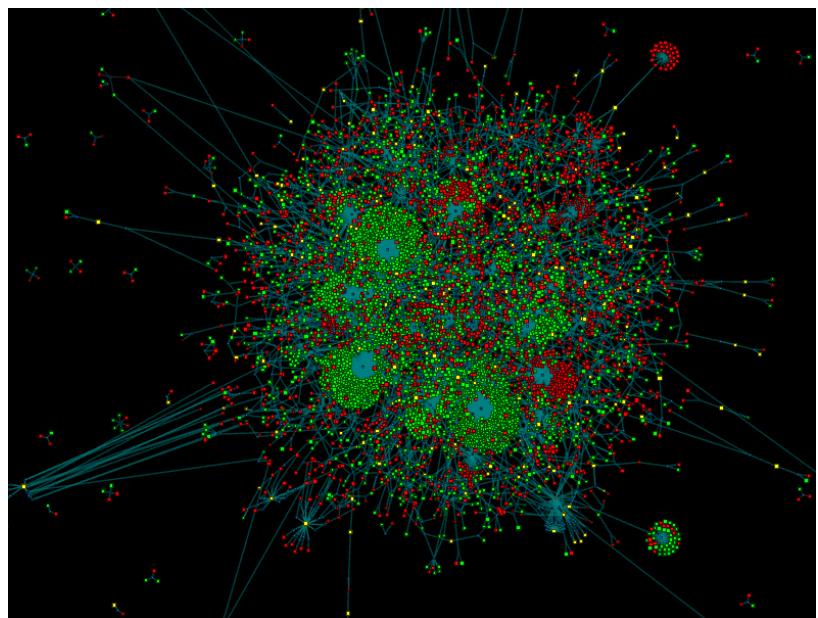
2.1.2.1 Блокчэйн юу хийдэг вэ

Блокчэйн нь ямар нэг мэдээллийн урсгалыг зохицуулагч төвлөрсөн удирдлагагүй peer-to-peer систем юм. Мэдээллийн бүрэн бүтэн, аюулгүй байдлыг хангахын зэрэгцээ төвлөрсөн хяналтыг халах нэг чухал арга нь бие даасан хэрэглэгчид бүхий том хэмжээний төвлөрсөн бус сүлжээтэй байх явдал юм. Ингэснээр тэдгээр компьютерууд тухайн сүлжээг нэгээс олон байршилд байршиулж байна гэсэн үг юм.

Блокчэйн төвлөрсөн бус байдалтай байгаа нь сүлжээний найдвартай байдлыг хангахаас гадна криптовалиутыг ашиглах боломжоор хангах зорилготой. Криптовалиут гэдэг нь дижитал токен бөгөөд зах зээлийн үнэлгээтэй, хувьцааны адилаар мөнгөн дэвсгэртээр арилжаалагддаг.

Криптовалиут нь блокчэйн бүрт бага зэрэг ялгаатай ажилладаг. Ерөнхийдөө техник хангамжуудыг ажиллуулах програм хангамжууд урьдчилан бэлтгэгдсэн байдаг. Тэдгээр програм хангамжууд нь блокчэйний протокол юм. Бидний сайн мэдэх блокчэйн протоколуудад Bitcoin, Ethereum, Ripple, Hyperledger болон Faction зэрэг орно. Зангилаа хэрэглэгчийн техник хангамжийн бүрэлдэхүүн нь сүлжээн дэх мэдээллүүдийг баталгаажуулж байдаг.

Зураг 2.1-д блокчэйн сүлжээний бүтцийг бодит хугацааны хөдөлгөөнт загварыг үзүүлэв. <http://dailyblockchain.github.io>



Зураг 2.1: Блокчэйн сүлжээний бүтэц

2.1.2.2 Блокчэйн яагаад хэрэгтэй вэ

Блокчэйнийг өнөөдөр компьютерын ухаанд "тав дахь хувьсал" буюу интернетэд өмнө нь байгаагүй "итгэлцлийн түвшин" гэж нэрлэж байна. Энэ нь блокчэйн өнөөдөр дэлхий дахинд маш олон хүний анхаарлын төвд байх гол шалтгаан болж байна.

Блокчэйн цахим мэдээлэлд итгэлцэл үүсгэж байна. Мэдээлэл блокчэйнд нэгэнт бичигдсэн тохиолдолд үүнийг устгах эсвэл засварлах нь бараг л боломжгүй зүйл юм. Энэ боломж нь өмнө нь компьютерын сүлжээний орчинд огт байгаагүй зүйл юм.

Мэдээлэл дижитал хэлбэрт тогтвортой бөгөөд найдвартай байх боломжтой болсон тул өмнө нь гүйлгээний ажлыг зөвхөн онлайн бус горимд хийдэг байсан хэрэглэгчид онлайнаар гүйцэтгэхэд найдвартай итгэж болохуйц болсон. Иргэдийн бүртгэл болон өмчлөх эрх зэрэг уламжлалт үйлчилгээнүүд бүгд онлайн горимд хийгдэж баталгаажих боломжтой. Банкны гүйлгээ жишээ нь мөнгө шилжүүлэх, орлого зарцуулалт зэрэг хугацаа их шаарддаг ажлуудыг бараг агшин зуурд хийдэг болсон. Аюулгүй, дижитал гүйлгээний бичилт нь дэлхийн эдийн засгийн хувьд асар их ач холбогдолтой зүйл юм.

Анхны блокчэйн апликэйшнууд өөрийн давтагдашгүй токеноор гүйлгээг баталгаажуулж найдвартай дижитал утгыг гүйлгээгээр дамжуулах нөхцөлөөр хангахаар загварчлагдан бүтээгдэж байсан. Үүнд мөнгө болон хөрөнгийн шилжүүлэлт зэрэг багтдаг. Гэвч блокчэйн сүлжээ нь зөвхөн мөнгөний утгыг дамжуулахаас хол давсан боломжит ирээдүйтэй технологи юм.

2.1.2.3 Блокчэйний бүтэц

Блокчэйн үндсэн гурван цөм хэсгээс бүрддэг :

- **Блок** : Өгөгдсөн хугацаанд гүйлгээний жагсаалт дансанд бичигддэг. Хэмжээ, хугацаа болон блок ажиллах хэмнэл нь блокчэйн бүрд харилцан адилгүй байдаг.

Криптовалиутын шилжүүлгийг баталгаажуулах бичилт хийх нь блокчэйн бүрийн хувьд нэн тэргүүний зорилт нь байдаггүй ч блокчэйн бүр криптовалиут болон токэн дамжих үйлдлийн бичилтийг хийсээр байдаг. Гүйлгээ гэдгийг энгийнээр мэдээллийн бичилтийг хийх гэж ойлгож болно.

- **Чэйн** : Блокуудыг хооронд нь математикийн ухаанаар хооронд нь холбох хаш утга. Энэ нь блокчэйнийг ойлгоход хамгийн төвөгтэй ойлголт. Чэйн нь мөн блокуудыг нэгтэн байлгаж математикаар итгэл үүсгэж байгаа "шидэт цавуу" юм.

Блокчэйндэх хаш нь өмнөх блокт байсан мэдээллээс үүсдэг. Хаш нь тухайн мэдээллийг блоктой заавар болон хугацаагаар холбох хурууны хээ болдог.

Блокчэйн нь хаштай харьцуулахад шинэ нээлт юм. Хаш нь 30аад жилийн өмнө бүтээгдсэн. Энэ эртний технологи шинэ технологитой хоршин ажиллаж байгаа шалтгаан нь хаш нь нэг чиглэлт тайлагдах боломжгүй шифр үүсгэдэг. Хаш функц нь мэдээллийг математикийн алгоритм ашиглан ямар ч хэмжээтэй байсан хамаагүй тогтсон хэмжээтэй бит стрингс хэлбэрт оруулдаг. Бит стрингс нь ихэвчлэн 32 тэмдэгтийн урттайгаар мэдээлэл хашлагдсан гэдгийг илэрхийлэхүйц бичиглэлтэй болсон байдаг. Secure Hash Algorithm (SHA) нь блокчэйнд ашиглагддаг криптографын хаш функцийн нэг юм. SHA-256 хамгийн өргөн ашиглагддаг бараг л дахин давтагдашгүй 256битийн (32байт) -н тогтсон хэмжээт хаш үүсгэдэг. Практик хэрэглээнд хашийг блокчэйнд мэдээллийг байршуулахад ашигладаг дижитал хурууны хээ гэж ойлгож болно.

- **Сүлжээ** : Сүлжээ нь бүрэн зангилаа(Full node)-уудын хэлхээнээс бүрдэнэ. Бүрэн зангилаа гэдгийг сүлжээний эрсдэлийг хариуцах зориулалттай компьютерт ажиллах алгоритм гэж ойлгож болно. Зангилаа бүр тухайн блокчэйнд хийгдэж байсан болон хийгдэж буй бүх гүйлгээний бичилтийг хадгалж байдаг.

Зангилаанууд нь хэн ч байж болох бөгөөд дэлхий даяар тархан байрласан байдаг. Бүрэн зангилааг ажиллуулах нь хундрэлтэй, өртөг өндөртэй мөн цаг хугацаа их шаардсан ажил тул зангилаа болох хэрэглэгчид үүнийг үнэгүй хийдэггүй. Тэд криптовалиут олж авахын тулд зангилааг өөрсдийн компьютер дээрээ ажиллуулдаг. Блокчэйний суурь алгоритм нь зангилаануудад үйлчилгээ үзүүлснийх нь төлөө урамшуулал олгодог. Урамшуулал нь Bitcoin гэх мэт токен болон криптовалиут байдаг.

Bitcoin болон блокчэйн гэх ойлголтуудыг ихэвчлэн биеэр нь орлуулж нэг утгаар ашигладах байдал их гардаг, гэвч энэ хоёр нь тусдаа ойлголт юм. Bitcoin өөрийн блокчэйнтэй. Bitcoin-ий блокчэйн нь bitcoin-ий гүйлгээг найдвартай амжилттай хийгдэх зорилго бүхий суурь алгоритм юм. "Bitcoin"-ын Bitcoin сүлжээнд ажиллаж буй криптовалиутын нэр бол "Блокчэйн"-ын нэг төрлийн програм хангамж юм.

2.1.3 Replicated database

Блокчэйн нь өгөгдлийн сан бүр ижил гүйлгээний утгын жагсаалт хадгалах Replicated database буюу оршуулсан өгөгдлийн сангийн сүлжээ байдлаар ажилладаг. Сүлжээний баталгаажуулагч эсвэл зангилаа гэж нэрлэгддэг сүлжээний гишүүд гүйлгээг нэвтрүүлэх эсвэл зогсоох үйлдлийг хийдэг. Баталгаажуулагч хэрэглэгч бүр тус тусдаа гүйлгээ болон блокийн мэдээллийг шалган нэвтрүүлдэг

Өгөгдлийн санг олшруулна гэдэг нь тухайн нэг компьютер эсвэл сервер дээрх мэдээллийг өөр бусад компьютер эсвэл серверүүдэд хуулбарлаж, тухайн сүлжээний хэрэглэгч бүр ижил хэмжээтэй ижил мэдээлэлтэй болохыг хэлнэ. Ингэж олшруулан тархсан өгөгдлийн сантай болсноор хэрэглэгчид байнга ханддаг чухал мэдээлэлдээ хүрэхийн тулд заавал бусдадаа хандах шаардлагагүй болох юм.

Өгөгдлийн сангийн олшруулалт үндсэн гурван аргаар хийгддэг:

- **Snapshot (шуурхай)олшруулалт** : Серверт шинэ мэдээлэл ороход тухайн мэдээлэл өөр нэг серверт эсвэл өөрт байх өөр өгөгдлийн санд тухай тухайн үедээ хуулагдана

- Merging (нэгдсэн) олшруулалт : Хоёр эсвэл түүнээс олон өгөгдлийн сан нэгдэж нэг өгөгдлийн сан болно
- Transactional (гүйлгээний) олшруулалт : Хэрэглэгч өгөгдлийн сангийн мэдээллийг тэр чигт нь хуулж авах бөгөөд авснаас хойш гарсан өөрчлөлтүүдийг тухайн үед нь шинэчилж авна

Тархсан өгөгдлийн сангийн удирдлагын систем нь мэдээллийн аль ч хэсэгт гарсан өөрчлөлт, нэмэлт болон устгалын үйл явцыг хянаж бусад өгөгдлийн сангудад ижил үйлдлийг хийдэг. Түүнчлэн хэрэглэгч бүр үргэлж бусад хэрэглэгчийн харж байгаа мэдээлэлтэй ижил мэдээллийг харж байдаг.

2.1.4 Блокчэйнд оролцогчид ба тэдний үүрэг

Блокчэйн сүлжээнд олон төрлийн үүрэг, үйл ажиллагаатай оролцогчид байдаг. Тэдгээрийг дэлгэрэнгүй тайлбарлая:

- **Блокчэйн хэрэглэгч :** Блокчэйн сүлжээнд нэвтрэх болон бусад сүлжээний хэрэглэгчидтэй гүйлгээ хийх эрх бүхий оролцогч(ихэвчлэн бизнесийн үйл ажиллагаатай). Блокчэйн технологи ард нь ажиллаж байх бөгөөд хэрэглэгчид технологийн талаар ямар ч ойлголтгүй байж болно. Ихэвчлэн аль нэг байгууллагын сүлжээний ард хэд хэдэн хэрэглэгч байх тохиолдол байдаг.
- **Хянагч (Regulator) :** Блокчэйн сүлжээнд хийгдэж байгаа гүйлгээг хянах тусгай эрх бүхий хэрэглэгч. Хянагчид гүйлгээ хийх эрхгүй байж болно.
- **Блокчэйн хөгжүүлэгч :** Хэрэглэгчдийг блокчэйн сүлжээнд гүйлгээ хийх боломжоор хангах аппликэйшин эсвэл ухаалаг гэрээг хийдэг програмистууд. Аппликэйшин нь хэрэглэгч болон блокчэйн хоёрын дунд үйлчлэх суваг болдог.
- **Блокчэйн сүлжээний оператор :** Блокчэйн сүлжээг тодорхойлох, үүсгэх, зохион байгуулах болон хянах тусгай эрх бүхий хүн. Блокчэйн сүлжээн дэх бизнес бүрт блокчэйн сүлжээний оператор байдаг.
- **Уламжлалт технологийн платформ :** Одоогийн ашиглагдаж байгаа компьютерийн системүүд нь блокчэйн хөгжих технологи болж болно. Тэдгээр системүүд мөн блокчэйнд эрэлт үүсгэх хэрэгцээ болдог.

- **Уламжлалт мэдээллийн эх сурвалж** : Одоо байгаа мэдээллийн систем нь ухаалаг гэрээний үйл явцад нөлөөлөх мэдээллээр хангах ба уламжлалт аппликацийнүүд болон блокчэйний хооронд хэрхэн харилцаа холбоо, мэдээлэл солилцохыг тодорхойлоход тусалдаг.
- **Эрх баталгаажуулагч(Certificate authority)** : Зөвшөөрөгдсөн блокчэйн (Permissioned blockchain) ажиллахад ямар төрлийн certificate шаардлагатайг тодорхойлж түүнийг үүсгэх эрх бүхий хүн. Жишээ нь блокчэйн хэрэглэгчдэд эсвэл бие даасан гүйлгээнд зориулж тус тусын certificate үүсгэж болно.

2.1.5 Блокчэйний хөгжлийн үе шат

Блокчэйн bitcoin үүсэхтэй зэрэгцэн үүсэн хөгжсөн. Энэхүү сүлжээнд хоорондоо хэзээ ч уулзаж байгаагүй бүлэг хүмүүс нэг системд бие биедээ итгэн хамтран ажиллаж болдог гэдгийг нотолсон.

Анхны Bitcoin сүлжээ нь Bitcoin криптовалиутын найдвартай байдлыг хангахаар бүтээгдсэн. Дэлхийгээр төвлөрсөн бус 5000 орчин бүрэн зангилаанаас бүрдэж байсан бөгөөд bitcoin арилжаалах болон утга шилжүүлэхэд гол зорилго нь оршиж байсан ч хэрэглэгчид энэ сүлжээнд үүнээс ч илүү боломж байгааг олж харсан. Сүлжээний далайц болон аюулгүй байдал зэргээс шалтгаалж бусад жижиг блокчэйнүүд болон блокчэйн аппликацийнудыг хамгаалахад ашиглагдах болсон.

Ethereum сүлжээ нь блокчэйн концепцын хоёр дахь хөгжлийн үе юм. Уламжлалт блокчэйн бүтцийг ашиглахаас гадна үүн дотор программын хэл оруулж өгсөн. Bitcoin - той адилаар дэлхийгээр төвлөрсөн бус 5000 орчим бүрэн зангилаанаас бүрдэнэ. Ethereum -ийн үндсэн зорилго нь Ether - г арилжаалах, ухаалаг гэрээ (smart contract) хийх, төвлөрсөн бус автомат байгууллага(DAOs) бүтээх байсан. Bitcoin - ий адилаар жижиг блокчэйнүүд болон блокчэйн аппликацийнүүдийн найдвартай байдлыг хангахад мөн ашиглагддаг.

Factom сүлжээ нь блокчэйн технологийн гурав дахь үе юм. Санал хураалтын систем агуулсан, мөн илүү их хэмжээний мэдээлэл агуулах багахан хэмжээний нэгдмэл сүлжээг ашигладаг. Мэдээлэл болон системийн аюулгүй байдлыг хангах зорилгоор бүтээгдсэн. Нэгдсэн зангилаанууд болон хязгааргүй тооны хянагч зангилаатайгаар ажилладаг. Сүлжээ нь жижиг тул төвлөрсөн бус сүлжээнд холбогдож хадгалагч блокчэйнүүдээ холбон ажилладаг.

2.1.6 Өнөөгийн блокчэйний хэрэглээ

Өнөөдрийн ихэнх амжилттай ажиллаж байгаа блокчэйн аппликэйшнууд нь түргэн шуурхай, хямд өртгөөр мөнгө болон бусад төрлийн утга дамжуулах зориулалттай аппликэйшнууд байна. Үүнд хувьцаат компаниудын хувьцаа арилжаалах, олсон улсын ажилчдадаа цалин өгөх, мөн нэг мөнгөн тэмдэгтийг өөр мөнгөн тэмдэгтээр солих зэрэг багтана.

Блокчэйн мөн програм хангамжийн аюулгүй байдлын багцын хэсэгт ашиглагдаж байна. Америкийн бүс нутгийн аюулгүй байдлын яам (U.S Department of Homeland Security) Зүйлсийн Интернет(Internet of Things) - н аюулгүй байдлыг хангах блокчэйн програмуудыг санхүүжүүлж байсан. Зүйлсийн интернет нь гаднаас чагнах болон бусад төрлийн халдлагад өртөх өндөр магадлалтай байсан тул блокчэйн технологиос хамгийн их боломж хүртсэн салбаруудын нэг болсон юм. Зүйлсийн интернет төхөөрөмжүүд илүү сайжирч, аюулгүй байдал нь үлэмж баталгаажсан. Тэдгээрийн жишээ нь эмнэлгийн систем, өөрийгөө жолоодох машин, болон аюулгүй байдлын системүүд юм.

DAO нь мөн маш сонирхолтой шинэ санаануудын нэг юм. Энэ төрлийн блокчэйн аппликэйшнууд нь компаниудыг онлайнаар нэгтгэн зохицуулах шинэ шийдэл болсон. DAO өмнө нь Ethereum сүлжээгээр зохицуулалт болон хөрөнгө оруулалтаа хийдэг байсан.

2.1.7 Блокчэйн аппликэйшн ирээдүйд

Улсын хэмжээнд газрын бүртгэл хийх, иргэдийн бүртгэл болон олон улсын зорчигч тээврийн аюулгүй байдлыг хангах програмуудын туршилт дээрх томоохон урт хугацааны судалгааны ажлууд хийгдэж байна. Их Британи, Сингапур, Арабын Нэгдсэн Эмират Улс зэрэг орнууд блокчэйнийг зардал бууруулсан шинэ төрлийн эдийн засгийн хэрэгсэл гэдэг талаас нь харж байгаа бөгөөд идэвхтэй хөрөнгө оруулалт болон судалгаа хийсээр байна.

Математик тэгшитгэлээр "итгэлцэл"гэх зүйл үүсгэнээр блокчэйн шаардлагатай салбарууддаа хүрч чадсан. Өмнө нь "итгэлцэл"гэх зүйл нь зарим салбарт ахадсан зүйл байсан бол блокчэйн үүссэнээр энэ нь байх боломжтой зүйл болсон. Түүнчлэн "итгэлцэл"гэх зүйл үгүй болсон газарт дүрэм сахиулах салбарынхны ажлыг хөнгөвчилсөн. Утгат суурилсан болон нийгэмд суурилсан гүйлгээг бид хэрхэн хийж байгаагаас хамаарч блокчэйн өөрчлөгддөг тул блокчэйн аппликэйшны нийгмийн болон эдийн зас-

гийн ойлголт нь сэтгэл хөдлөлийн болон улс төрийн туйлшралд өртөж байна.

2.1.8 Технологи болон хууль, эрх зүй

Блокчэйний хөгжүүлэлт хийх орчин улам төгөлдөржихийн хамт, хийсвэр мөнгө талаасаа, харамсалтай нь мөнгө угаалтанд ашиглагдах, гэмт хэрэгт ашиглагдах зэрэг нь мөн ихэссээр байна. 2016 оны 5 сард Японд хийсвэр мөнгөний тухай хууль батлагдсан.

Уг хууль хэрэгжиж эхлэхээр, хийсвэр мөнгө “Төлбөрийн хэрэгсэл болгон ашиглаж болох хөрөнгө” гэж тодорхойлогдсон бөгөөд (ердийн марк болон кредит карттай адиллаар) хийсвэр мөнгийг хууль ёсны мөнгөн тэмдэгттэй солих үед татвар ногдуулахгүй болох юм.

Мөн уг хуульд, хийсвэр мөнгийг хууль ёсны мөнгөн тэмдэгттэй солих үйл ажиллагааг бүртгүүлсэн хуулийн этгээд явуулах бөгөөд суурь хөрөнгийн талаарх шаардлага болон үйл ажиллагааны явц дахь мэдээллийн хяналт, тогтмол шалгалт зэргийг нарийн дүрмүүдээр зааж өгсөн байна.

2.1.9 Блокчэйний боломжууд

Блокчэйнийг цаашид ямар салбарт хэрэглэгдэхээр харагдаж байгаа талаар танилцуултъя. Эхний хэрэглээний салбар бол, bitcoin гол төлөөлөл нь болж буй криптовалиут юм.

Уламжлалт банк санхүүгийн байгууллагаар дамжуулж гүйлгээ хийх нь төвөгтэй шат дамжлагатай мөн шимтгэл өндөртэй, хугацаа их шаарддаг. Блокчэйн ашигласан хийсвэр мөнгөний хувьд ийм дундын зуучлагч шаардахгүйгээр гүйлгээ хийх боломжтой бас гүйлгээний шимтгэл бага, цаг хугацаа хэмнэдэг. Ялангуяа улс хооронд мөнгө илгээхэд дээрх давуу талуудыг мэдрэх болно. 2015 оны байдлаар, дэлхий даяар илгээж буй мөнгөн дүн ойролцоогоор 60 их наяд иентэй дүйцэхүйц том зах зээл байна.

Дараагийн салбар нь баримт бичгийн баталгаажуулалт (нотариат) юм. Засах боломжгүй гэдэг шинж чанарыг ашиглан, блокчэйн дээр баримт бичиг, эсвэл баримт бичгийн хаш утгыг хадгалснаар, тэрхүү баримт бичиг нэг цаг үед байсан, мөн тухайн үеийн агуулга нь өөрчлөгдөөгүй гэдгийг баталж чадна.

Эстониа улсад, гэрлэлтийн баталгаа, гэрээслэл, газар эзэмшилийн гэрчилгээ зэргийг блокчэйнд хадгалснаар, уламжлалт нотириатыг орлох оролдлого хийж байна. Мөн тус

улсад хувь хүний эмчилгээний түүх үрүү хандах хандалтад блокчэйнд суурилсан технологийг ашиглаж байна.

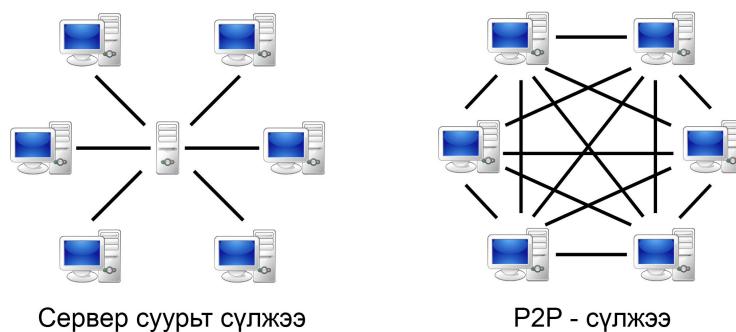
Технологиос гадна, хууль эрх зүйн хүрээнд ч бас өөрчлөлт орж байна. Ялангуяа Fintech-ийн хувьд олон компани хүчээ үзэж байна.

2.2 Төвлөрсөн бус сүлжээ (Decentralized network)

Компьютеруудыг хэрэглэх хандлага зонхилох үед персонал компьютерууд дотоод сүлжээгээр дамжин төв сервертэй холбогддог байсан. Эдгээр серверүүд маш их өгөгдөл боловсруулдаг учир персонал компьютероос хүчин чадлын хувьд маш өндөр байсан. Түүнээс хойш персонал компьютер хүчирхэг болсоор ойр орчмын төв серверүүдээс өгөгдлийг боловсруулахдаа илүү болсон. Яагаад гэвэл PC-ээс PC-рүү эсвэл төвлөрсөн бус тооцоолол нь хувийн компьютерыг төв серверийг тойрч бусад компьютеруудтай шууд хамтран ажиллах боломжийг хангаж чаддаг. Клиент серверийн аль аль нь хүсэлт илгээх эсвэл үйлчилгээ үзүүлэх эсэхээс хамаардаг бол төвлөрсөн бус систем дэх бүх зангилааг зиндаа нэг гэж авч үздэг. Θөрөөр хэлбэл нэг клиент нь нөгөөгөөсөө мэдээлэл авч байхад нөгөө клиент эргүүлээд мэдээлэл тэгш эрхтэйгээр өгч байна гэсэн үг юм.

Зураг 2.2-д Peer to peer сүлжээ болон сервер суурьт сүлжээний топологиудыг үзүүлэв.

Зураг 2.2: Peer to peer сүлжээ болон сервер суурьт сүлжээний топологи



Peer-to-peer (P2P) сүлжээ нь хэрэглэгч зангилаа бүр ижил эрхтэй мөн аль ч зангилаа нь холболтын горим үүсгэх боломжтой төвлөрсөн бус сүлжээний загвар юм. Клиент

нь үйлчилгээний хүсэлт илгээж, сервер нь хүсэлтийг биелүүлэх клиент/сервер загвараас ялгаатай нь P2P сүлжээнд зангилаа бүр клиент болон серверийн хоёр үүргийг давхар гүйцэтгэдэг.

P2P сүлжээний загвар нь клиент/сервер сүлжээний загвараас дараах байдлаар ялгаатай:

- Контентууд болон нөөцүүд хэрэглэгч бүрд ижил хуваагддаг, харин клиент/сервер загварын хувьд зөвхөн төв компьютер дээр байрладаг
- P2P сүлжээ нь сервер суурьт сүлжээтэй харьцуулахад илүү найдвартай, сүлжээний ашиглалт өндөртэй
- P2P сүлжээн дэх компьютерууд ганц сервер компьютероос хамааралгүйгээр өөрсдөдөө байгаа нөөцөө хувааж тархсан тооцооллын боловсруулалтыг хийнэ
- P2P сүлжээний компьютер нь сүлжээн дэх өөр компьютероос хэрэгцээт мэдээллээ ямар нэг серверээр дамжилгүйгээр шууд татаж авах боломжтой

P2P систем нь сүлжээний урсгал, их хэмжээний параллель тооцооллын орчин, тархсан хадгалах төхөөрөмжүүд болон бусад үйл ажиллагаанд нууц чиглүүлэлт үүсгэхэд ашиглагддаг. Ихэнх P2P програмууд аудио, видео мэдээлэл болон бусад бүх төрлийн дижитал форматаар бичигдсэн файл солилицох, харилцаа холбоонд ашиглагдах, мэдээлэл хуваалцахад төвлөрсөн байдаг, гэвч P2P-тэй холбоотой програм хангамжийн нууцлал болон зохиогчийн эрхийн зөрчлүүд их гардаг.

Ерөнхийдөө peer-to-peer програмууд хэрэглэгчдэд үйл ажиллагааны олон параметрүүдийг удирдах боломжоор хангадаг, жишээ нь : тухайн агшинд хэдэн холболтод хандах эсвэл нэвтрүүлэх, хэний системийг холбох эсвэл хязгаарлах, ямар үйлчилгээг санал болгох, мөн сүлжээнд хэдэн системийн нөөцийг ажиллуулах гэх мэт.

P2P сүлжээний топологи нь ARPANET - ийн үеэс судлагдаж ирсэн хэдий ч 1990 - д оны сүүлээр Napster гэх мэт дуу хуваалцах програмууд гарч P2P холболтын загварын давуу тал нийтэд танигдаж интернетийн сүлжээнд ашиглагдаж эхэлсэн. Napster болон түүний Gnutella гэх мэт залгамжлагчид мөн BitTorrent зэрэг програмууд дуу хөгжим болом киноны зах зээлийн ашигт шууд нөлөөлж хүмүүсийн мэдээллийг эзэмших болон хэрэглэх хандлагад илт өөрчлөлт хийсэн.

Napster, OpenNap болон IRC@find гэх мэт сүлжээ болон сувгууд нь зарим үйлдэлдээ (хайлт гэх мэт) клиент/сервер бүтцийг ашигладаг. Gnutella, Freenet зэрэг сүлжээнүүд бүрэн P2P загвартай гэгддэг ч бусад зангилаануудын байршилыг тодорхойлох лавлах(directory) сервер ашигладаг.

Төвлөрсөн бус тооцооллын систем нь peer-to-peer сүлээнд ажилладаг. Төвлөрсөн бус P2P сүлжээ гэдэгт, сүлжээнд оролцогч буюу зангилаа нь газарзүйн хувьд тархсан байдаг ба зангилаа хооронд мэдээлэл солилцоо нь агшин зуур хийгддэггүй, тархах байдлаар явагддаг учраас “төвлөрсөн бус” гэдэг утгыг, мөн зангилаа нь сервер зэргээр дамжилгүйгээр өөр зангилаа-тэй шууд холбогддог “P2P(peer to peer)” гэдэг утгыг агуулж байдаг.

Төвлөрсөн бус P2P сүлжээнд гүйлгээг баталгаажуулахын тулд, зангилаа хоорондын мэдээлэл солилцоо шаардлагатай болно. Дээрх мөнгө шилжүүлэх жишээн дээр мөнгө шилжүүлэлт зөв явагдсан эсэхийг баталгаажуулахын тулд, хэнд хэчинээн төгрөг байгаа вэ гэдэг мэдээллийг сүлжээнд байгаа бүх зангилаа дээр мэдэж байх хэрэгтэй.

Тодорхойгүй тооны олон оролцогчтой сүлжээнд, мэдээллийг солилцохдоо, тэдгээр мэдээллийг засах эрсдэлтэй биш үү, ялгаатай зангилаа дээр ялгаатай үр дүнд хүрвэл яаж нэгдсэн нэг үр дүнд саналаа нэгтгэх вэ гэдгийг бодох шаардлагатай гарч байна.

Peer-to-peer сүлжээ нь голдуу физик сүлжээний топологи дээр виртуал бүрхэх сүлжээний (Overlay network) зарим загварыг хэрэгжүүлдэг. Мэдээллүүд үндсэн TCP/IP сүлжээн дээгүүр дамжуулагдсаар байдаг ч application layer-т peer-үүд логик бүрхэх холбоосор хоорондоо шууд холбогдож харилцдаг. Давхаргууд нь peer олох болон индексжуулэх, мөн P2P системийг физик сүлжээний топологиос хамааралгүй болгоход ашиглагддаг. Зангилаанууд давхарга сүлжээгээр бие биетэйгээ хэрхэн холбогдсон байдал, мөн нөөцүүд хэрхэн индексэжсэн болон байршсан байдлаас шалтгаалж бүтэцлэгдсэн болон бүтэцлэгдээгүй сүлжээ гэж ангилдаг(эдгээр хоёрын хосолмол бүтэцтэй байдаг). Gnutella, FastTrack гэх мэт P2P сүлжээнүүд нь бүтэцлэгдээгүй сүлжээ юм.

Төвлөрсөн бус сүлжээ нь дараах давуу талуудтай

- Суурилуулах болон тохируулахад хялбар
- Холбогдсон компьютерууд нь серверээс хамаарахгүй
- Хувь хэрэглэгчид өөрсдийн хамтран хуваалцаж буй эх сурвалжийг хянаж чадна
- Худалдан авах болон байгуулахад үнэтэй биш

- Сүлжээний тусгай програм хангамж шаардлаггүй
- Сүлжээнд ажиллах тусгай администратор шаардахгүй

Төвлөрсөн бус сүлжээ нь дараах сул талуудтай

- Сүлжээний хамгаалалт нь зөвхөн тухайн эх сурвалжид тухайн цаг хугацаанд хамарна
- Хэрэглэгчид эх сурвалж болгонд өөр өөр олон нууц үг өгдөг.
- Холбогдсон компьютер болгон өөрийн эх сурвалжаа хамгаалах шаардлагатай

2.2.1 Төвлөрсөн бус сүлжээний архитектур

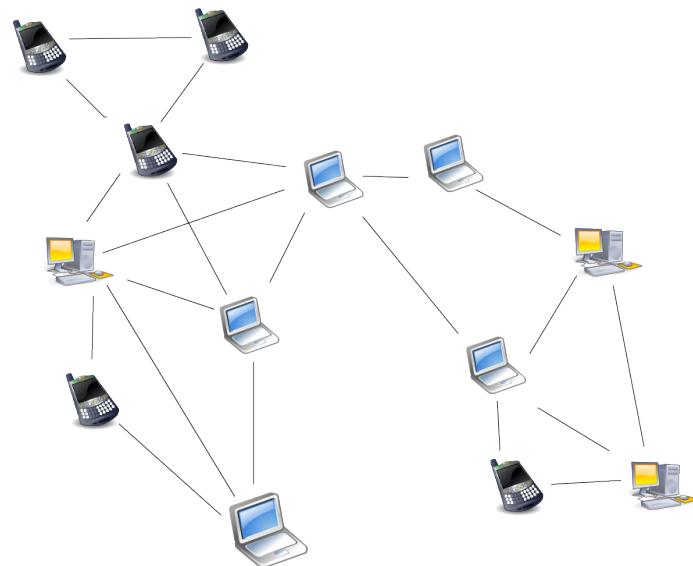
Peer-to-peer сүлжээ нь голдуу физик сүлжээний топологи дээр виртуал бүрхэх сүлжээний (Overlay network) зарим загварыг хэрэгжүүлдэг. Мэдээллүүд үндсэн TCP/IP сүлжээн дээгүүр дамжуулагдсаар байдаг ч application layer-т peer-үүд логик бүрхэх холбоосоор хоорондоо шууд холбогдож харилцдаг. Давхаргууд нь реег олох болон индексжүүлэх, мөн P2P системийг физик сүлжээний топологиос хамааралгүй болгоход ашиглагддаг. Зангилаанууд давхарга сүлжээгээр бие биетэйгээ хэрхэн холбогдсон байдал, мөн нөөцүүд хэрхэн индексэжсэн болон байршсан байдлаас шалтгаалж бүтэцлэгдсэн болон бүтэцлэгдээгүй сүлжээ гэж ангилдаг(эдгээр хоёрын хосолмол бүтэцтэй байдаг). Gnutella, FastTrack гэх мэт P2P сүлжээнүүд нь бүтэцлэгдээгүй сүлжээ юм.

2.2.1.1 Бүтэцлэгдээгүй сүлжээ

Бүтэцлэгдээгүй peer-to-peer сүлжээ нь загварын хувьд бүрхэх сүлжээн дээр тодорхой бүтцийг байгуулдаггүй, харин зангилаанууд хоорондоо санамсаргүй байдлаар холболт үүсгэж зохион байгуулалтад ордог. (Gnutella, Gossip, Kazaa зэрэг нь бүтэцгүй P2P протоколын жишээ юм)

Бүтэцлэгдээгүй сүлжээнүүдийн дээгүүр дахин шинэ бүтэц нэмэгдэхгүй тул байгуулахад амар бөгөөд давхаргын өөр өөр байршилд зохион байгуулах боломжтой. Түүнчлэн сүлжээн дэх бүх peer-үүдийг үүрэг оролцоо ижил учир бүтэцлэгдээгүй сүлжээ нь маш олон тооны peer-үүд ойр ойрхон сүлжээнд холбогдох болон гарах үе гэх мэт ачаалал өндөртэй үед маш бат бөх байж чаддаг.

Зураг 2.3-д бүтэцлэгдээгүй peer-to-peer сүлжээний загварыг үзүүлэв.



Зураг 2.3: Бүтэцлэгдээгүй P2P сүлжээний загвар

Бүтцийн дутагдалтай байдлаас шалтгаалж бүтэцлэгдээгүй сүлжээнд зарим хязгаарлагдмал байдлууд бий болдог. Тухайлбал, сүлжээн дэх peer мэдээллийн тодорхой нэг хэсгийг олох хэрэгцээ гарвал, хайлтын хүсэлт сүлжээн дэх тухайн мэдээллийг агуулж болох аль болох олон peer - үүдээр урсаж гарна. Энэ урсгал нь сүлжээнд маш их хэмжээний сигналын ачаалал үүсгэж CPU/memory - н ачааллыг нэмэгдүүлдэг ч хайлтын хүсэлт үргэлж амжилттай биелнэ гэсэн баталгаа байдаггүй. Түүнчлэн peer-үүдийн хооронд ямар ч харилцан хамаарал байдаггүй тул тухайн хайлтын урсгал хүсэж буй мэдээлэл нь хадгалагдаж байгаа peer-ээ олно гэх баталгаа мөн байдаггүй. Олон peer-үүдэд хадгалагдаж буй түгээмэл файлууд олдох магадлал өндөр байдаг бол хэдхэн peer-т байгаа мэдээллийг хайхад олдох үр дүн маш бага байдаг.

2.2.1.2 Бүтэцлэгдсэн сүлжээ

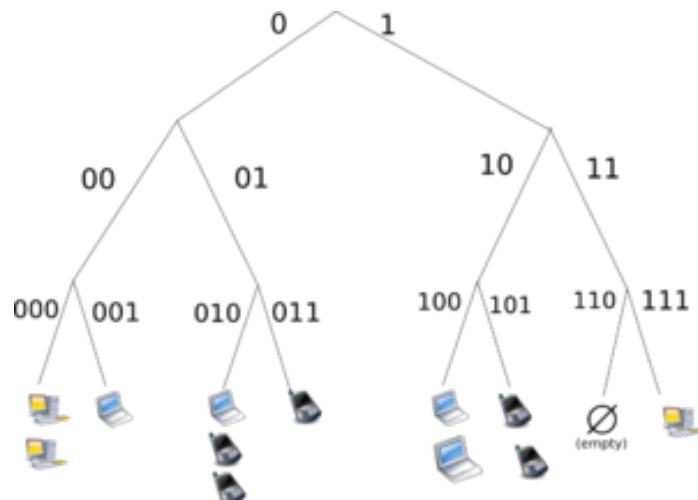
Бүтэцлэгдсэн сүлжээ нь давхарга тодорхой топологи болох зохион байгуулагддаг, мөн протокол нь сүлжээнд аль ч peer хүссэн файл болон нөөцийг хэдий маш ховор байсан ч үр ашигтайгаар хайж олох баталгааг хангадаг.

Хамгийн өргөн ашиглагддаг бүтэцлэгдсэн P2P сүлжээний төрлүүд нь хайж байгаа мэдээллээ хэн эзэмшиж байгааг тодорхойлох зорилгоор ашигладаг бүрэлдэхүүнт хаш

(consistent hashing) - н төрөл болох distributed hash table (DHT) - г ашигладаг. DHT - д хадгалагдаж буй хослол(түлхүүр, утга)-н hash table - г ашиглан сүлжээний нөөцийг олох боломжтой болгодог, мөн ямар ч идэвхтэй зангилаа үр ашигтайгаар өгөгдсөн түлхүүрт нийцэх утгыг буцаана.

Сүлжээний үр ашигтай байдлыг хангахын тулд бүтэцлэгдсэн сүлжээн дахь зангилаа-нууд тухайн нөхцөлийг хангасан хөршийн жагсаалтыг дэмждэг байх ёстой. Ингэснээр сүлжээний өндөр ачаалалтай үед зангилаануудыг тэсвэр багатай болгодог. Бодит ачаалалын үе дэх P2P нөөц олох шийдэлд хийсэн тооцооллоор нөөц зарлах/илрүүлэх ачаалал өндөр, мөн статик болон динамик ачааллын тэнцвэр алдагдах зэрэг DHT - д суурилсан хэд хэдэн асуудлыг илрүүлсэн.

Зураг 2.4-д Бүтэцлэгдсэн peer-to-peer сүлжээний загварыг үзүүлэв.



Зураг 2.4: Бүтэцлэгдсэн P2P сүлжээний загвар

2.2.1.3 Хосолмол загвар

Хосолмол загвар нь peer-to-peer сүлжээ болон клиент-сервер загварын хослол юм.

Нийтлэг хосолмол загвар нь peer-үүд нэг нэгнээ олоход зориулагдсан төвлөрсөн сервертэй байдаг. Энэ төрлийн загварын томоохон жишээ нь Spotify юм. Маш олон тооны хосолмол загварууд байдаг бөгөөд тэдгээр нь бүгд бүтэцлэгдсэн клиент/сервер сүлжээгээр загварчлагдсан төвлөрсөн үйл ажиллагаагаар тохиролцож, харин peer-үүд бу-

тэцлэгдээгүй цэвэр peer-to-peer сүлжээгээр хангагддаг. Одоогийн байдлаар хосолмол загвар нь төвлөрсөн үйл ажиллагаат хайлттай бөгөөд зангилаанууд нь бүтэцлэгдээгүй сүлжээний төвлөрсөн бус үйл ажиллагааны давуу талыг ашигласан нь цэвэр бүтэцлэгдсэн болон цэвэр бүтэцлэгдээгүй сүлжээний загваруудаас харьцангуй илүү гүйцэтгэлтэй байж чадаж байна.

2.3 Нууцлал аюулгүй байдал

2.3.1 Хаш функц

Хаш функц нь блокчэйн технологийн үндсэн суурь хэсэг юм. Хэрэв хаш функцийг ойлгочихвол хорт үйлдлийг илрүүлэх (tamper proof), тоон хурууны хээ зэрэг бусад концепцуудыг ойлгоход хялбар болно.

Хаш концепц нь үнэндээ маш энгийн. Энэ технологийг тайлбарласан техникийн хэл нь л хүмүүсийн толгойг эргүүлдэг. Хаш функцийг энгийнээр тайлбарлавал энэ нь тодорхой нэг оролтын утгыг авч гаралтын утга үүсгэдэг функц юм.

Энэ тодорхойлолтыг дэлгэрүүлбэл, хаш функц ямар ч хэмжээтэй утгыг оролтдоо аваад тогтмол урттай гаралтын утга үүсгэдэг.

Зураг 2.5-д MD5 гэж нэрлэгддэг хаш функцийн нэг төрлөөр жишээ авав.

```
mnkhbmb@3421:~$ echo Bi egchdee 500tugrug zeelew | md5sum
eeaaa32633d1c56f451eb4aa688cb878 -
mnkhbmb@3421:~$ █
```

Зураг 2.5: MD5 -аар хашлах үйлдэл

Үнд авсан стрингс утгаа санамсаргүй тоо болон үсгээс бүрдсэн “eeaaa32633d1c56f451eb4aa688cb878” гэх гаралтын утга болгон гаргасан байна. Энэ үйлдлийг мэдээллийг хураангуйлах (message digest) гэж нэрлэдэг. Түүнчлэн тоон хурууны хээ ч гэж нэрлэгдэх нь бий. Дээрх жишээн дэх “Bi egchdee 500tugrug zeelew” гэсэн оролтын утгын зөвхөн ганц тэмдгийг өөрчлөх буюу жишээ нь “Bi egchdee 200tugrug zeelew” болгоход гаралтын утга нь тэр чигтээ өөрчлөгдөх болно.

2.3.1.1 Хаш функцийн төрлүүд

Олон төрлийн хаш функц байдаг. Блокчэйний хувьд үндсэн ашигладаг хаш функц нь SHA256 болон RIPEMD. 128 эсвэл 256 гэх тоонууд нь үндсэндээ гаралтынхаа утгын уртыг илэрхийлдэг. SHA256 нь 256бит утга гаргана гэсэн үг.

Зураг 2.6-д SHA256 гэж нэрлэгддэг хаш функцийн нэг төрлөөр жишээ авав.

```
mnkhbmb@3421:~$ echo Bi egchdee 500tugrug zeelew | sha256sum
36142eed179443a8bf11e9bea88c0c88669a9a71ce294239545da82fc3b635b
mnkhbmb@3421:~$ █
```

Зураг 2.6: SHA256 гаралтын утга

Дээрх зурагт SHA256 командыг Линукс дээр ажиллуулаад гаралтдаа 256бит буюу 64 тэмдэгтийн урттай болсон байна.

2.3.1.2 Θөрчлөлтийг илрүүлэх

Ирсэн мэдээллийг замдаа өөрчлөгдсөн эсэхийг мэдэх хамгийн амар арга нь илгээгчийн мэдээллийн гаралтын хаш утгыг ирсэн мэдээллийн хаш утгатай харьцуулах юм. Хэрэв хаш утгууд яг ижил байвал мэдээлэл алдаагүй иржээ гэдэгт итгэлтэй байж болно.

2.3.1.3 Давхцал

Маш олон хүмүүс мэдээллийн хураангуй хэзээ ч давхцахгүй байх боломжтой юу гэдэгт өргэлзэн, хэзээд дахин давтагдашгүй байна гэдэг боломжгүй гэж үздэг.

Мэдээж гаралтын утга тогтсон урттай тул хязгааргүй тооны дахин давтагдашгүй утга байна гэж байхгүй ч энэ технологийн нууц нь хоёр өөр утга ижил хаш гаралттай байх тохиолдлыг олохын тулд бүх компьютеруудыг ашиглахад хэдэн арван сая жил шаардагдана. Иймд энэ технологи ойрын ирээдүйн хэрэгцээнд хангалттай баталгаатай гэсэн үг юм.

2.3.1.4 Нэг чиглэлт функц

Өөр нэг хаш функцийн чухал шинж нь нэг чиглэлт үйлдэл хийдэг. Энэ нь мэдээллийг хураангуйлахад маш хялбар боловч хураангуйллыг эргэн тайлах нь бараг л боломжгүй

зүйл юм. Өмнөх жишээ шиг мэдээж огт боломжгүй биш боловч гаралтын утгыг олоход мөн л асар их хугацаа шаардана.

2.3.1.5 Шахалт

Хаш функцийн бас нэг ойлголт нь шахалт. Том хэмжээтэй өгөгдөл стрингсээр илэрхийлэгдэх маш богино өгөгдөл болон гардаг. Үүнийг мэдээлэл дамжуулалтын явцад алдаа гарсан, эсвэл өөрчлөлт орсон зэргийг илрүүлэхэд ашиглаж болдог.

2.3.1.6 Хаш функц блокчэйнд хэрхэн хэрэглэгддэг вэ

Блокчэйн үйл ажиллагаандаа хаш функцийг байнга ашигладаг. Блокчэйн дахь мэдээллийн блок бүрд хашлагдсан байдаг. Хэрэв блок өөрчлөгдвэл, жишээ нь хэн нэгэн өөрт байгаа bitcoin -ий хэмжээг өөрчлөх, эсвэл хэн нэгэнд хэр өртэй гэдгээ өөрчлөхийг оролдвол хаш утга нь өөрчлөгдөөд бусад блок бүр ямар нэг өөрчлөлт гарсныг тэр дороо мэднэ.

Өмнөх блокийн хашлагдсан утгыг шинэ блокийн хаш утгыг үүсгэхэд ашигладаг тул блокуудын холбоо үүсдэг.

2.3.2 RSA алгоритм

RSA нь интернет дээгүүр хувийн болон нууц мэдээлэл дамжуулахад өгрөн ашиглагддаг нийтийн түлхүүрээр мэдээллийг нууцлах крипто-систем юм. RSA-г 1978 онд Масачусетийн Технологийн хүрээлэнгийн (Massachusetts Institute of Technology) R.Rivest, A.Shamir, L.Adelman нар бүтээсэн. Нийтийн түлхүүрт шифрлэлт буюу асимметрик шифрлэлт нь нэг нийтийн болон нэг хувийн хоёр өөр боловч математикийн уялдаатай түлхүүрүүд ашигладаг. Нийтийн түлхүүр нь бүгдэд нээлттэй бол хувийн түлхүүр нь нууц байх ёстой. RSA шифрлэлтэд нийтийн болон хувийн түлхүүрүүд хоёул зурvasыг шифрлэх боломжтой. Энэ шинж нь RSA алгоритмыг хамгийн өргөн ашиглагддаг асимметрик алгоритм болгосон.

RSA алгоритм нь өнөөгийн мэдээлэл технологийн хамгаалалтын гол тулгуур болж байна. Интернетээр худалдаа хийх үед хөтчийн веб хаягийн өмнөх цоожны зураг онлайн дэлгүүртэй хийж буй харилцаа шифрлэгдсэн байгааг илэрхийлнэ. Цоожны зурган дээр даралт хийж, дэлгэрэнгүй мэдээлэл дотроос тоо болон үсгүүдийн дарааллыг харж

болно. Энэ нь 16-тын тооллоор илэрхийлэгдсэн хэн ч харж болох нийтэд дэлгэсэн түлхүүр юм. Кредит картын дугаарыг оруулах үед нийтэд ил харагдах түлхүүр автоматаар дуудагдаж, дугаарыг шифрлэн дэлгүүрт илгээдэг. Ил түлхүүр үнэхээр аюулгүй байж чадах уу гэсэн эргэлзээ төрнө. Үүний нууц нь зөвхөн нэг чиглэлт функцийн үр дүн юм. Бид телефон утасны жагсаалтаас хүний нэрээр утасны дугаарыг олж болох ч, эсрэгээр дугаараас нэрийг олж болдоггүйтэй адил юм.

RSA алгоритм анхны тоог ашигладаг. Анхны тоо нь 1, 3, 5, 7, 11 гэх мэтчилэн хязгааргүй үргэлжилнэ. Эрдэмтэд 2500 жилийн туршид бүхий л анхны тоог нэгэн зэрэг илэрхийлэх нэгдсэн томьёог хайсаар ирсэн боловч олж чадаагүй л байна. Энэ нь анхны тоог шифрлэлтэд ашиглах үндэс болжээ. Дэлгүүр хэрэглэгчийн мэдээллийг нууцлахын тулд урьдчилан 2 анхны тоог сонгодог. Тэдгээрийн үржвэр нь нийтэд үзүүлэх түлхүүр болно. Кредит картын дугаар энэ түлхүүрээр шифрлэгдэн илгээгдэж, дэлгүүр анхны 2 тоог мэдэх учир шифрийг тайлж кредит картын дугаар уншигдана. Нөгөө талаас хакерууд түлхүүрийг анхны тооны үржвэрт задалж чадвал кредит картын дугаарыг мэдэж чадах мэт санагдана. Гэвч энэ нь боломжгүй юм. Одоогийн байдлаар RSA шифрлэлтийн түлхүүр нийт 617 оронгоос бүрдэж байна. Энэ нь өнөөгийн ямар ч супер компьютер, хэдэн ч ширхгийг ашигласан үржвэрийг олох боломжгүй том тоо юм.

RSA алгоритмыг Америкийн Үндэсний Стандартчиллын Газар (NIST)-aac PKCS1, ANSI X9.31, IEEE 1363 стандартуудаар баталгаажуулсан байдаг бөгөөд мэдээллийн жижиг блокуудыг шифрлэх, түлхүүр солилцох үйлдлийг ашигладаг програм хангамжууд болон SSH, OpenPGP, S/MIME, болон SSL/TLS зэрэг маш олон протоколуудад, мөн тоон гарын үгийн загварт хэрэглэгдэж байна.

RSA алгоритмын түлхүүрийг 512бит, 1024бит, 2048бит, 4096бит урттайгаар сонгон авч болдог. Төсөөлбөл 64, 128, 256, 512 үсэгтэй нууц үг байна гэж ойлгож болно. Ийм урт нууц үгийг цээжлэх хэцүү. Тиймээс нууц үгийг файл дээр бичээд компьютерт хадгалдаг. Нийтийн түлхүүрийг харилцагч бүр мэддэг байх ба хувийн түлхүүрийг ганцхан өөртөө хадгалах ёстой. Нийтийн болон хувийн түлхүүрүүд нь бие биенээсээ харилцан хамааралтай хосолмол шинжтэй байдаг. Аливаа нэг хосын хувийн түлхүүр өөр нэг хосын нийтийн түлхүүртэй зохицон ажиллах боломжгүй. Нийтийн түлхүүрийг бусдад түгээхдээ шууд файл хэлбэрээр дамжуулах, нийтийн түлхүүр хадгалах сервер дээр байршуулах зэрэг аргууд ашигладаг. Хувийн түлхүүрийг бол зөвхөн өөрийн компью-

терт хадгална. RSA алгоритмаар ямар ч хэмжээний өгөгдлийг нууцалж болно. Өгөгдлийг нийтийн түлхүүрээр нууцалж, хувийн түлхүүрээр тайлна. RSA алгоритмын давуутал нь өгөгдлийг нууцлах болон баталгаажуулах чадвартай байдаг. Нууцлах бол бидний мэддэгээр баримт бичгийг бусад хүмүүс гартаа оруулсан ч унших боломжгүй болгохыг хэлнэ. Харин баталгаажуулах нь баримт бичигт тамга даран баталгаажуулдаг шиг тийм үйлдлийг тоон баримтад хэрэгжүүлдэг. Үүнийг тоон гарын үсэг гэж нэрлэн заншжээ. RSA алгоритмыг тоон гарын үсэг, сертификатад голлон ашиглаж байна.

RSA нийтийн түлхүүр нь (n, e) гэсэн бүхэл тоон хосоос бүрдэх ба энд RSA модуль нь ижил битийн урттай санамсаргүйгээр үүсгэсэн (нууц) p, q хоёр анхны тоонуудын үржвэр байна. Өөрөөр хэлбэл $n = p * q$. Шифрлэх илтгэгч нь :

$$1 < e < \varphi(n), \quad \gcd(e, \varphi(n)) = 1$$

нөхцөлийг хангах бүхэл тоо, энд $\varphi(n) = \varphi = (p - 1)(q - 1)$. Хувийн түлхүүр d -ийг мөн шифр тайлах илтгэгч гэж нэрлэх ба

$$1 < d < \varphi(n), \quad ed \equiv 1 \pmod{\varphi}$$

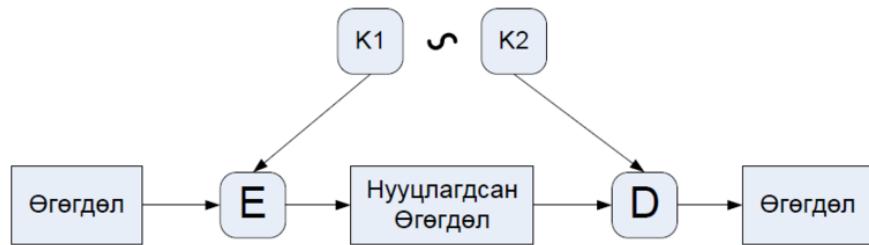
нөхцөлийг хангах бүхэл тоо байна. (n, e) нийтийн түлхүүрээс хувийн түлхүүр d -ийг тодорхойлох бодлого нь n тооны p, q үржвэрүүдийг тодорхойлох бодлоготой тооцооллын хувьд нэг болохыг баталсан. Аливаа том тоог анхны тоонуудын үржвэрт задлах асуудал нь тооцооллын хувьд хүнд бодлого юм.

Нийтийн түлхүүрийг харилцагч бүр мэддэг байх ба хувийн түлхүүрийг ганцхан өөртөө хадгалах ёстой. Нийтийн болон хувийн түлхүүрүүд нь бие биенээсээ харилцан хамааралтай хосолмол шинжтэй байдаг. Аливаа нэг хосын хувийн түлхүүр өөр нэг хосын нийтийн түлхүүртэй зохицон ажиллах боломжгүй. Нийтийн түлхүүрийг бусдад түгээхдээ шууд файл хэлбэрээр дамжуулах, нийтийн түлхүүр хадгалах сервер дээр байршуулах зэрэг аргууд ашигладаг. Хувийн түлхүүрийг бол зөвхөн өөрийн компьютерт хадгална.

Зураг 2.7-д нийтийн түлхүүртэй алгоритмыг дүрслэн үзүүлэв.

2.3.3 Цахим гарын үсэг

Тоон гарын үсэг нь мэдээллийн эх үүсвэрийн үнэн зөв байдлыг баталгаажуулахын тулд, мөн тухайн мэдээлэл бүрэн бүтэн байгааг нотлон шалгахад мэдээллийн хүлээн



Зураг 2.7: Нийтийн түлхүүртэй алгоритм

авагчид эрх олгодог. Иймээс нийтийн түлхүүрт тоон гарын үсэг нь танилт болон өгөгдлийн бүрэн бүтэн байдлыг хангадаг. Тоон гарын үсэг нь гар бичмэлийн гарын үсэгтэй ижил зорилготой. Гэсэн хэдий ч, гар бичмэлийн гарын үсэг нь хуурамчаар үйлдэхэд хялбар байдаг. Тоон гарын үсэг нь гар бичмэлийн гарын үсгийг бодвол бараг л хуулбарлах боломжгүйгээс гадна мэдээллийн агуулгууд болон гарын үсэг зурагчийг жинхэнэ байдлыг нотолдог бөгөөд дараах 2 зүйлийг баталгаажуулдаг мэдээлэл юм. Үүнд:

- Цахим баримт буюу файлд гарын үсэг зурсан этгээд буюу эзэн, хариуцагч нь хэн бэ гэдгийг
- Тухайн файлд гарын үсэг зурагдсанаас хойш санаатай болон санамсаргүй байдлаар ямар нэгэн өөрчлөлт ороогүй эсвэл эвдрээгүй гэдгийг

Зарим тохиолдолд, энэ мэдээллийг тухайн файлаас нь салгах боломжгүйгээр түүнд хавсаргасан байдаг. Өөрөөр хэлбэл, ямар нэгэн файл үүсгэхэд түүний нэр, хэмжээ, төрөл, үүсгэсэн, өөрчилсөн огноо зэрэг мэдээлэл нь файлын агуулгад биш гэхдээ дайвар байдлаар тухайн файлтайгаа хамт байдагтай адил зүйл. Дараах зүйлсийг тоон гарын үсэгт тооцохгүй. Жишээлбэл:

- Ямар нэгэн материал дээр үзгээр гарын үсгээ зураад тухайн материалыа скайндэж эсвэл фото зургийг нь авч цахим хэлбэрт оруулсан хуулбар
- Зурмал гарын үсэг бүхий факс
- Ямар нэг баримтын агуулга дотор скайндаж оруулсан, зурмал гарын үсгийн зураг
- Цахим шууданд хавсаргасан, зурмал гарын үсгийн зураг гэх мэт

Эдгээр нь тоон гарын үсэгтэй ямар ч хамааралгүй, зүгээр л нэг файл, дүрс, тэмдэгт бөгөөд хүмүүсийн ихэнх нь эдгээр хэлбэрийг тоон гарын үсэг гэж бодож төөрөлддөг. Харин эдгээр арга, хэлбэрийг тоон гарын үсгийн мөрөөдлийн, зөгнөлт хэлбэр гэж үзэх нь бий. Үнэн хэрэгтээ, эдгээр мэдээлэл нь тухайн баримтын үнэн худал болон хариуцагчийг бүрэн баталгаажуулдаггүй тул хүчин төгөлдөр гарын үсэг хэмээн тооцож ашиглах боломжгүй юм. Хэн нэгний нийтийн түлхүүрийг ашиглан мэдээллийг шифрлэхийн оронд, та өөрийн хувийн түлхүүрээр шифрлэх хэрэгтэй. Хэрэв тухайн мэдээлэл таны нийтийн түлхүүрээр тайлагдан уншигдах боломжтой байвал тэр нь танаас үүсгэгдсэн мэдээлэл байх ёстой.

Өдөр тутмын амьдралд файл болон бичиг баримтыг илгээж, хүлээж авахдаа хүлээж авсан файл үнэхээр зөв хүнээс илгээгдэж ирсэн эсэхийг баталгаажуулж чадахгүй байж болох юм.

Жишээ нь Бат Доржид чухал материал илгээх тохиолдолд, муу санаатай хэн нэгэн Батын оронд өөр материал илгээж магадгүй, эсвэл Батын явуулсан материалыг замаас нь хулгайлж, засварлаад Доржид явуулж магадгүй. Энэ үед Доржийн хүлээж авсан файл “Батаас илгээсэн зөв файл мөн” гэдгийг хэрхэн шалгах вэ. Энэ асуудлыг шийдэж өгөх арга нь цахим гарын үсэг юм.

Дээрх жишээ шиг олон тохиолдолд файл болон бичиг баримтыг илгээх үед, хүлээж авагч нь тухайн файлыг илгээгч нь үнэн зөв илгээгч байсан, бичиг баримт нь мөн үнэн зөв, засварлагдаагүй байсан гэдгийг баталгаажуулах шаардлагатай.

Цахим гарын үсгээр, түлхүүрийн хослолыг (нууц болон нийтэд ил) ашиглан, гарын үсгийг үүсгэж, гарын үсгийг шалгаснаар дээрх шаардлагыг хангадаг. Нууц түлхүүр нь гарын үсэг гэж нэрлэгддэг бөгөөд, гарын үсэг зурах хүнд л байна. Харин, нийтэд ил түлхүүр нь шалгалтын түлхүүр гэж нэрлэгддэг бөгөөд, хэн ч олж авах боломжтой байдлаар нийтэд ил болгосон байдаг. Нууц түлхүүр болон нийтэд ил түлхүүр нь дараах онцлогуудтай.

- Нууц түлхүүрээр нууцалсан өгөгдлийг зөвхөн ил түлхүүрээр задлах боломжтой
- Ил түлхүүрээр нууцалсан өгөгдлийг зөвхөн нууц түлхүүрээр задлах боломжтой

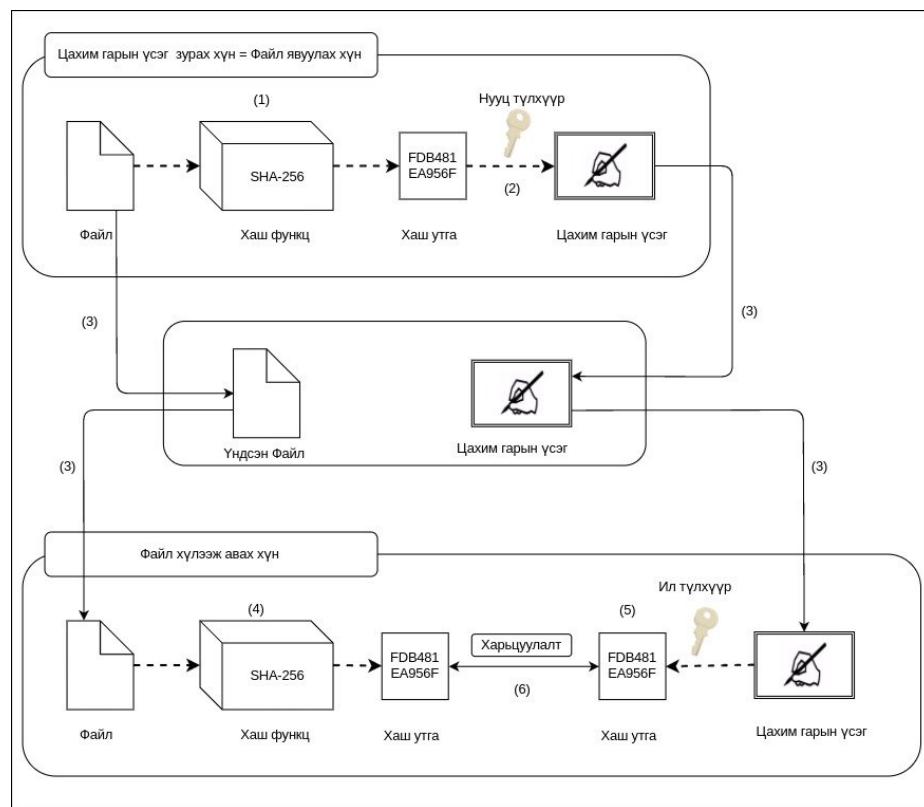
Ил түлхүүрээр нууцалсан өгөгдлийг зөвхөн нууц түлхүүрээр задлах боломжтой Ил түлхүүрээр нууцлах нь “Интернет дэлгүүрт кредит картын мэдээлэл илгээх”, “Нэвтрэх нууц үг илгээх” зэрэгт ашиглагддаг. Харин, нууц түлхүүрээр нууцалсан өгөгдөл нь

2.3. НУУЦЛАЛ АЮУЛГҮЙ БАЙДАЛ

БҮЛЭГ 2. ОНОЛ

Зөвхөн, нууц түлхүүртэй хүн л нээнэ гэдэг чанарыг ашиглаж “хэн задалсан бэ” гэдгийг нь баталгаажуулах арга(цахим гарын үсэг) болгон ашигладаг.

Зураг 2.8-д Батаас Доржид бичиг баримт илгээх тохиолдлыг жишээ болгон цахим гарын үсгээр явуулахыг Цахим гарын үсэгтэй файл явуулах урсгал-д үзүүллээ.



Зураг 2.8: Цахим гарын үсэгтэй файл явуулах урсгал

1. Бат (Гарын үсэг зурах = нууц түлхүүртэй хүн) үндсэн файлын хаш утгыг тооцоолно.
2. Батын нууц түлхүүрээр олсон хаш утгыг кодлоод, түүнийг гарын үсэг гэж үзнэ.
3. Батаас үндсэн файл болон гарын үсгийг Доржид илгээнэ.
4. Дорж хүлээж авсан файлаас хаш утгыг нь бодож олно.
5. Дорж хүлээж авсан гарын үсгийг Батын нууц түлхүүрт харгалзах ил түлхүүрээр задалж, үндсэн файлд харгалзах хаш утгыг олж авна.
6. Дорж 4-т бодож олсон “үндсэн файлын хаш утга” болон 5-д задалж олсон “үндсэн

файлын хаш утга"-г харьцуулна.

7. Уг харьцуулалтаар 4 болон 5-үүд ижилхэн байвал уг файл Батаас явуулсан файл мөн бөгөөд ямар нэг засваргүйгээр хүлээж авсан гэдгийн баталгаа болно.

Ийм байдлаар, цахим 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.

2.4 Тохиролцооны протоколууд

Өмнө хэлсэнчлэн, блокчэйн бол блок тус бүрийг нэг эгнээнд жагсаасан бүтэцтэй байдаг. Оролцох бүх зангилаа дээр ижил мэдээлэл бүхий блок ижил дарааллаар жагсан байх шаардлагатай. Уг блокийн дарааллыг шийдэх арга болгож блокчэйнд янз бүрийн нийцтэй байдлын алгоритмыг ашигладаг. Жишээлбэл, PoW(Proof of Work), PoS(Proof of Stake), PoI(Proof of Importance), PBFT(Practical Byzantine Fault Tolerance)

2.4.1 PoW(Proof of Work)

PoW бол bitcoinд ашиглагддаг алгоритм бөгөөд ерөнхийдөө майнинг/mining/ гэж нэрлэгддэг уйл ажиллагаанд хийгддэг зүйл юм. PoW-оор блок дотор агуулагддаг гүйлгээний мэдээлэл болон өмнөх блокийн хаш утган дээр санамсаргүй тоо(nonce) нэмж, хаш утга тооцоолоод явна. Бодож олсон хаш утга урьдчилан тохируулсан шалгуур утгаас бага болтол нь санамсаргүй тоог өөрчилж, дахин тооцоолол хийнэ. Нөхцөлд таарах хаш утгыг олбол, уг блокийг идэвхтэй блок болгож, оролцогчдод түгээж, хүлээн зөвшөөрүүлнэ.

Хүлээн зөвшөөрөх тал нь хүрч ирсэн блоконд агуулагдах санамсаргүй тоо болон мэдээлэл тус бүрийн хаш утгыг зөвхөн нэг удаа тооцоолж үнэхээр блокчэйний нөхцөлийг хангаж байгаа эсэхийг шалгана. Энэ үед хийгдэх шалгах(тооцоолох) процесс нь зөвхөн нэг удаа хийгдэх бөгөөд майнинг хийхэд явагддаг их хэмжээний тооцоололтой харьцуулахад маш богино хугацаанд тооцон шалгаж болдог гэдгээрээ онцлогтой.

Bitcoin-д урьдчилан тохируулсан нөхцөлд таарсан блокийг үүсгэж чадсан нөхцөлд, блок үүсгэгчид урамшуулал болгон BTC/bitcoin/-г өгдөг.

Одоогийн байдлаар 1 блок үүсгэлтээр олж авах урамшуулал 12.5 BTC учраас хувь хүнд ногдох урамшуулал гэдэг утгаараа маш өндөр мөнгөн дүн юм. Bitcoin-д энэ мэтийн урамшууллаар мотивацилагдаж, хаш тооцооллын өрсөлдөөн явагдаж байдаг.

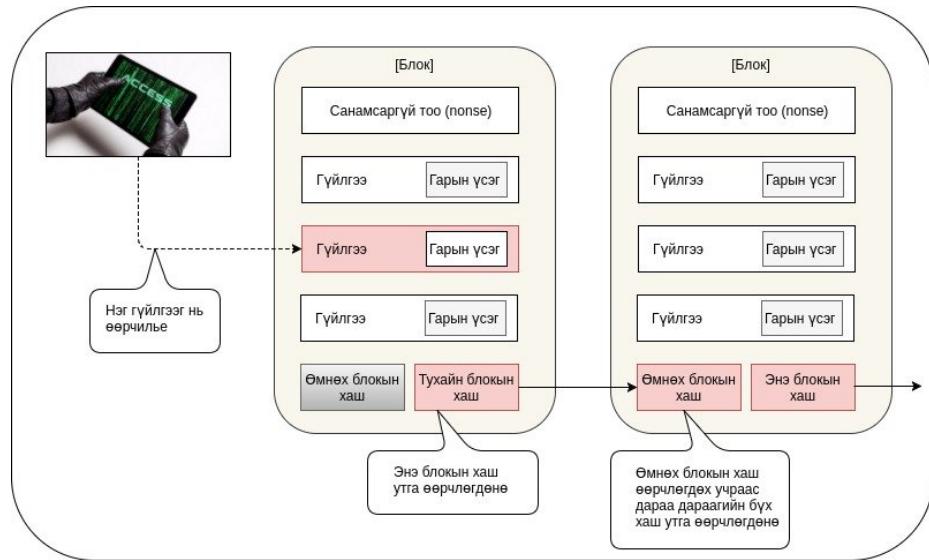
Нэмж хэлэхэд, bitcoin-ы майнингид Sha256 гэдэг алгоритм ашиглагддаг бөгөөд энэ алгоритмд зориулан оптимизаци хийгдсэн ASIC(Application Specific Integrated Circuit) гэдэг зориулалтын цахилгаан хэлхээ ашигласнаар өндөр хурдны майнинг хийх боломжтой болдог. Хаш утгын бодолтыг илэрхийлэх үзүүлэлт болгож хашрэйт(хаш үүсгэсэн тоо/секунд) ашиглагддаг бөгөөд 2017 оны 3 сарын байдлаар bitcoin систем бүхэлд нь авч үзвэл хашрэйт 3,252PH/s(Petahash/second) байдаг бөгөөд маш өндөр тооцон бодох чадвартай болохыг харж болно.

Харьцуулалт болгож, Intel Core i7 5820K бүхий CPU-гээр майнинг хийсэн тохиолдолд хашрэйт нь ойролцоогоор 10MH/s учир, хувь хүн CPU-гээр майнинг хийсэн нөхцөлд блок үүсгэх магадлал 325 тэрбумд 1 болох юм. Солир таарах магадлал 10 тэрбумын нэг гэж иэрлэгддэг учраас бодит байдал дээр CPU-гээр хожихгүй гэдэг нь тодорхой.

Bitcoin-д блокийг зэрэг олох магадлал байж болох учир олон газарт зэрэг олдсон тохиолдолд гинж салалт үүсэх болно. Ийм тохиолдолд, “Хамгийн урт гинж бүхий салаа нь хамгийн их хэмжээний тооцооллын зардлаар олдсон” гэдэг зарчим дээр тулгуурлаж, хамгийн урт гинж бүхий салааг сонгож авна гэсэн байдлаар явагдана. Хамгийн урт гинжийг сонгож авах арга нь гинжийг өөрчлөх асуудлын хувьд ч хамгаалалт болох үр нөлөөтэй.

Зураг 2.9-д хорон санаалсан хэрэглэгч, нэг блок дахь гүйлгээний агуулгыг өөрчилье гэж үзсэн тохиолдлыг бодож үзүүлэв(Гүйлгээний мэдээллийг зассан үед).

Энэ тохиолдолд, гүйлгээний агуулгыг өөрчлөх учраас блокийн хаш утга бас өөрчлөгднө. Блокийн хаш утга өөрчлөгдмөгц, өмнө нь хангаж байсан нөхцөл (хаш утга шалгуур утгаас бага)-ийг хангаж чадахгүй болох учраас дахин санамсаргүй тоог өөрчилж, таарах хаш утгыг олох шаардлага үүснэ.



Зураг 2.9: Гүйлгээний мэдээллийг зассан үед

Энэ блок нь гинжний толгой хэсгээс /гинжний хамгийн шинэ, сүүлд нэмэгдсэн хэсэг/ бусад тохиолдолд, дараагийн блокод энэ блокийн хаш утга ашиглагдаж байгаа учраас, дараагийн блокийн хаш утгыг мөн өөрчилж бичих шаардлага үүснэ. Ингэмэгц, ээлж дараалан хаш утгыг дахин тооцоолж, хаш утгуудыг өөрчилж бичих шаардлага үүсч, энэ нь гинжний толгой/гинжний хамгийн шинэ, сүүлд нэмэгдсэн хэсэг/ хүртэл үргэлжлэх хэрэгтэй болно. Засъя гэж бодсон блокоос блокийн эхэн/гинжний хамгийн шинэ, сүүлд нэмэгдсэн хэсэг/ хүртэлх өөрчлөх хурд(өөрчлөгчийн тооцон бодох resource) нь жинхэнэ гинжний өсөх хурд (bitcoin системийн бүх тооцон бодох resource)-г давж гараагүй тохиолдолд уг дайралт амжилтгүй болох учраас гинжний өөрчлөлтийн эсрэг бат бөх гэж нэрлэгддэг.

Bitcoin-д хамгийн урт гинжийг хамгийн их зардал гаргасан гэж үздэг PoW(Proof of Work)-ийн тусламжтайгаар зангилаа хоорондын мэдээллийг нэгэн ижил саналд нийцүүлж байгааг танилцуулсан боловч, хувийн блокчэйнд оролцогч зангилааны тоог хязгаарлах боломжтой учраас, Paxos гэх мэт уламжлалт, түгээмэл тохиролцооны алгоритмыг ашиглах нь элбэг байдаг.

Нийтийн(public) болон хувийн (private) блокчэйний тохиролцооны алгоритмуудыг харьцуулбал, public блокчэйний сонгож авсан тохиролцооны алгоритм нь оролцогч зангилаануудын тоо олшрох тусам, гүйлгээний баталгаажуулалтын хурданд нөлөө гарах нь багасах шинж чанартай боловч, гүйлгээний процессын throughput/хурд/ өндөр биш

Харин хувийн блокчэйнд зангилаа тоо нэмэгдэхэд гүйлгээний баталгаажуулалтын хурд буурах боловч, тогтсон тооны зангилаануудын хүрээнд өндөр throughput-тэй байж чаддаг.

2.4.2 Эцэслэн шийдэх чанар(finalty)

Нийтийн болон хувийн блокчэйний тохиролцооны алгоритмд finalty гэж нэрлэгддэг шинж чанарын ялгаа бас бий. Finalty гэдэг нь нэг удаа хийгдсэн гүйлгээний үр дүнг цуцлахгүй(эцэслэн шийдэх) гэдгийг илэрхийлиэ. Энэ чанар нь бодит байдал дээр гүйлгээ хийх үед чухал элемент гэж хэлж болно. Оролцох зангилаа-д хязгаарлалт байхгүй нийтийн блокчэйний хувьд finalty-г авч явах нь хэцүү юм.

Жишээ нь блокчэйн дээр Батын үлдэгдэл 1000 төгрөг гэж бичигдсэн байсан гэж үзье. “Батаас Дорж уруу илгээх 600 төгрөг(шилжүүлэг БД гэе)” болон “Батаас Болд руу илгээх 700 төгрөг(шилжүүлэг ББ гэе)” нь нэгэн зэрэг өөр өөр зангилаа уруу хүснэгт(request) явсан гэж үзье

Хараахан аль ч гүйлгээ нь блокчэйн дээр тэмдэглэгдээгүй учраас хүсэлт хүлээж авсан зангилаа-ууд аль ч гүйлгээнд Батад хангалттай үлдэгдэл байгаад, гүйлгээг хийхэд асуудалгүй гэж үзнэ. 2 гүйлгээ нь 2-уулаа хүлээн зөвшөөрөгдчихвэл Батын үлдэгдэл хасах 300 төгрөг болж, систем бүхэлдээ хасах үлдэгдэл гэсэн буруу байдалд шилжчих нэ.

Энэ асуудлыг шийдэхийн тулд, [Гүйлгээ БД] юм уу[Гүйлгээ ББ]-гийн аль нь “түрүүлж үүссэн” бэ гэдгийг шийдэх шаардлага гарч байна. [Гүйлгээ БД] нь [Гүйлгээ ББ]-гээс түрүүлж үүссэн гэж үзвэл, [Гүйлгээ БД]-гийн дуусах мөчид Батын үлдэгдэл 400 төгрөг болж, [Гүйлгээ ББ] нь үлдэгдэл мөнгө хүрэлцэхгүй учраас буруу шилжүүлэг болж, блокчэйнд бүртгэгдэхгүй. Эсрэгээрээ [Гүйлгээ ББ] нь [Гүйлгээ БД]-ээс түрүүлж үүссэн бол, [Гүйлгээ БД] нь буруу шилжүүлэг болно.

Нийтийн блокчэйнд зангилаа бүр өөрийн хадгалж буй статус дээр үндэслэж, гүйлгээний шалгалтыг явуулдаг. Гүйлгээний шалгалт дууссан үед шалгалт дууссаныг сүлжээн доторх зангилаа-уудад цацдаг(broadcast). Шалгалт дууссан тухай мэдэгдэл хүлээж авсан зангилаа шалгалт зөв эсэхийг баталгаажуулаад өөрийн статусыг шинэчилдэг. Энэ зангилаа нь шинэ гүйлгээ шалгахаар бол, энэхүү шинэчлэгдсэн статус дээр үндэслэж гүйлгээг шалгана.

Дээр бичсэнчлэн, өөр өөр зангилаа дээр ялгаатай гүйлгээ бүр шалгагдаж, дууссан тухай мэдэгдэл сүлжээнд цацагдсан тохиолдолд, дууссан тухай мэдэгдлийг хүлээж авсан зангилаа өөрийн статусыг аль нэг гүйлгээний үр дүнгээр шинэчлэх шаардлага гарна. Энэ үед дууссан тухай мэдэгдэл хүлээж авсан зангилаа шалгалтын үр дүн тус бүрийн гинжний аль уртыг нь сонгож, статусаа шинэчилнэ.

Гинжний уртаас хамаарч, өмнө нь орсон гүйлгээ нь блокчэйнд бичигдэнэ. Хойно нь орсон гүйлгээний хувьд, зангилаа нь өмнө орсон гүйлгээний үр дүнг тооцсоны дараах шинэчлэгдсэн статусаар дахин шалгалт явуулна.

Дахин шалгалтын үр дүнд, гүйлгээ нь үнэн зөв байвал сүлжээн дотор дахин цацаж(broadcast) бусад зангилаа дээр хүлээж авах хүртэл хүлээнэ. Харин буруу байвал, уг гүйлгээний хүсэлт нь алдаа болно.

Өмнөх жишээн дээр, [Гүйлгээ БД]-ийн гинж [Гүйлгээ ББ]-ийн гинжнээс урт бөгөөд, [Гүйлгээ БД] нь блокчэйнд бичигдсэн гэж үзье. Үүний үр дүнд, Батын хамгийн сүүлийн үлдэгдэл 1000 төгрөгөөс 600 төгрөгөөр хасагдаж, 400 төгрөг болно. Энэ байдалд, [Гүйлгээ ББ]-г шалгаад, үлдэгдэл хүрэлцэхгүй учраас [Гүйлгээ ББ] нь буруу гүйлгээ болж алдаа болно. [Гүйлгээ БД]-г шалгасан нөхцөлийг бодож үзвэл, үлдэгдэл 1000 төгрөг байх үед шалгаад зөв гэсэн дүгнэлт хийгээд, гүйлгээг гүйцэтгэсэн(сүлжээн доторх цацсан) боловч, түүний дараагаар өөр гүйлгээ гүйцэтгэгдэж, тэр нь давуу эрхтэй байсан учраас, үлдэгдэл нь 400 төгрөг болж, [Гүйлгээ БД] нь буруу болсон байна.

Нэгэн зэрэг хийгдэх гүйлгээ нь 2-оос олонгүй байна гэж мэдэж байгаа тохиолдолд, нэг талынх нь гүйлгээг дууссаны дараа нөгөө нэгийг нь гүйцэтгэвэл, дээрх шиг цуцлах тохиолдлыг гаргахгүй байж чадна. Гэвч, тодорхойгүй олон тооны зангилаа оролцож байгаа нийтийн блокчэйнд, нэгэн зэрэг хийгдэх гүйлгээ хэд байхыг хэлж мэдэхгүй. [Гүйлгээ БД] болон [Гүйлгээ ББ]-гээс өөр гүйлгээ бас нэгэн зэрэг хийгдэж байгаад, хоёр гүйлгээ хоёулаа цуцлагдах магадлал ч бий.

Энэ мэтчилэн нийтийн блокчэйнд гүйлгээг гүйцэтгэсэн үр дүн цуцлагдахгүй гэсэн finally гэдэг шинж чанарыг хадгалж чаддаггүй.

Харин, оролцогч зангилаа-ын тоо нь хязгаарлагдсан хувийн блокчэйнд Paxos гэх мэтийн тохиролцооны алгоритмаар гүйлгээг эцэслэж чаддаг.

Жишээ нь, бүх зангилаа-оор олонхийн саналаар [Гүйлгээ БД]-г сонгох уу эсвэл [Гүйлгээ ББ]-г сонгох уу гэдгийг шийдэж чаддаг. Сонгогдсон гүйлгээ нь гинжин дээр бүртгэгдэж, түүнээс хойш цуцлагдахгүй болно. Олонхийн саналаар шийдэж байгаа бо-

лон үр дүнг нь бүх зангилаа дээр хүргэж чадаж байгаа нь оролцогч талуудын тоог хязгаарласан учраас юм.

2.4.3 Ухаалаг гэрээ(Smart contract)

Bitcoin-д зоос(коин)-ны шилжилтийн мэдээллийг бүх оролцогчдод дамжуулна гэсэн тогтолцоотой байсан. Үүний дээр, өөр мөнгөний мэдээлэл болон машин, үл хөдлөх хөрөнгийн эзэмших эрх гэх мэт зүйлсийг token/кодолсон тэмдэгтийн цуваа/ болгоод bitcoin-ы гүйлгээнд нэмэлт байдлаар оруулж, эдгээрийг өгч авалцдаг болгох өнгөт койн(colored coin) гэсэн санаа бас гарч ирсэн юм. Гэсэн хэдий ч, bitcoin-ы оршин байгаа тогтолцоог тэр хэвээр нь ашиглах учраас, агуулах мэдээллийн хэмжээнд хязгаар байгаа, мөн гүйлгээнд bitcoin хэрэгтэй болох зэрэг хязгаарлалтууд байсан. Иймд, Ethereum нь ухаалаг гэрээ гэдэг ойлголтыг оруулсан блокчэйн гэдгийг гаргаж, түүний дараагаар олон тооны блокчэйнд ухаалаг гэрээг оруулж ирсэн.

Ухаалаг гэрээг ашиглaval ямар зүйлийг хийж чаддаг болох вэ. Өргөн ашиглагддаг жишээ гэвэл “Автомат зарагч машинд зоос оруулахад, бараа гарч ирдэг” гэсэн дараалал бүхий урсгал бас ухаалаг гэрээ юм. Энэ мэтчилэн ямар нэг нөхцөлийн дор тогтсон үйлдэл хийдэг зүйлийг ухаалаг гэрээ гэж хэлдэг.

Ухаалаг гэрээ нь нэг үгээр хэлбэл “блокчэйн дээр ажиллана” гэсэн онцлогтой ердийн програм гэж хэлж болно. Ухаалаг гэрээ нь блокчэйн болгоноор нэршил нь өөр өөр байдаг боловч, цаанаа бодит бие нь Javascript(төрлийн хэл), Golang, Java, C# гэх мэтийн ердийн програмчлалын хэлээр бичиж болох програм бөгөөд блокчэйний статус болон хадгалагдаж байгаа дата зэргийг уншиж бичих зориулалттай зүйл юм.

Гэхдээ, “Блокчэйн дээр ажиллана” гэдэг дээр анхаарах зүйл бий. Энэ үгнээс ямар ажиллагаа төсөөлөгдж байна вэ? Блокчэйн бүхэлдээ 1 нийтлэг процессын байгууллага, эсвэл оролцогчдын аль нэг нь төлөөлөөд програмыг ажиллуулдаг гэж төсөөлөгддэж байна уу. Үнэндээ аль алинаас нь өөр бөгөөд, бүх зангилаа дээр ижил програм ажиллаж, хариултыг нь тааруулдаг гэсэн ажиллагаа болж байгаа юм.

Блокчэйн дээр бүх зангилаа нь ижил дата хуваалцдаг, гэдгийг аль хэдийнээ тайлбарласан боловч, энэ нь ухаалаг гэрээний хувьд ч мөн нэгэн адил юм.

Ердийн програмд санамсаргүй тоо ашиглаж, гаднах өгөгдлийн эх сурвалжаас утга олж авчирч, процесс хийх зэргийг ихэвчлэн хийдэг боловч, энэ мэт тодорхой бус шинжийг агуулсан ажиллагаа нь нэгэн ижил өгөгдлийг хуваалцана гэсэн шинж чанарыг

баримтлах шаардлагатай ухаалаг гэрээний хувьд чадахгүй зүйл бөгөөд детерминистик (тогтсон, тодорхой) байдлаар бүх процесс үргэлжилж байх шаардлагатай.

Ажиллуулах бүрд санамсаргүй тоо ашиглах эсвэл гадны сервертэй холбогдох шаардлагатай үед тэдгээр үйлдлүүдийг oracle гэж нэрлэгддэг 3-дагч этгээдээр гүйцэтгүүлж, олсон утгыг нь ухаалаг гэрээнд дамжуулах гэсэн арга бий. Энэ тохиолдолд, блокчэйн нь зорин байж хийсэн тархмал систем учраас oracle нь цорын ганц эвдрэлийн цэг болохооргүй байх хэрэгтэйг анхаарах хэрэгтэй.

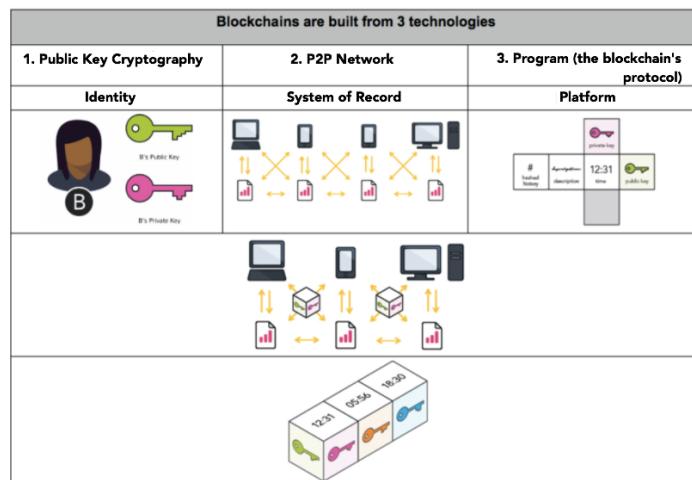
БҮЛЭГ 3

Судалгаа

3.1 Блокчэйн технологи хэрхэн ажилладаг вэ

Онолын хэсэгт Блокчэйн технологи гэж юу болох, ямар технологиуд блокчэйнийг бүрдүүлдэг тухай бичсэн бол одоо блокчэйн технологи хэрхэн ажилладаг талаар судалснаа тайлбарлай.

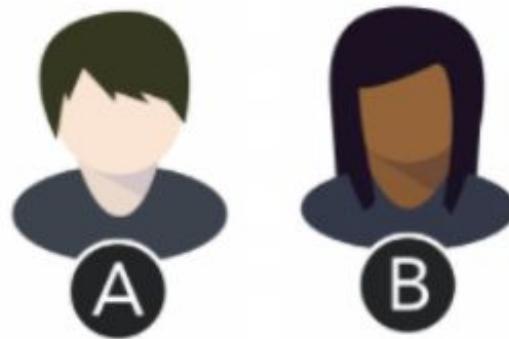
Блокчэйний ажиллагаа үндсэн гурван технологид суурилдаг тухай онолын хэсэгт дэлгэрэнгүй бичсэн. Энэ гурван технологи нь 1) хувийн түлхүүрт криптограф, 2) хуваалцдаг данстай тархсан сүлжээ 3) сүлжээний гүйлгээ болон бичилт хадгалалт болон хамгаалалтын үйлчилгээ үзүүлэх технологиуд юм.



Зураг 3.1: Блокчэйний үйл ажиллагааны ерөнхий бүтэц

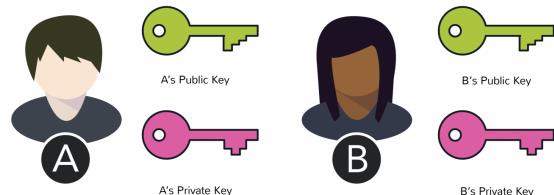
3.1.1 Криптограф түлхүүр

Хоёр хэрэглэгч интернетээр гүйлгээ хийх хүсэлт гаргана :



Зураг 3.2: Гүйлгээ хийх хэрэглэгчид

Хоёр хэрэглэгч тус бүр хувийн болон нийтийн түлхүүртэй.



Зураг 3.3: Хэрэглэгч тус бүр хувийн болон нийтийн түлхүүртэй

Блокчэйн технологийн энэ бүрэлдэхүүн хэсэг нь аюулгүй цахим танилт үүсгэх зорилготой. Цахим танилт нь хувийн болон нийтийн криптограф түлхүүрүүдийн хослолд суурилдаг. Тэдгээр түлхүүрүүдийн хослол нь тоон гарын үсэг болж ашиглагддаг.



Зураг 3.4: Хувийн болон нийтийн түлхүүрийн хослолоор тоон гарын үсэг үүснэ

3.1. БЛОКЧЭЙН ХЭРХЭН АЖИЛЛАДАГ ВЭ

БҮЛЭГ 3. СУДАЛГАА

Дан ганц найдвартай тоон гарын үсэг байлаа гээд аюулгүй цахим холбоо үүсгэхэд хангалтгүй юм. Адилтган танилтыг шийдэхийн хажуугаар гүйлгээг батлах болон зөвшөөрөл өгөх санаа байнга хамт байх ёстой.

Блокчэйний хувьд энэ нь тархсан сүлжээгээр эхэлдэг.

3.1.2 Тархсан сүлжээ

Тархсан сүлжээ ашиглахын хэрэгцээ болон давуу талыг дараах жишээтэй харьцуулж ойлгож болно. Хэрэв ойд мод уналаа гэж үзэхэд, модыг унаж байгааг бичих камер байсан гэж үзвэл бид мод уначихсан гэдэгт эргэлзэхгүй болно. Бид юунаас болсон, хэрхэн болсон зэрэг тодорхой зүйлгүй байсан ч харсан зүйлээрээ баталгаа хийдэг.

Блокчэйний хувьд сүлжээний хэрэглэгчид нь камерын оронд математик тооцооллоор нэг зэрэг нэг зүйлийг гэрчлэх замаар баталгаажуулалтыг хийдэг. Ерөнхийдөө сүлжээ том байх хэрээр найдвартай байдал нэмэгдэнэ гэж үздэг.

Bitcoin - ний сүлжээний хамрах хүрээ нь bitcoin - ний хамгийн давуу шинж болдог. Bitcoin сүлжээнд бичилт хийх үед 3,500,000 TH/s буюу дэлхийн томоохон 10,000 банк нийлснээс илүү хүчин чадлаар хамгаалагддаг гэсэн үг юм. Ethereum - ийн хувьд 12.5 TH/s буюу Bitcoin - той харьцуулахад бага ч гэсэн Google - с том бөгөөд үүсээд 2 жил болж байгаа, одоогоор туршилтын шатандaa байгаа гэж хэлж болно.

3.1.3 Бичилтийн систем



Зураг 3.5: Бичилтийн систем

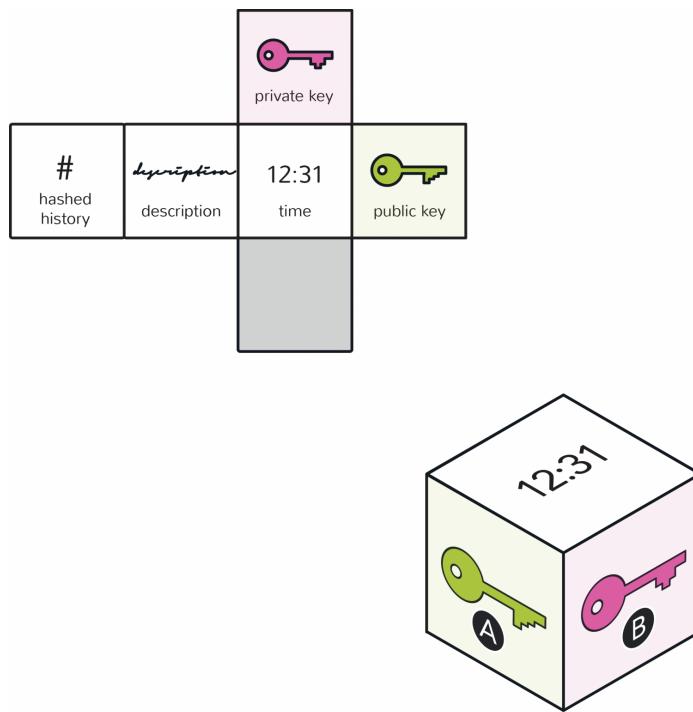
Сүлжээнд криптограф түлхүүрүүд холбогдсон үед цахим харилцаанд хамгийн ашигтай хэлбэр болдог. Үйл ажиллагаа нь А хэрэглэгч өөрийн хувийн түлхүүрийг авснаар

3.1. БЛОКЧЭЙН ХЭРХЭН АЖИЛЛАДАГ ВЭ

БҮЛЭГ 3. СУДАЛГАА

эхлэх ба зарим төрлийн мэдэгдэл үүсгэн (bitcoin - ний хувьд цахим мөнгөний нийлбэрийг илгээх гэх мэт) В хэрэглэгчийн нийтийн түлхүүрт холбодог.

3.1.4 Протокол

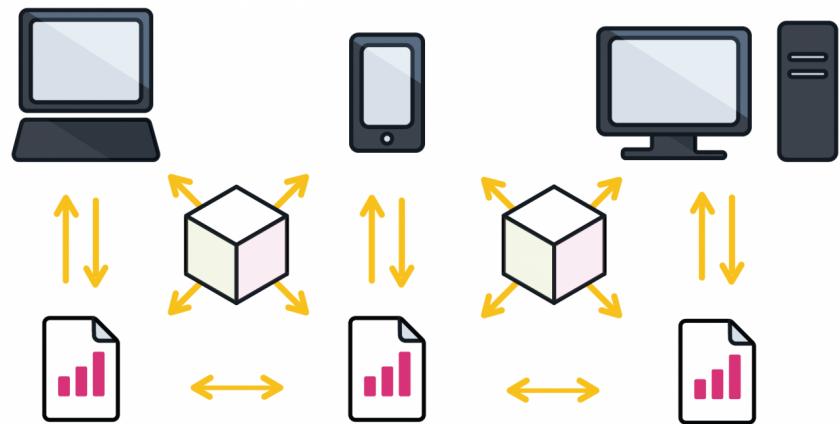


Зураг 3.6: Блокийн бүтэц

Блок нь тоон гарын үсэг, хугацааны тамга, холбогдох мэдээлэл зэргийг агуулах ба сүлжээн дэх бүх зангилаануудад цацагдана(broadcast).

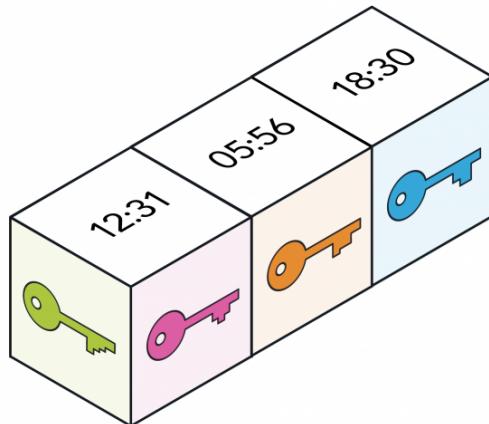
Зарим хүний хувьд "сүлжээг аюулгүй байлгахад оролцох тэр их тооцооллын чадлыг хаанаас цуглуулах юм бэ?" гэсэн асуулт гарч болно. Нээлттэй буюу нийтийн блокчэйний хувьд олборлолт(mining) гэдэг зүйл энэ асуултын хариулт болно. Компьютеруудыг сүлжээнд үйлчилснийх нь төлөө урамшуулал өгөх байдлаар блокчэйн сүлжээ ажилладаг. Хэрэглэгчийн хувийн ашиг сонирхол нийтийн хэрэгцээнд ашиглагдана гэсэн үг юм.

Bitcoin - ий хувьд протоколынх нь үндсэн зорилго нь нэг bitcoin-ийг ижил хугацаанд өөр өөр гүйлгээнд ашиглагдахгүй байлгах явдал юм. Энэ зорилгод хүрэхийн тулд сүлжээнд зангилаанууд proof-of-work математик тооцооллыг бодон bitcoin бүрд гүйлгээний түүхийг баталгаажуулж ажилладаг.



Зураг 3.7: Протокол дамжих үйл ажиллагаа

Олборлогчид ерөнхийдөө шинэ блокыг хүлээн зөвшөөрөх эсвэл хуурамч гэж үзэн блокыг буцаах эсэхийг CPU-нийхээ хүчин чадлаар сонгон сүлжээнд саналаа өгөх үйл явцыг хийдэг. Хэрэв дийлэнх олборлогчид нэг шийдэлд санал нэгдвэл тэд тухайн блокыг гинжинд(chain) холбоно. Тухайн блок хугацаагаар тамгалагдах ба мэдээлэл болон зуравс хадгалж болно.



Зураг 3.8: Гинжинд холбогдсон блокын цуваа

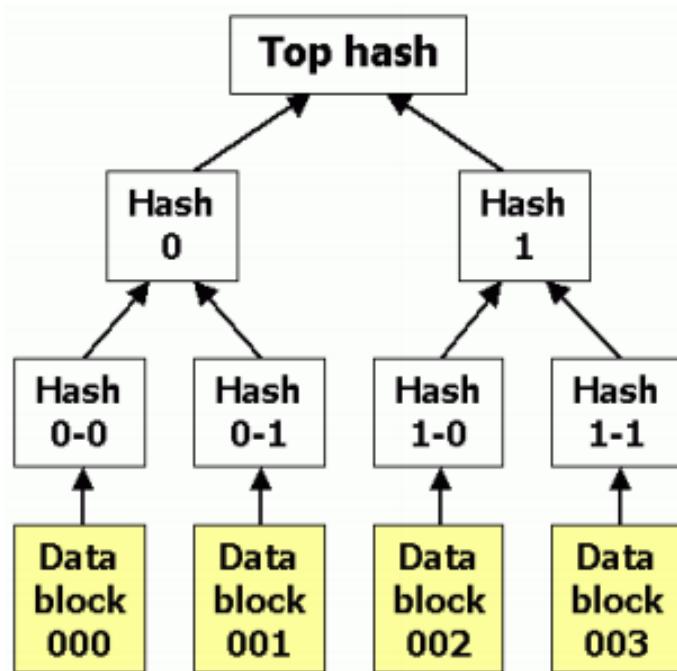
Блокын төрөл, хэмжээ болон баталгаажуулалт нь блокчэйн бүрийн хувьд өөр байж болдог. Энэ нь блокчэйний протоколоос буюу ямар гүйлгээг баталгаатай гүйлгээ гэж үзэх болон үзэхгүй байх болон шинэ блокыг хэрхэн үүсгэх удирдлагын дүрмээсээ хавьтаж болдог.

маардаг. Баталгаажуулалтын үйл ажиллагагаа блокчэйн бүрд тусгайлан зориулагдан хийгдэж болно.

3.1.5 Блок хэрхэн үүсдэг вэ

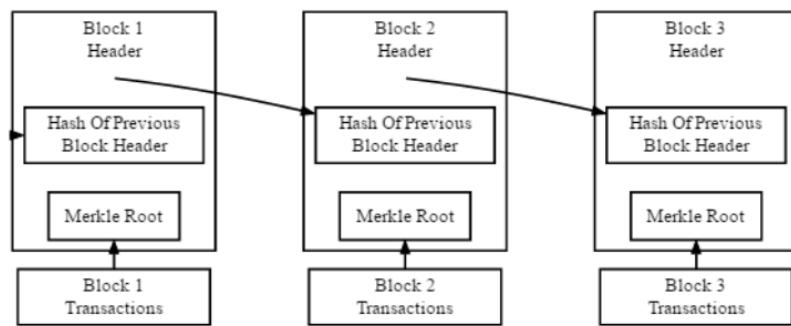
Блокчэйн технологи анхандаа Bitcoin - ийг гүйлгээний нийтийн дансанд ашиглагдаж байсан. Блокчэйн тэдгээр гүйлгээг блокт хадгалж илүү олон гүйлгээ хийгдсэнээр эцэст нь блок бүрэн гүйцэд болдог. Блок бүрдмэгцүүтгүүд linear chronological (шугаман даарайдал) -р блокт нэмэгддэг.

Блокчэйний анхны блокыг "Genesis block(Үүсэл блок)" өөрөөр "Block 0" гэж нэрлэдэг. Genesis блок нь ихэнхдээ програмдаа хатуугаар бичигдсэн байдаг ба өмнөх блокийн утгыг агуулдаггүйгээрээ онцлог. Genesis блок нэгэнт үүссэн бол "Блок 1" үүсэж genesis блокт залгагддаг. Блок бүр гүйлгээний мэдээллийн хэсэгтэй байдаг ба энэ хэсэгт гүйлгээ бүрийг хашлан утгыг нь хуулж аваад хос хосоор нь нийлүүлж хашладаг, энэ үйлдлийг ганц хаш үлдтэл нь давтана хийнэ (зураг 3.9). Хамгийн сүүлд үлдсэн хашийг merkle root буюу модны үндсэн гэж нэрлэдэг. Блокын толгойд (block header) merkle root хадгалагддаг.



Зураг 3.9: Хаш хүснэгт

Гүйлгээний утгыг өөрчлөгдөөгүй гэдгийг баталгаажуулахын тулд блок бүр өмнөх блокийнхоо толгой мэдээллийг хадгалдаг, ингэснээр мэдээллийг өөрчлөх тохиолдолд зураг 3.10 - т харуулснаар тухайн гүйлгээний утгыг хадгалж буй блокоос гадна удаах блокуудыг мөн өөрчлөх шаардлагатай болно гэсэн үг юм.



Зураг 3.10: Bitcoin блокын хялбаршуулсан загвар

Блокчэйн peer-to-peer сүлжээгээр холбогдоо загварчлагдсан байдаг, зангилаа буюу peer бүр блок болон арилжаанд суурилан бие биетэйгээ харьцана. Нэгэнт сүлжээнд холбогдсон бол зангилаанууд сүлжээн дэх бусад зангилаануудын мэдээллийн шидэж эхэлдэг, ингэснээр тархсан сүлжээнд зангилаанууд нэг нэгнээ олох арга хэрэгждэг. Сүлжээнд зангилаа байх зорилго нь биелэгдээгүй байгаа гүйлгээ болон дөнгөж олборлосон блокийг баталгаажуулах. Зангилаа үйл ажиллагаандaa орохоос өмнө эхлээд анхны блокийг татаж авах шаардлагатай. Анхны блокийг татаж авах нь шинэ зангилааг блок 1 - с хамгийн сүүлийн блок хүртэлх бүх блокийг татуулж баталгаажуулах бөгөөд энэ үйл ажиллагаа дууссанаар тухайн зангилааг синхрончлогдлоо гэж үзнэ.

3.2 Блокийн багтаамж

Блокийн хэмжээ ашиглагдаж буй технологиосоо хамаарч харилцан адилгүй байна. Иймд блокчэйний хамгийн том жишээ болох Bitcoin - оор жишээ авч тайлбарлай. Bitcoin сүлжээнд хийгдэж байгаа бүх гүйлгээ энэ сүлжээнд бичигдэж байдаг, нийтийн дансуудыг дурын этгээд харж болох ч хэн ч өөрчилж чадахгүй. Тэдгээр дансууд нь блокуудаас бүрдэх ба хоорондоо криптографаар нийцэн нийлдэг.

Bitcoin - ий блокчэйнийг бүрдүүлж байгаа блокуудын хэмжээ 1MB-р хязгаарлагдсан байдаг. Энэ хязгаар нь Bitcoin блокчэйнийг секундэд 7 хүртэлх гүйлгээ хийж чаддаг

3.2. БЛОКИЙН БАГТААМЖ

БҮЛЭГ 3. СУДАЛГАА

байх хэмжээ юм. Дунджаар 10 минут тутамд шинэ блок бий болдог боловч тэдгээр нь баталгаажаагүй байдаг.

Энэ хэмжээний хязгаарлалт нь Bitcoin протоколд хатуугаар кодчилогдсон байдаг бөгөөд энэ блок сүлжээг төвлөрсөн бус байх нөхцөлийг бүрдүүлдэг. Төвлөрсөн бус байдал гэдэг нь Bitcoin - ийг тогтвортой ажиллах түлхүүр нь юм. Том хэмжээтэй блок нь олборлогчдод хүнд ачаалал үүрүүлж, жижиг үйл хэмжээний олборлогчдыг шахан гаргах эрсдэлтэй.

Хэрэглэгч гүйлгээ хийх үед, гүйлгээ тухайн үед олборлогдсон блокт нэмэгдээд дараа нь тухайн блокийн удаах блокоор баталгааждаг. Гүйлгээний дээр олон блок нэмэгдэх тусам хувиршгүй байдал нь баталгаатай боллоо гэж үздэг. Гүйлгээ нь энгийнээр тухайн гүйлгээний хураангуйлсан мэдээллийн багц бөгөөд бусад мэдээллүүдийн адил блокт нэмэгдэхдээ тодорхой зاي багтаамж эзэлдэг.

Одоогийн байдлаар Bitcoin блокчэйний блок бүр 1MB хэмжээтэй мэдээллийг агуулах багтаамжтай байгаа нь Bitcoin - ий блокт хэдэн ширхэг гүйлгээний мэдээлэл багтах нь гүйлгээний мэдээлэл өөрөө хэр хэмжээтэй гэдгээс шалтгаалж хязгаарлагдмал гэсэн үг юм. Гэвч үргэлж ийм байгаагүй.

3.2.1 Блок хэмжээний асуудал

Bitcoin - ий эхэн үед блокийн хэмжээ нь хязгааргүй байсан. Гэсэн ч DOS(Denial Of Service) халдлагаар их хэмжээний блок дүүргэлт үүсгэх нөхцөлөөс сэргийлж блокийн хэмжээнд анх өөрчлөлт оруулсан. Ингэснээр жирийн хэрэглэгчид Bitcoin ашиглах хугацаанд ганц л түрийвч ашигладаг байсныг өмнө нь Bitcoin QT гэж нэрлэдэг байсан бол одоо Bitcoin Core гэж нэрлэх болсон. Үүнийг хэрэглэгч блокчэйнийг бүхлээр нь татаж авахад шаардагддаг бөгөөд энэ нь хэрэв хэрэглэгч томоохон хэмжээний блок үүсгэх бол, тухайн түрийвч ажиллаж байгаа энгийн компьютер хэзээ ч гүйцэхгүй бөгөөд энэ шалтгаанаар зарим хэрэглэгчид хэзээ ч bitcoin - oo зарцуулах боломжгүй болно гэсэн үг юм.

Өнөө үед маш олон хүн блокийн хэмжээг хязгаарлах нь одоо цагт ямар ч хэрэггүй ба ингэж хязгаарлах нь тухайн цахим мөнгийг нийтийн хэрэгцээнд хангалттай хургэж тэлэх боломжгүй болгож Bitcoin - ийг зарим талаар гэмтээж байгаа гэж үздэг. Одоогийн байдлаар Bitcoin секундэд 4-7 н гүйлгээг хийх боломжтой байгаа нь VISA болон PayPal зэрэг системтэй харьцуулахад тааруу үзүүлэлт юм.

Энэ асуудал Bitcoin хэрэглэгчдийн дунд багтаамжийн хязгаарлалтыг дэмжих болон үгүйсгэх байдлаар маш том маргааныг үүсгэсээр байна. Ихэнх нь блокийн багтаамжийг ихэсгэнээр Bitcoin олборлолтын төвлөрөлд нөлөөлж багтаамж ихсэхийн хэрээр олборлох төхөөрөмжийн шаардагдах хүчин чадал өснө гэж үзэж байгаа бол үлдсэн хэсэг нь багтаамжийг ихэсгэх нь Bitcoin - ийг бусад өргөн хэрэглээний төлбөрийн системүүдтэй өрсөлдөхүйц хэмжээнд хүргэнээ гэдэг талаас нь харж байна.

Эцэст нь зөвхөн олборлогчид болон бүр зангилаа хэрэглэгчид л coin - ийг үүсгэж гүйлгээг баталгаажуулж байгаа тул тэдэнд шийдвэр гаргах эрхтэй байдаг. Гэвч тэд дэлхийгээр тархсан, төвлөрсөн бус, мөн тэд ихэвчлэн хэн гэдэг нь ч мэдэгдэхгүй нууцлагдмал байдаг. Харин сүлжээний хэсэгт салаалалт үүсгэх болбол дийлэнх олборлогчид болон бүрэн зангилаанууд өөрчлөлтийг хүлээн зөвшөөрсөн байх ёстой.

3.2.2 Давуу тал

Блокийн хэмжээ их байх маш олон шалтгаанууд байдаг. Одоогийн блокийн хэмжээ Bitcoin - ийг зөвхөн 4-7 гүйлгээг нэг секундэд хийх хязгаартай болгодог. Ингэснээр жирийн хэрэглэгчдийн дунд яаралтай гүйлгээ хийх өрсөлдөөнөөс шалтгаалж гүйлгээний зардал өсөж яваандаа Bitcoin хангалттай алдартай болох үед зарим хэрэглэгчид сүлжээнээс шахагдан гарах нөхцөл үүснэ.

Блокийн хэмжээ ихэссэнээр хэрэглэгчид өндөр төлбөр төлөлгүйгээр олборлогчид илүү ашиг хүртэх боломжтой болно.

Түүнчлэн олон хүн блокийн хэмжээг ихсэх нь зангилаануудад маш их ачаалал нэмж, хадгалах төхөөрөмжийн багтаамж өндөр байхыг шаардана гэдгийг сануулж байгаа юм. Иймд блокийн хэмжээг нэг шөнийн дотор л экспоненциалиар өсгөхгүй ба, сүлжээнд хэрэгцээ гарахтай зэрэгцэн бага багаар ихэсгэх хэрэгтэй гэж үзэж байгаа.

3.2.3 Сул тал

Хэдий блокийн хэмжээ том байх хэрэгтэй гэдэгт олон хүн санал нэгтэй байгаа ч блокийн хэмжээг 1MB -д хязгаарлах нь зүйтэй гэж үзэх хуучинсаг үзэлтэй талд мөн л хангалттай үндэслэлтэй шалтгаан байгаа юм.

Бүрэн зангилаа хэрэглэгчдийн дунд зурвасын өргөний шаардлага байх бөгөөд энэ нь нэмэгдсээр бүрэн зангилааны тоо цөөрөх талтай.

Түүнчлэн сүлжээний хамрах хүрээг өсгөхөд заавал том хэмжээтэй блок, эсвэл хатуу

салаалалтын шаардлагагүй segwit, sidechain гэх зэрэг шийдлүүд байдаг тул блокийн хэмжээг ихэсгэх нь чухал биш гэж үзэх хүн олон байдаг.

Мөн Bitcoin - ийг хатуу салаалалтаар өөрчлөх нь тогтвортгүй байдал үүсгэх бөгөөд ингэж сүлжээг хувааснаар салаалсан хоёр блокчэйнд бэрхшээлтэй учрах зам болно гэж үздэг.

3.3 Блокчэйний хэрэглээ

Блокчэйн технологийг интернет хөгжлийн шинэ эрин үе гэж нэрлэх нэг чухал шалтгаан нь энэ технологийг чадлын цар хүрээ буюу маш олон төрлийн салбарт хувьсал хийх потенциал нь юм. Одоогоор блокчэйн технологи зөвхөн Bitcoin зэрэг цахим мөнгөний гүйлгээнд ашиглагдаж байгаа ч компьютер технологийн судлаач эрдэмтэд олон салбарт блокчэйн технологийн цар хүрээг судалсаар байна.

3.3.1 Худалдаа

Олон улсад худалдаа хийх бизнесийн үед хэд хэдэн хуулийн этгээдээс(гааль, боомтын удирдлага, ачааны тэрэг эсвэл төмөр замын төмөр замын фирмүүд гэх мэт) зөвшөөрөл авах шаардлага гардаг. Блокчэйнийг хуулийн этгээдүүд зөвшөөрөлд гарын үзэг зурах байдлаар ашиглах боломжтой бөгөөд ингэснээр бүх талын этгээдүүд зөвшөөрлийн статус, бараа бүтээгдэхүүн хүргэгдсэн эсэх, хүлээн авагч нийлүүлэгчид төлбөрөө төлсөн зэрэг мэдээллүүдийг авч болохоор болно. Эдгээр нь дараах давуу талтай :

- Тувэгтэй, олон процесийг энгийн бөгөөд дан ганц процесс болгоно
- Зохицуулалт эсвэл алдаа болон маргаанд зарцуулах хугацаа багассанаар үндсэн үйл ажиллагаанд анхаарал хандуулах боломж нэмэгдэнэ
- Хянагч, хэрэглэгч, байгууллага гурвын хооронд итгэлцэл болон хяналт, хариуцлагын түвшин нэмэгдэнэ.

3.3.2 Олон улсын гүйлгээ

Банкуудад *nostro/vostro* дансуудыг зохицуулах арга зам шаардлагатай байдаг. *Nostro*(бидний) гэдэг нь гадаадын банканд тухайн орны мөнгөн тэмдэгтээр хадгалагдаж буй дотоодын банкны дансыг илэрхийлдэг. *Vostro*(чиний) нь эсрэгээр гадаадын дансыг өөрийн

3.3. БЛОКЧЭЙНИЙ ХЭРЭГЛЭЭ

БҮЛЭГ 3. СУДАЛГАА

банканд хадгалахыг хэлдэг. Ийм төрлийн дансууд нь гадаад валиутын гүйлгээ болон арилжааг хялбаршуулан зохицуулахад ашиглагддаг. *Nostro/vostro* дансуудын гүйлгээ блокчэйнд хадгалагдсанаар автомат дансны зохицуулгаар шилэн байдал болон үр ашиг нь мэдэгдэхүйц нэмэгдэнэ. Үр ашиг нь :

- Банкуудын *nostro/vostro* дансуудын хооронд хийгдэж байгаа гүйлгээ ганц л интерфэйсээр зохион байгуулагдана.
- Гүйлгээний статус, одоогийн баланс, болон тухайн хугацаанд хийгдэж буй гүйлгээ зэрэг нь илүү тодорхой харагдана
- *Nostro/vostro* дансуудын хооронд тогтмол, цаг алдалгүй, үнэн зөв зураглал бий болно.

3.3.3 Даатгал

Даатгалын үйлчилгээ үзүүлэгчдэд нэхэмжлэлийн процесс, тухайн тохиолдол(осол аваар гэх мэт) - ийг даатгах нь зөв эсэхийг баталгаажуулах, мөн үйлчлүүлэгчид шударга бөгөөд цагаа олсон нөхөн төлбөр төлөх зэрэг үйл ажиллагааг үр ашигтайгаар хийх шаардлага байсаар байдаг. Автомат даатгалын нөхөн төлбөрийн боловсруулалт, гэрээний нөхцөл зэрэг нь ухаалаг гэрээнд бичиж блокчэйнд хадгалан Интернетэд бүгдэд нээлттэйгээр тавих боломжтой. Даатгал олгох шаардлагатай үйл явдал тохиолдож, итгэгдсэн эх сурвалжаас энэ талаар мэдээлэл аваад даатгалын гэрээ автоматаар ажиллаж ухаалаг гэрээнд бичигдсэн гэрээний нөхцөлөөр нэхэмжлэлийн процесс үйлдэгдэж, үйлчлүүлэгчид төлбөр очих болно.

- Даатгалын нэхэмжлэлийн үйл ажиллагааны зардал буурна
- Даатгалыг зальдах гэмт хэрэг буурна
- Хэрэглэгчийн сэтгэл ханамжийг нэмэгдүүлнэ

3.3.4 Эмнэлгийн цахим бүртгэл

Цахим эмнэлгийн бүртгэл нь одоогоор дата төвүүдэд хадгалагдаж байгаа бөгөөд хандалт нь эмнэлэг болон тусlamжийн төвүүдийн сүлжээгээр л хязгаарлагддаг. Энэ төрлийн мэдээллийг төвлөрүүлэх нь аюулгүй байдлын хувьд эмзэг, өртөг өндөртэй байдаг.

3.3. БЛОКЧЭЙНИЙ ХЭРЭГЛЭЭ

БҮЛЭГ 3. СУДАЛГАА

Блокчэйн эмчлүүлэгч бүрд эмчилгээний түүхийг эмч, хянагч, эмнэлэг, даатгал зэрэг бүхий л мэдээлэлтэй нь аюулгүй механизмаар бичиж хадгалах боломжтой болгоно. Ингэж хадгалснаар :

- Θвчтөний түүхийг хуурамчаар үйлдэхээс сэргийлиэ
- Даатгалын нэхэмжлэлийг бодитой бөгөөд хурдан үүсгэх, даатгалын нөхөн олговрыг үр ашигтайгаар хүртээх
- Θвчтөний түүхээс эмийн санчид тохирох эмийг олгоход хялбар болно

3.3.5 Зүйлсийн интернет(IoT)

Машинуудын хоорондын харилцаатай холбоотой аль төрлийн харилцааг Блокчэйнд бичилт хийж үр ашиг болон найдвартай байдлыг дээшлүүлж зардлыг багасгах боломжтой. Солилцооны логистикийн хэрэгцээг IoT-н үйл ажиллагааг автоматжуулахаар блокчэйнд оруулж болно.

Одоогоор тээврийн логистикуудад маш олон төрлийн этгээдүүд оролцож байна. Үүнд үйлдвэрлэгчид, дамжуулагчид, тээвэрлэгчид, гаалийн байгууллага мөн даатгалын байгууллагууд орно. Түүнчлэн тэдгээр оролцогч талууд хэдий өөр өөр зорилготой, өөр өөрийн үүрэгтэйгээр оролцож байгаа ч нэг нэгтэйгээ байнгын харилцаатай бөгөөд нэг нэгээсээ хамааралтай ажилладаг. IoT - н хувьд блокчэйнийг идэвхжүүлснээр нийтийн данс маягаар чингэлэгүүдийг нэг системээр гүйж байгаа мэт тээвэрлэх болно. Ухаалаг гэрээ нь IoT - н сангаар автоматаар шинэчлэгдэж блокчэйнт олон улсын тээврийн IoT болж тохируулагдаж болно. Энэ тохиолдолд :

- Тээвэрлэлтийн процесс шилэн болсноор үр ашиг нэмэгдэнэ
- Гүйлгээ найдвартайгаар бичигдсэнээр итгэлцэл нэмэгдэнэ
- Цагийн хуваарь нарийвчлагдаж IoT ашигласны зардал багасна
- Оролцогчид IoT - р бизнесийн үйл ажиллагаагаа автоматжуулах болон тохируулах боломжтой болно

3.4 Bitcoin-ий нийтлэг буруу ойлголтууд

Хүмүүс үргэлж шинэ зүйлд эргэлзээтэй ханддаг, нэн ялангуяа ойлгоход бэрхшээлтэй зүйлүүдэд. Иймд Bitcoin яахын аргагүй энэ дэлхийд урьд өмнө үзэгдээгүй шинэ мөнгөн тэмдэгт тулд хүмүүсийг эргэлзүүлж, хэд хэдэн буруу ташаа ойлголт үүсгэж байгаа нь энгийн үзэгдэл юм.

Тэдгээр Bitcoin - ий талаарх ташаа ойлголтоос жишээ болговоос:

- **Bitcoin халдлагад өртөж байсан :** Одоогийн байдлаар Bitcoin - ийг амжилттай хакдаж bitcoin хулгайлж авсан тохиолдол нэг ч гараагүй. Гэсэн хэдий ч Bitcoin - ийг ашигладаг төвлөрсөн системүүд халдлагад өртсөн тохиолдол олон гарсан. Мөн турийвч болон Bitcoin арилжааны сайтууд аюулгүй байдлаа сайн хангаагүйгээс халдлагад өртөх тохиолдол өргөн гардаг. Bitcoin - ий нийгэмлэгийн зүгээс дээрх асуудалтай тэмцэхээр турийвч шифрлэлт, олон гарын үсэг, оффлайн турийвч, цаасан турийвч, техник хангамжит турийвч зэрэг coin - уудыг аюулгүй байлгах олон шийдлийг хөгжүүлсэн.
- **Bitcoin - г ашиглаж хүмүүсийн мөнгийг хулгайлж байна :** Bitcoin - ний хагас нэргүй(semi-anonymous) шинж нь ransomware халдлагад ашиглагдах тохиолдол их гарч байна. Сургууль болон эмнэлгийн байгууллагууд ихэвчлэн энэ төрлийн халдлагын хохирогч болдог. Гэсэн хэдий ч бэлэн мөнгтэй адилгүй нь блокчэйнд үргэлж ул мөр үлддэг тул мөрдөгчдөд мөшгөх боломжтой байдаг.
- **Bitcoin нь пирамид систем :** Bitcoin олборлогчдын өнцгөөс харвал Bitcoin нь харин ч пирамид системийн эсрэг зүйл юм. Bitcoin протокол нь өөрийгөө иддэг зарчимтай юм шиг загварчлагдсан. Нэмж орсон олборлогч бүр олборлох ачааллыг(difficulty) - г нэмэгдүүлдэг. Нийгмийн өнцгөөс харвал Bitcoin нь цэвэр арилжаа юм. Bitcoin - ий ханш нь худалдааны эрэлт, нийлүүлэлт, үнэлэгдсэн утга зэргээсээ хамаарч хэлбэлздэг.
- **21 сая coin олборлогдсоны дараа Bitcoin үгүй болно :** Bitcoin - д гарах токений тоо хязгаартай байдаг. Энэ тоо нь 21 сая байхаар хатуу кодлогдсон. Баргцаалсан хугацаагаар хамгийн сүүлийн coin 2140 онд олборлогдож дуусна гэсэн таамаг байдаг. Хэн ч тэр үед юу болохыг таамаглаж чадахгүй байгаа ч, олборлогчид үргэлжид гүйлгээний төлбөрөөс ашиг хүртсээр байх юм. Түүнчлэн хэрэв

олборлолт зогсвол bitcoin эмзэг болж, мэдээллүүд ч блокчэйндээ түгжигдэх тул блокчэйний хэрэглэгчид болон Bitcoin өөрсдөө сүлжээгээ хамгаалхын тулд ажилласаар байх болно.

- **Хангалттай хүчирхэг тооцооллын хүчээр Bitcoin сүлжээнд халдаж болно :** Энэ хэдий үнэн боловч энэ маш хүндрэлтэй байхаас гадна тухайн үйл ажиллагаанд бараг л ашиг байхгүй. Илүү олон зангилаа байх хэрээр Bitcoin сүлжээ төдий чинээ халдлагад тэсвэртэй байдаг. Үүнийг давж гарахын тулд халдагчдад Ирланд улс дахь бүх эрчим хүчний үйлдвэрлэлтэй тэнцэхүйц хэмжээний эрчим хүч шаардагдана. Мөн энэ төрлийн дайралтаас гарах үр ашиг нь хязгаарлагдмал. Халдлага амжилттай боллоо гэхэд ердөө өөрийн гүйлгээгээ л буцаах боломжтой болно. Хэн нэгний Bitcoin-ийг хулгайлах эсвэл хуурамч гүйлгээ юм уу coin үүсгэх боломжгүй.
- **Bitcoin бол сайн хөрөнгө оруулалт :** Bitcoin нь хүмүүсийн валиут солилцох соёлд шинэ бөгөөд маш сонирхолтой хувьсал болсон. Мөн ямар ч засгийн газар эсвэл байгууллагын харьялал дор байдаггүй ба хүмүүс үүнийг ямарваа бараа материал болон үйлчилгээ худалдаж авахад ашиглаж байгаа болохоор л өөрийн гэсэн үнэлгээтэй болсон. Хүмүүсийн Bitcoin хэрэглэх хүсэл сонирхол үргэлжийн хэлбэлзэлтэй байгаа. Иймд Bitcoin нь хянуур байх шаардлагатай тогтвортгүй хөрөнгө оруулалт юм.

3.5 Bitcoin ба залилан

Bitcoin - ний ертөнц яг л Зэрлэг Америкийн эхэн үеийг санагдуулж байна. Хэнийг сайн залуус хэнийг муу залуус гэдгийг болгоомжтойгоор олж мэдэж сурх нь чухал. Хэрэв чи занганд нэгэнт орвол бараг л гарыгүй болно.

Энэ хэсэгт криптовалиутын ертөнцөд хамгийн түгээмэл тохиолддог турван залилангийн тухай тайлбарлая. Тэд бүгд чиний coin-уудыг хулгайлах зорилготой бөгөөд яг л уламжлалт залилагчид шиг мэргэжлийн аюулгүй мэт харагдана.

3.5.1 Хуурамч сайтууд

Зарим Bitcoin арилжааны болон веб түрийвчийн томоохон сайтуудыг дуурайлгасан хуурамч сайтууд байдаг. Энэ төрлийн залилан Bitcoin ертөнцөд их өргөн тохиолддог.

Залилагчид хохирогчдын оруулсан нэвтрэх эрхийн мэдээллийг хулгайлах эсвэл тэднийг алдуулж өөрсдийн дансанд Bitcoin илгээлгэх замаар мөнгө олох гэж оролддог.

Энэ асуудалд өртөхгүйн тулд үргэлж URL - ийг нягтлан шалгаж байх хэрэгтэй ба, зөвхөн secure веб(<https://> - р эхэлдэг вэбүүд) ашиглах хэрэгтэй. Хэрэв вебсайт болон нэхэмжлэл эргэлзээтэй санагдвал, тухайн сайтыг [Badbitcoin.org](http://www.badbitcoin.org)(www.badbitcoin.org) - ийн жагсаалтад бүртгэгдсэн байгаа эсэхийг шалгах хэрэгтэй. Энэ хэдий бүрэн төгс жагсаалт биш ч, маш олон тооны залилагчдыг бүртгэсэн байгаа.

3.5.2 Эхлээд мөнгөө явуул!

"Эхлээд чи Bitcoin - oo илгээ, тэгээд би барааг чинь илгээх болно". Энэ үг сэжигтэй байгаа биз? Энэ төрлийн залилан нь мөнгө шилжүүлгийн залилантай төстэй бөгөөд хэн нэгэн бараа худалдах гэж буй мэт дүр үзүүлж төлбөрийг авах боловч бараа нь хэзээ ч ирэхгүй юм.

Bitcoin - ий хагас нэргүй(semi-anonymous) шинж болон төлбөр буцаагдах боломжгүй байдал нь нийлээд залиланд хохирсон тохиолдолд эргэж хохирлоо барагдуулахад маш хүндрэлтэй болгож байгаа юм. Түүнчлэн засгийн газар Bitcoin - ий гүйлгээг хамгаалах ямар ч арга хэмжээ авдаггүй тул голыг сэлүүргүй туулж гарах нь өөрөөс таньл хамаарах юм.

Залилагчид таны итгэлийг олохын тулд хуурамч биеийн байцаалт үзүүлэх эсвэл бүр таны таньдаг байж болох хүнийг ч дуурайх оролдлого хийнэ. Тэдний илгээсэн мэдээллийг үргэлж давхар шалгаж байх хэрэгтэй.

Энэ төрлийн залилангаас сэргийлэх хамгийн сайн арга нь үргэлж зөн совингоо дагах ба хэзээ ч алдахад харамсахгүй байхаасаа илүү Bitcoin - ийг бүү эрсдэлд оруул. Хэрвээ оффлайн орчинд тухайн хүний биеийн байцаалтыг шалгах боломжтой бол тэгж шалгасан нь найдвартай.

3.5.3 Хурдан баяжих арга

Криптовалиутын өртөнцөд хурдан баяжих схем маш эрчимтэй дэлгэрч байна. Сайн мэдээ нь хэрвээ чи юу хайж байгаагаа мэдэж байвал залилан гэдгийг нь маш амар мэдэх боломжтой.

Ихэвчлэн тэд маш өндөр хэмжээний буцаан олголт амладаг бөгөөд зарим төрлийн хүн элсүүлэх процесс явагддаг. Энэ процесс нь сүлжээний бизнестэй адилаар гэр бүл

эсвэл найз нөхдөө доороо элсүүлэхийг асууж эхлэх ба энэ нь ямар ч эрсдэлгүй хөрөнгө оруулалт бөгөөд таныг хэзээ ч мөнгөө алдахгүй хэмээн амлах болно.

Хэчинээн тухайн схем яг л үнэн мэт санагдах, магадгүй үнэн байсан ч тухайн байгууллага хөрөнгө оруулалтаасаа танд буцаан олголтоос гадна өөрсдөө хэрхэн ашиг олж байгааг няхуур хянаж үзэх хэрэгтэй. Хэрэв тэдний олох ашиг хөрөнгө оруулагчдын буцаан олголт хоёрын харьцаа нэг л ойлгомжгүй байвал, энэ нь залилан юм.

Хөрөнгө оруулалтаа хуульчид болон мэргэшсэн нягтлан бодогчдын дор хийж бай. Тэд танд ямар эрсдэлд хүрч болох болон татварын тухай ойлгоход туслах болно.

3.6 Bitcoin олборлолт

Bitcoin - г олох олон төрлийн арга байдаг. Bitcoin олборлох нь сүлжээнд оролцсоноор Bitcoin олж байгаа ажил юм. Ихэвчлэн үнэтэй бөгөөд тусгайлан бэлтгэгдсэн төхөөрөмжөөр хийгддэг. Энэ төхөөрөмж нь мөн блокчэйн ба олборлох pool(олон тооны олборлогчид нэг ажилд хамтран ашигаа хувааж авах нэгдэл) - д холбогдох зориулалт бүхий Bitcoin олборлох програмтай байх хэрэгтэй.

- **Bitcoin-QT** : Bitcoin-QT нь Satoshi Nakamoto - н өөрийн бичсэн анхны програм. <https://bitcoin.org/en/download> - с татаж авч болно.
- **CGminer** : CGminer хамгийн алдартай олборлох програмуудын нэг. Нээлттэй эхийн програм бөгөөд Windows, Linux үйлдлийн системүүдэд ажиллах боломжтой. www.github.com/ckolivas/cgminer - с татаж авна.
- **Multiminerapp** : Multiminerapp нь ашиглахад хялбар клиент. www.multiminerapp.com - с татаж авах боломжтой.

Bitcoin нь маш өрсөлдөөнтэй орчин бөгөөд хэрэв тусгай бэлтгэгдсэн төхөөрөмж авахаас өөрөөр Bitcoin олох боломжгүй юм. Тухайн төхөөрөмжууд нь дунджаар 500 - 5000 \$ - ийн өртөгтэй байдаг. Amazon.com нь энэ төрлийн төхөөрөмж хайхад зохимжтой ба маш олон төрлийн олборлох төхөөрөмжийн сонголттой бөгөөд худалдан авагчдын сэтгэгдлүүдээс санаа авч сонголт хийх нь зүйлтэй юм.

3.6.1 Cloud олборлолт

Cloud олборлолт нь хэрэглэгчийг заавал төхөөрөмж худалдан авч програм хангамж татах шаардлагагүйгээр ажлын өдөрт л Bitcoin олж эхлэх боломж олгоно. Олон төрлийн cloud олборлолт хийх платформууд байх бөгөөд дараах сайтаар жишээ авч cloud олборлолт хийх дарааллыг үзүүлэв:

1. **<https://hashflare.io/panel> - руу орно.**

Cloud олборлолтын ашиг нь хөрөнгө оруулалтаасаа бага байх тохиолдол бий. Иймд аль платформыг хянуур сонгох нь ашигтай ажиллах суурь болно.

2. **Нүүр хуудсыг доош гүйлгэн SHA-256 Cloud Mining - ийн дор байрлах Buy Now товч дээр дарна.**

Энэ хэсгийг бичиж байх үед энэ сонголт нь хамгийн бага хөрөнгө оруулалтаар хамгийн өндөр ашиг өгөхөөр байна. Гэвч энэ нь өөрчлөгдөх магадлалтай тул хянуур байх нь зүйтэй.

3. **Бүртгүүлэх үйл ажиллагаанд орно.**

4. **Bitcoin хаягаа холбоно.**

Хэрэв Bitcoin хаяггүй бол дараагийн хэсэгт хэрхэн Bitcoin түрийвч нээх тухай бичсэн байгаа. Bitcoin түрийвч байж олборлолтын ашгаа хүлээн авах юм.

5. **Бага хэмжээний олборлох чадал худалдаж ав.**

Ингэснээр bitcoin - ий сүлжээнд холбогдох болно.

6. **Олборлолтын pool-д нэгд.**

Энэ чамд олборлолтын ашгаа ганцаараа олборлосноос хурдан авах боломжийг олгоно.

Баяр хүргэ! Одоо хойшоо суугаад олборлолтын ашиг орж ирэхийг хүлээж сууж болохоор боллоо.

3.7 Bitcoin цаасан түрийвч үүсгэх

Цаасан түрийвч гэдэг нь Bitcoin - ий нийтийн болон хувийн түлхүүрээ цаасан байдлаар хадгалж авахыг хэлнэ. Ингэж хадгалах нь бүрэн онлайн тул, хэрэв зөв хийж чадвал

3.7. BITCOIN ЦААСАН ТҮРИЙВЧ ҮҮСГЭХ

БҮЛЭГ 3. СУДАЛГАА

Bitcoin - oo хадгалах хамгийн найдвартай аргуудын нэг юм. Давуу тал нь хувийн түлхүүрээ цахим орчинд хадгалахгүй тул хакеруудын бай болох эрсдэлээс хамгаалагдана. Цаасан түрийвч үүсгэх нь хялбар бөгөөд доорх дарааллаар үүсгэж болно:

1. www.bitaddress.org - руу орно. (Зураг 3.11)
 2. Хулганы сумыг санамсаргүй байдлаар 100% болтол нь гүйлгэнэ. (Зураг 3.12)
 3. Paper Wallet товч дээр дарна.(Зураг 3.13)
- Ингэж дарснаар хэвлэж авах боломжтой цаасан түрийвч үүсгэх боломжтой болно.
4. Addresses to Generate хэсгээс 1 гэдгийг сонгоно. (Зураг 3.14)
 - Хэрэгтэй бол нэг дор хэд хэдэн түрийвч үүсгэж болно.
 5. Generate товч дээр дарна. (Зураг 3.15)
 6. Print товч дээр дарна. (Зураг 3.16)

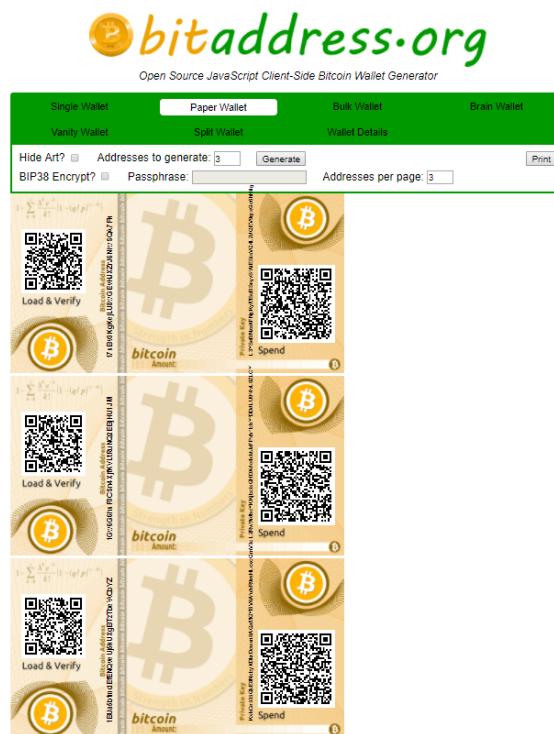


Зураг 3.11: www.bitaddress.org

Үүсгэсэн түрийвчээ бусдад харуулах эсвэл түрийвч үүсгэх процесийг нийтийн компьютерт хийх нь зохимжгүй үйлдэл юм. Мөн хэвлэн принтерээ интернет холболтоор салгаж хувийн тохиргоонд тохируулснаар хувийн түлхүүрээ хакеруудад алдах эрсдэлээс сэргийлнэ.



Зураг 3.12: Хулганы сумыг санамсаргүй гүйлгэнэ



Зураг 3.13: Print wallet



Зураг 3.14: Generate 1



Зураг 3.15: Generate



Зураг 3.16: Print

3.8 Ethereum

Ethereum нь өнөөдрийн байдлаар магадгүй хамгийн цогц бүтэцтэй блокчэйнд тооцогдож байна. Өөртөө Turing-complete гэж програмчлалын хэлтэй (хөгжүүлэгчдийг ямар ч төрлийн апликацийн хөгжүүлэх боломжоор хангасан бүрэн үйлдэлтэй програмын хэл). Ethereum нь протокол нь дундаж програмчлалын хэлний хийж чадах бүхий л зүйлсийг хийж чадахаас гадна блоцхэйний дотор суурилсан тул аюулгүй байдлын ашиг тус нэмэгдсэн.

Ethereum - н экосистем нь одоогоор тархсан апликацийн бүтээх хамгийн сайн платформ болж байна. Гайхалтай баримтжуулалт болон хэрэглэгчид ээлтэй интерфейс ажлын бүтээмжийг нэмж шуурхай ажиллах боломж олгоно. Шуурхай хөгжүүлэх хугацаа,

жижиг апликацийний аюулгүй байдал, апликаційн тэй харьцах байдал нь хялбар зэрэг нь энэ системийн түлхүүр шинж юм.

Turing-complete програмчлалын хэл нь Ethereum - ийг шинэ програм бичих тал дээр Bitcoin - оос хавгүй илүү хүчирхэг байх үндсэн онцлог нь болдог. Ethereum - н скрипт хэл нь Twitter апликаційн шиг програмыг хамгийн бага мөр кодоор маш өндөр түвшний хамгаалалттайгаар бүтээнэ. Smart contract - уудыг мөн Ethereum дээр бүтээдэг. Ethereum протокол нь апликацийний цоо шинэ төрлийг нээсэн. Та ямар ч төрлийн бизнес, засгийн газар болон байгууллагын үйл ажиллагааг сонгон авч цахим дүрслэлийг нь Ethereum - д бүтээж болно.

3.8.1 Тархсан апликаційн

Ethereum - н хамгийн хувьсал хийсэн бөгөөд маргаантай тодорхойлолт бол өөрийгөө удирдах, тархсан апликаційн (DAPP) юм. DAPP нь цахим хөрөнгө болон DAO зэргийг удирдаж зохион байгуулах чадвартай.

DAPP нь төвлөрсөн хөрөнгө болон байгууллагуудыг орлох зорилготойгоор бүтээгдсэн. Энэ санаа нь хүмүүсийн анхаарлыг маш их татаж байгаа бөгөөд олон хүн үүгээр засгийн газар зэрэг үнэмлэхүй хүчийг унагаж болно гэж итгэж байгаа юм.

Etheria (www.etheria.world) нь Minecraft - тай ижил төстэй тоглоом бөгөөд энэ нь энэ технологийн ажиллагааг харуулсан сонирхолтой жишээ юм. Энэ тоглоом нь Ethereum оршин тогтнож байгаа цагт аль нэг газраас хянагдах эсвэл хаагдах боломжгүй юм. Хэрэв ямар нэг зүйл Ethereum - д бүтээгдвэл энэ нь аль нэг байгууллагын шаардлагаар устгдах хангалттай шалтгаантай байсан ч практикийн хувьд боломжгүй зүйл юм.

3.8.2 Decentralized autonomous organization (DAO)

DAO нь Ethereum дахь виртуал аж ахуйн нэгжийг илэрхийлсэн нэг төрлийн Ethereum апликаційн юм. DAO - г бүтээснийхээ дараа байгууллагынхаа захиргаанд бусдыг оролцогчоор урьж болдог. Оролцогчид нь нэргүй бөгөөд бие биетэйгээ хэзээ ч уулзаагүй байж болно

DAO хөрөнгө оруулалтад мөнгө босгохоор бүтээгдсэн, гэсэн ч сайн дурын болон ашгийн бус зорилгоор ашиглагдах боломжтой. Ethereum - аар мөн аливаа удирдлагын түвшний програмын загварыг гаргаж болно. Харин юуг удирдах вэ гэдэг нь тухайн байгууллагын тодорхойлох ажил болно.

Зураг 3.17: www.etheria.world

DAO - н ерөнхий ажиллагаа :

1. Байгууллагын үйл ажиллагаанд зориулсан smart contract - г бичнэ
2. DAO - д хүмүүс хөрөнгө оруулж, өмчлөх эрхийг илэрхийлсэн токен ана. Энэ загвар нь компанийн хувьцааны үйл ажиллагаатай төстэй боловч гишүүд хөрөнгийн удирдлагад эхний өдрөөсөө оролцдогоороо төстэй.
3. Хөрөнгө оруулалт хангалттай өсөж эхэлмэгц DAO гишүүддээ хэрхэн мөнгөө зарцуулах саналуудыг тавьж эхэлнэ
4. Гишүүд өгөгдсөн саналуудад санал хураалт явуулна
5. Урьдчилан тохирсон хугацаа өнгөрч, хангалттай тооны гишүүд саналаа өгмөгц оруулсан саналыг дэмжих дэмжигдэхгүй нь шийдэгдэнэ.
6. Гишүүд DAO - н үйлчилгээнд хамтран ажиллагч мэт оролцно

Уламжлалт хөрөнгө оруулалтын системээс ялгаатай нь зөвхөн удирдах зөвлөл хөрөнгө оруулалттай холбоотой шийдвэрийг гаргах бус DAO - н гишүүд хөрөнгөө 100 хувь удирдана. Тэд бүгд санал хураалтаар шинэ хөрөнгө оруулалт болон бусад шийдвэрийг гаргадаг. Энэ төрлийн үйл ажиллагааны загвар нь уламжлалт санхүүгийн удирдлагуудыг шахан гаргах аюул үүсгэж байна.

DAO нь үйл ажиллагааны явцад өөрчлөгдөхгүй кодоор бичигддэг. Ингэснээр хакерууд хөрөнгөтэй холбоотой асуудалд хуучныхаа аргаар асуудал үүсгэх боломжгүй

болж байгаа юм. Хакерууд ямар ч тохиолдолд хэний ч санаагүй аргаар кодод нөлөөлж хөрөнгө татах арга олчихсон л байдаг. DAO - н кодын хувиршгүй шинж нь DAO нэгэнт Ethereum - д орсон тохиолдолд ямар ч алдааг засах боломжгүй болно.

3.8.3 Блокчэйнийг хакдах нь

Ethereum өнөөдрийг хүртэл нэг ч удаа халдлагад өртөж байгаагүй. 2016 онд тохиолдсон DAO хак нь үнэндээ Ethereum системд тохиолдсон хак байгаагүй бөгөөд, хүмүүс ихэвчлэн Ethereum хакдуулсан гэж ойлгодог. Ethereum нь үнэхээр төгс ажиллагаатай. Асуудал нь энэ төгс байдлаас үүсдэг. Хэрэв их хэмжээний мөнгө болон хэрэглэгчдийнх нь дийлэнхи нь аюул заналд өртвөл тухайн системийг тэр чигт нь дахин ачааллах шаардлагатай болдог.

Ethereum шиг блокчэйний үйл ажиллагааг засаж сайжруулах ганцхан гарц нь хатуу салаалалт(hard fork) буюу протоколын суурьт өөрчлөлт оруулах юм. Хатуу салаалалт нь өмнөх баталгаажсан блок болон гүйлгээний баталгаажилтыг цуцалдаг. Ethereum энэ ажиллагааг халдагч DAO - с татаж авах гэж буй мөнгийг хамгаалахын тулд хийдэг. DAO хак нь одоогоор хамгийн их ашиг олсон халдлага болсон.

Ихэнх залилан болон хакдах оролдлогууд нь криптовалиутын орчинд хийгддэг. Эдгээр халдлагуудын ихэнх нь аппликэйшн болон төвлөрсөн арилжааны системд чиглэсэн байдаг. Тэнд л жинхэнэ хөрөнгийн утга байх бөгөөд энгийн мөнгөтэй адил засгийн газраас ямар нэг хамгаалалт авдаггүй. Мөн криптовалиутын нэргүй шинж нь залилан үүсэх нөхцөлийг нэмдэг. Тэдгээр залилагчийг мөрдөж олж авах туйлын хэцүү. Криптовалиутын нийгэмлэг нь үүний эсрэг тэмцдэг бөгөөд өөрсдийгөө хамгаалах шинэ хэмжигдэхүүн бүтээхээр ажилладаг.

Нэг газрыг халдахаар оролдох нь тархсан сүлжээг бүхэлд нь халдахаас харьцангуй хялбар бөгөөд зардал багатай. Хэрэв та хaa нэгтээ блокчэйний өртөнцөд халдлага гарсан тухай олж мэдвэл энэ нь ердөө вебсайт эсвэл криптовалиутын түрийвч халдагдсан тухай мэдээлэл байхаас сүлжээ тэр чигтээ халдагад өртсөн тухай биш юм.

3.8.4 Smart contract

Ethereum - н smart contract гэдэг нь яг л гэрээний заалт шиг бөгөөд ялгаатай нь үүнд тухайн заалтыг мөрдүүлж байх төвлөрсөн удирдлага байхгүй. Ethereum протокол нь эдийн засгийн шахалт үзүүлэх замаар smart contract - г мөрдүүлдэг. Мөн Ethereum

сүлжээнд оролцоход шаардагдах хэрэгжилт болон шаардлагуудыг мөрдүүлдэг.

Etehreum smart contract нь хууль ёсны журам мөрдүүлэгч биш юм. Учир нь хэрэглэгчдэд ямар нэг гуравдагч журам мөрдүүлэгч шаардлагагүй бөгөөд хууль ёсны систем зөвхөн засгийн газраар удирдагддаг. Засгийн газар нь төвлөрсөн эрх мэдэл бүхий байгууллага бөгөөд заримынх нь ардчилсан зарчим нь өөр тул тохиролцоонд хүрэх нь янз бүр. Ethereum - н smart contract - тайгаар оролцогч бүр санал оруулах эрхтэй.

Ethereum smart contract - ийг 100 хувь агуулгүй гэж ойлгох нь ташаа юм. DAO хак нь энэ технологид эрсдэлд үүсэж болно гэдгийг харуулсан хамгийн том жишээ юм. Энэ технологи нь хөгжлийнхөө дөнгөж эхэн үедээ байгаа бөгөөд хүчин чадал нь төдий нотлогдоогүй байгаа энэ системд их хэмжээний хөрөнгө оруулах нь тийм ч ухаалаг алхам биш юм. Үүний оронд, бага багаар туршиж, шинэ contract - г алдаагүй болгох хөгжилд хувь нэмэр оруулах нь чухал байна.

3.8.5 Ether криптовалиут

Ether нь Ethereum блокчэйн дэх криптовалиутын нэр юм. Ether нь proof-of-work олборлолтоор сүлжээгээ найдвартай байлгахад олгох урамшуулал юм, энэ нь Bitcoin олборлогчдод урамшуулал болгон олгодог токентой адил. Ethereum сүлжээнд аливаа код ажиллахад Ether шаардагддаг. Ethereum - д contract хийдгэхэд, Ether - г gas fee(шатахууны төлбөр) байдлаар ашиглана. Хэрэглэгч Ethereum аппликэйшион болон contract - г ашиглаж л байгаа бол ether - т өөрийн ханш байсаар байх болно.

Ether - н ханш өсөлт нь ethereum - г алдаршихад нөлөөлсөн. Энэ токен дэлхий даяар маш өргөн арилжаалагддаг. Зарим шинэ хөрөнгө оруулалтын сангүүд үүнийг хөрөнгө оруулалтын машин мэтээр хаарж байна. Гэсэн ч хэлбэлзэлтэй шинж болон зах зээлд эзлэх хэмжээ нь багаас шалтгаалж ether нь эрсдэлтэй хөрөнгө оруулалтад тооцогдоно.

3.9 Etehreum дээр ажиллах

Энэ бүлэгт Ethereum платформд үйл ажиллагааг хэрхэн эхлэх тухай бичлээ. Ethereum -д аль ч зүйлийг эхэлсэн, хамгийн эхэнд Ethereum турийвчтэй байх шаардлагатай.

Ethereum турийвч нь ether токенийг хадгалана. Ethereum турийвчийг татаж авах нь тодорхой хугацаа шаарддаг ч интерфэйс нь маш ойлгомжтой бөгөөд үйл ажиллагааны зааварчилгааг дагаж ажиллахад хялбар.

Ethereum түрийвчтэйгээр тестийн ether авч байгууллагын contract - аа туршиж болно. Яаж ажилладгийг нь мэдэхийн тулд заавал олборлолт хийх шаардлагагүй.

3.9.1 Ethereum олборлолт

Ethereum - д дэлхий даяар тархсан компьютерууд contract болон сүлжээг хамгаалах байдлаар ажилладаг. Тэдгээр компьютеруудыг зангилаа гэж дуудах бөгөөд Ether криптовалиут олборлодог.

Зангилаа хэрэглэгчид олборлолтод хэр хугацаа болон хувь нэмэр оруулснаас хамаарч урамшуулал олгодог. 12 секунд тутамд таван ether урамшуулал болж олгогддог. Урамшуулал нь Ethereum блокчэйний хамгийн сүүлийн блокийг үүсгэсэн хэрэглэгчид очдог.

Шинэ блок бүр сүүлд хийгдсэн гүйлгээний жагсаалттай байдаг. Proof-of-work тохиролцооны алгоритм нь хамгийн их тооцооллын хүч гаргасан компьютер хамгийн их урамшуулал авах нөхцөлийг баталгаажуулна. Мөн бага хэмжээний хүчтэй компьютер ч урамшуулах авах бөгөөд өндөр хүчин чадалтайг бодвол удаан юм. Хэрвээ та Ethereum олборлолтод оролцохыг хүсвэл өөрийн хувийн компьютероор ч хийж болох боловч нэг бүтэн блокийг амжилттай олборлож урамшуулал авахад маш их хугацаа шаардана.

Ether олборлох нь техник дөнгөж сонирхож эхэлж байгаа хүний хийх ажил биш юм. Олборлолт хийхийн тулд наад зах нь command line - д ажиллаж чаддаг байх хэрэгтэй. Хэрвээ command line - ий талаар ямар ч ойлголтгүй бол магадгүй энэ л таны шантрах цэг болж мэдэх юм. Харин олборлолт хийхээр шийдсэн бол Ethereum GitHub(<http://github.com/ethereum>) дахь хамгийн сүүлийн үеийн зааварчилгааг дагахыг зөвлөж байна.

3.9.2 Ethereum түрийвч үүсгэх

Ethereum түрийвчтэй болохын тулд дараах зааврын дагуу ажиллана:

1. www.ethereum.org - руу орно
2. Download товч дээр дарна

Download товчийг олохын тулд нүүр хуудсыг доош нь гүйлгэх шаардлагатай.

3. Ethereum wallet - г нээнэ

4. Uset Net Test дээр дарна

Энд та test ether - г туршиж болно. Энэ нь амьдрал дээрх жинхэнэ олборлолттой харьцуулахад хурдан боловч тодорхой хугацаа шаардана.

5. Хүчтэй нууц үг сонгох хэрэгтэй

Сонгосон нууц үгээ аюулгүй газар хадгалах хэрэгтэй

6. Startup menu дээр дарна

Ethereum test net - г татаж байх хугацаанд үзэж сонирхохоор хэд хэдэн зөвлөмжүүдийг дэлгэцэд үзүүлнэ. Татах хугацаа ойролцоогоор 10 минут хэртэй үргэлжилнэ.

7. Develop => Start mining - г сонгоно

Энэ алхмыг бүү алгас. Учир нь дараа дараагийн проектод ether хэрэг болно
Ингээд ether түрийвчээ үүсгэлээ, одоо ирээдүйн smart contract төслүүдээсээ test ether олох боломжтой боллоо.

3.10 Өөрийн анхны Decentralized autonomous organization бүтээх нь

DAO нь ирээдүйд дэлхий дахин хэрхэн бизнес явуулдаг зарчмыг өөрчлөх болно. Дэлхийн аль өнцгөөс хэн ч шинээр компани үүсгэж байгуулж, тэр нь урьдчилан тохиролцсон(ree-ager-on) дурмээр зохицуулагдаж, тэр дүрэм нь блокчэйн сүлжээнд мөрдөгдөх боломжтой болно. DAO - г бүтээх нь магадгүй таны бодож байгаагаас ч хялбар ажил юм. Энэ бүлэгт та хэрхэн өөрийн анхны DAO - г турших тухай бичлээ.

DAO - гоо амжилттай бүтээж туршихын тулд эхлээд Ethereum түрийвч үүсгэсэн байх хэрэгтэйгээс гадна тодорхой хэмжээний Ethereum test net олборлолт хийсэн байх шаардлагатай.

1. www.ethereum.org/dao - руу орно
 2. Хуудсыг доош гүйлгэн Code box хэсэгт очих бөгөөд тухайн кодыг сору хийж авна.
 3. Өмнөх бүлэгт хийсэн Ethereum түрийвчээ нээнэ
- DAO - гоо Ethereum түрийвч дотроо хөгжүүлнэ

```

1 pragma solidity ^0.4.10; //We have to specify what version of the compiler this code will use
2
3 contract Voting {
4
5     // We use the struct datatype to store the voter information.
6     struct voter {
7         address voterAddress; // The address of the voter
8         uint tokensBought; // The total no. of tokens this voter owns
9         uint[] tokensUsedPerCandidate;
10    }
11
12    /* mapping is equivalent to an associate array or hash
13     The key of the mapping is candidate name stored as type bytes32 and value is
14     an unsigned integer which used to store the vote count
15    */
16
17    mapping (address => voter) public voterInfo;
18
19    /* Solidity doesn't let you return an array of strings yet. We will use an array of bytes32
20     instead to store the list of candidates
21    */
22
23    mapping (bytes32 => uint) public votesReceived;
24
25    bytes32[] public candidateList;
26
27    uint public totalTokens; // Total no. of tokens available for this election
28    uint public balanceTokens; // Total no. of tokens still available for purchase
29    uint public tokenPrice; // Price per token
30
31

```

Зураг 3.18: Code box доторх код

3.10.1 Test net

DAO проектын дараагийн үе нь DAO - ийнхаяа framework - г тохируулах юм. Ингэхийн тулд :

1. Ethereum түрийвч дотроо Develop => Network => Test Net - г сонгоно
2. Contracts цэсний Deploy Contract -г сонгоно
3. Θмнөх бүлэгт сору хийж авсан кодоо Solidity code box - д paste хийж өгнө
4. Contract Picker -ээс Congress - г сонгоно
5. Хэрэв шаардлагатай бол доорх хувьсагчуудаас сонгож болно
 - *minimum quorum* : тухайн саналыг гүйцэтгэхэд шаардлагатай хамгийн бага саналын тоог зааж өгнө
 - *minutes for debate* : тухайн саналыг гүйцэтгэхэд шаардлагатай хамгийн бага хугацааг минутаар тодорхойлох
 - *margin of votes* : тухайн саналыг дэмжигдэхэд 50 хувиас дээш санал авсан байх ёстойг тодорхойлно. Шаардлагагүй бол 0 - оор үлдээд болно

3.10.2 Засаглан болон санал хураалт

Одоо DAO - нхаа удирдлагад нэр өгч болно. Мөн minimum quorum буюу хэдэн хүний санал авч байж шийдвэр гарах доод хэмжээгээ зааж өгөх шаардлагатай.

- DAO - д нэр өгнө Компанидаа нэр өгөхтэй ижил
- Debate time - н хувьд 5 минутыг сонгоно
- Margin of Votes for Majority -г 0 дээр тааруулна Энэ нь танай ажлыг хэр ардчилсан бэ гэдгийг тодорхойлно
- DAO -н үнийг тодорхойлж өгнө Θmnөх бүлэгт түрийвчээрээ дамжуулж test net -д Ether олборлосон. Хэрэв тухайн алхмыг алгассан бол буцаад очоод хий. DAO - г бүтээхэд бага хэмжээний test net Ether хэрэг болно
- Deploy дээр дарж нууц үгээ бичиж өгнө DAO байршуулалт хийхэд бага зэрэг хугацаа орж болно. Хийгдэж дуусаад хянах самбар гарч ирэх ба доош нь гүйлгэвэл таны DAO ажиллаж байгааг харж болно.

3.10.3 DAO -д хөрөнгө оруулах

Туршигдаагүй болон бүрэн судлагдаагүй contract - уудад итгэн их хэмжээний хөрөнгө оруулалт хийхгүй байх хэрэгтэй. Томоохон contract- ууд ихэвчлэн хакеруудын бай болох эрсдэлтэй байдаг. DAO хак нь хамгийн сайн гэж бодсон contract хүртэл хэний ч санаагүй сул талтай байдаг гэдгийн жишээ болно.

Smart contract болон блокчэйн хэдий хөгжлийн эхэн шатандаа байдаа ч биднийг дэлхийн өнцөг бүрээс хэнтэй ч хамтран ажиллах боломжийг олгоно. Гэвч эрсдэлийг бууруулах үүднээс мэддэг бөгөөд итгэлтэй хүмүүстэй ажиллахыг зөвлөдөг.

Аюулгүй байдлын хувьд шинэ алдаа гарахтай зэрэгцэн байнгын хөгжиж байдаг. Бүх шинэ шилдэг туршилтуудыг судалж дүгнэж байх шаардлагатай. Эрсдэлд оруулж буй хөрөнгө болон contract -уудаа хэрхэн нийтэд дэлгэхээ нь хянуур бөгөөд үе шаттай байх хэрэгтэй.

3.10.4 Системд алдаа олох

Санамсаргүй тоо үүсгэгч зэрэг системд шаардлагатай жижиг хэсгүүдийг өөрөө бүтээх гэж оролдох шаардлагагүй. Ингэхийн оронд олон нийт хэдийн туршиж ажиллагаа нь баталгаажсан хэрэгслүүдийг ашиглах илүү үр дүнтэй.

<https://github.com/ethereum/wiki/wiki/safety> - д Ethereum нийгэмлэгийн цуглуулсан маш том алдааны цуглуулга байхаас гадна аюулгүй smart contract бүтээх маш олон ашигтай зөвлөгөөнүүд байдаг.

3.11 Нотариат

Нотариат нь 1925 оноос манай улсад үүсч хөгжсөн төрийн үйлчилгээ бөгөөд 1998 оноос төрийн зарим чиг үүргийг төрийн бус байгууллагаар гүйцэтгүүлэх болсноор тус байгууллага нь бие дааж төрийн бус байгууллага болсон. Монгол улсын хэмжээнд 244 нотариатч, нийслэлийн 8 дүүрэгт 178, орон нутагт 68 тус тус ажиллаж байна. Нотариатч ажиллаагүй суманд буюу нийт 302 сумын засаг даргын Тамгын газрын дарга, хилийн чанадад дипломат төлөөлөгчийн газрын албан тушаалтан Хууль зүйн сайдаас эрх аван нотариатын үүрэг гүйцэтгэгчээр ажиллаж байна. Нотариат дараах үйлчилгээнүүдийг иргэдэд үзүүлдэг. Үүнд:

- Гэрээ хэлцэл, гэрчлэх.
- Гэрээслэл гэрчлэх.
- Итгэмжлэл гэрчлэх.
- Θвлөх эрхийн гэрчилгээ олгох.
- Θвлөгдөх эд хөрөнгийг хамгаалах.
- Хуулийн этгээд үүсгэн байгуулах бичиг баримт гэрчлэх.
- Эд хөрөнгийн эрхийн бүртгэлтэй холбогдох баримт бичиг гэрчлэх.
- Гэр бүлийн гишүүдийн дундаа хамтран болон хэсгээр өмчлөх эд хөрөнгөөс ноогдох хэсгээ өмчлөх эрх гэрчлэх.
- Баримт бичигт зурсан гарын үсгийн үнэн зөвийг гэрчлэх.

- Баримт бичгийн хуулбар гэрчлэх.
- Нотариатын мэдэгдэх хуудас бичих.

3.11.1 Гэрээний тухай

Хэлэлцэгч талууд харилцан тохиролцсоны үндсэн дээр хүлээх эрх, үүрэг хариуцлагаа баталгаажуулсан бичиг баримтыг гэрээ гэнэ. Нотариатын байгууллага иргэдэд:

- Автомашин худалдах, худалдан авах гэрээ
- Орон сууц худалдах, худалдан авах гэрээ
- Иргэд хоорондын зээлийн гэрээ
- Галт зэвсэг худалдах, худалдан авах гэрээ
- Ажлын гэрээ
- Түрээсийн гэрээ
- Орон сууц хөлслөх гэрээ
- Хамтран өмчлөгч хасуулах хэлцэл
- Хамтран өмчлөгч нэмүүлэх хэлцэл
- Газар эзэмших эрх шилжүүлэх гэрээ
- Өмчлөлийн газар худалдах худалдан авах гэрээ гэх мэт гэрээ хэлцэл гэрчлэх үйлчилгээг үзүүлдэг.

3.11.2 Итгэмжлэлийн тухай

Иргэний хуульд заасан бусдыг тодорхой үйлдэлд төлөөлөх эрхийг итгэмжлэл гэнэ. Хуульд бусдыг төлөөлж болох бүх үйлдэлд итгэмжлэл үйлдэж болдог. Жишээ нь:

- Захиран зарцуулах
- Худалдан борлуулах
- Барьцаанд тавих

3.11. НОТАРИАТ

БҮЛЭГ 3. СУДАЛГАА

- Баримт бичигт төлөөлж гарын үсэг зурах
 - Хил гаальд төлөөлөх
 - Асран хамгаалах зэрэг олон төрлийн итгэмжлэлийн төрлүүд байдаг.

3.11.3 Цахим нотариат

2015 оны 1-р сарын 1-ээс өмнө нотариатын байгууллага иргэдэд доорх загварын маягтыг гараар бөглөн хувилж үйлчилдэг байсан.

АВТОМАШИН ХУДАЛДАХ ХУДАЛДАН АВАХ ГҮРЗЭ

Он-сар өдөр

Ийлээсэн газар

Иргэний хуулиин 243.1 дэх хэсгийн заалтыг үндэслэн нэг талаас хаягт орших би

Худалдагч

Иргэний нэр, нэр

Хаягт орших

Худалдан

авагч бид

Иргэний нэр, нэр

Харилцан тохиролцсоны дагуу энэхүү гэрээг байгуулав

1. Худалдагч _____ би худалдан авагч
-д улсас оруулж ирсэн.

Улсын дугаартай, _____ ёнгтэй, _____ маркын, _____ хадалгүүртэй, _____ арал, кузовтой автомашиньг худалдаж байна.

2. Дээрх автомашин нь худалдагч _____ мийн хувийн ёмч бөгөөд энэ нь _____ түн Замын цагдаагийн газраас _____ оны _____ дугаар сарын _____-ны өдөр олгосон _____ серийн _____ дугаар бүхий Тээврийн хэсэгээгээр тохиролцсоно.

3. Автомашиний худалдах унийг _____ тоогоор /
_____ /үсгээр/ төгрөг /доллар, юань, рубль/-өөр
2 тал харилцан тохиролцсон бөгөөд төлбөрийг _____ оны _____ дугаар сарын _____-ны өдөр төлж дуусгана.

4. Гэрээ байгуулах үед уг автомашин худалдагдаагүй, барьцаалгагдаагүй, битүүмжлэгдээгүй, түрээслэгдээгүй, ёмчлэлийн ямар нэгэн маргаан байхгүй болно.

5. Худалдагч автомашиньг худалдан авагч шинжлүүлэн өгөхдөө худалдган өтөх акт үйлдэн. Тус актад худалдан авагч талын хүснэгтээр автомашини бүрэн бүтэн байдал, эвдрэл гэмтлийг зохих шинжлээний байгууллагаар шинжлүүлсэн баримтыг хавсаргаж болно.

6. Энэ гэрээтэй холбогдсон гарах зардлыг хоёр тал харилцан тохиролцож төлнэ.

7. Нэмэлт нөхцөл :

ГЭРЭЭ БАЙГУУЛСАН :

ХУДАЛДАГЧ :

ХУДАЛДАН АВАГЧ :

Иргэний үнэмлэхний № _____ Иргэний үнэмлэхний № _____
Регистрийн № _____ Регистрийн № _____

Зураг 3.19: Маягт

Харин “Цахим Нотариат” ажлын хэсэг байгуулагдаж бүх нотариатч нарыг маягтыг

3.11. НОТАРИАТ

БҮЛЭГ 3. СУДАЛГАА

Microsoft Word програм дээр шивж иргэдэд үйлчлэхийг уриалснаар бичгийн хэлбэр гаргагдахгүй байх асуудлыг шийдвэрлэсэн

Автомашин худалдах худалдан авах гэрээ

2016 он 03 сар 28 өдөр

БГД

Иргэний хуулийн 243 дугаар зүйлийн 243.1 дэх хэсгийн заалтыг үндэслэн нэг талаас БГД 1-р хороо 1-1 тоотод оршин суух Батовогтой Болд би /худалдагч тал/, нэгээ талаас БГД 2-р хороо 2-2 тоот-д оршин суух Дорж овогтой Цэцгээ /худалдан авагч/ бид харилцан тохиропцож энэхүү гэрээг байгуулав.

- Худалдагч Б.Болд би худалдан авагч Д.Цэцгээ-д Япон улсаас оруулж ирсэн, 00-00 ҮҮҮ улсын дугаартай, Хар өнгөтэй, Toyota Prius маркийн, NHW0000000 аралтай авто машины худалдаж байна.
- Дээрх автомашин нь худалдагч Б.Болд миний хувийн ёмч бөгөөд энэ нь АТ газраас 2016 оны 03 сарын 28 өдөр олгосон 00000000 гэрчилгэээр нотлогдоно
- Автомашин худалдах үнийг 10000000 /тоогоор/ Арван сая төгрөг /үсгээр/ төгрөгөөр 2 тал харилцан тохиропцсон бөгөөд төлбөрийн тооцоог 2016/03/28 өдөр бүрэн төлж дууссан.
- Гэрээ байгуулах үед уг автомашин худалдагдаагүй, барьцаалагдаагүй, битүүмжлэгдээгүй, түрээслэгдээгүй, ёмчлэлийн ямар нэгэн маргаангуй болно.
- Худалдагч автомашины худалдан авагчид шилжүүлэн өгөхдөө хүлээлгэн өгөх акт үйлдэнэ. Тус актад худалдан авагч талын хүснэгтээр автомашины бүрэн бүтэн байдал, эвдрэл гэмтлийг зохих шинжилгээний байгууллагаар шинжлүүлсэн баримтыг хавсаргаж болно.
- Энэ гэрээтэй холбогдон гаах зардлыг хоёр тал харилцан тохиропцож төлнө.
- Нэмэлт нөхцөл: Төлбөрийн тооцоо бүрэн дууссан /...../. Гэрээг талууд дуншиж танилцаж зөвшөөрсний үндсэндээр гарын үсэг зурав.

Гэрээ байгуулсан:

ХУДАЛДАГЧ:

Нэр: Б.Болд
/...../.
Регистр: ҮҮ-99999999
Утас: 99999999

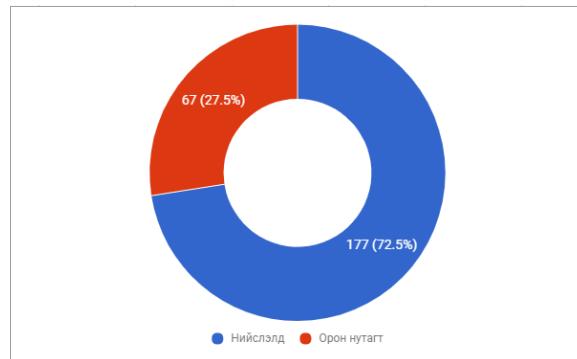
ХУДАЛДАН АВАГЧ:

Нэр: Д.Цэцгээ
/...../.
Регистр: ҮҮ-88888888
Утас: 88888888

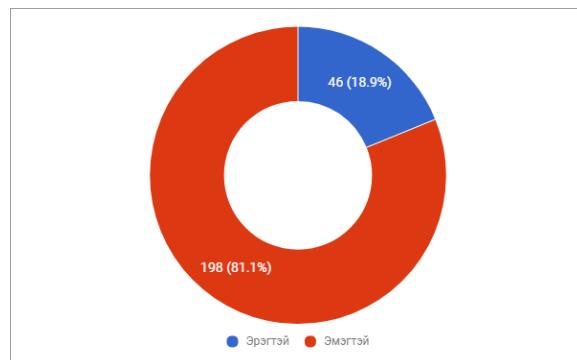
Зураг 3.20: Шивсэн гэрээний маягт

3.11.4 Нотариатчийн судалгаа

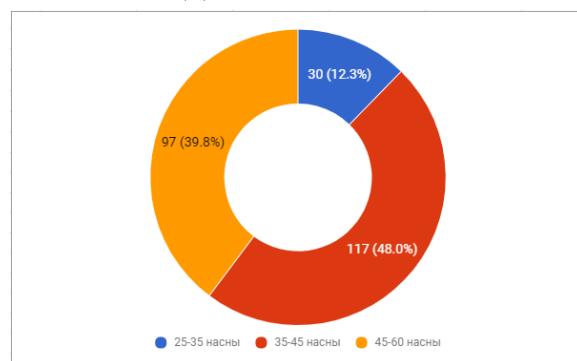
Монгол улсад үйл ажиллагаа явуулдаг нотариатч 246. Үүнийг нарыг бүсчлэлээр нь авч үзвэл:



(a) Бүсчилсэн байдал



(b) Хүйсийн байдал



(c) Насны байдал

3.11.5 Олон улсын чиг хандлага

Дэлхийн олон улс орны нотариатын байгууллага цахимаар үйл ажиллагаагаа явуулдаг бөгөөд тэдгээрийн үндсэн шинж чанарууд адил боловч өөр өөрийн гэсэн өвөрмөц тогтолцоотой. Жишээ болгож таван улс орны нотариатын үйл ажиллагааг харьцуулан судаллаа. Эстони Улс 2007 онд анх Цахим нотариатын системийг нэвтрүүлж эхэлсэн. Цахим нотариатын онцлог шинж нь уг системийн программ хангамжид суурилж үйлчилээг нэвтрүүлснээр иргэн ганц удаа өөрийн биеэр Нотариат дээр ирж үйлчилгээг авна гэсэн зарчмыг баримталсан.

АНУ нь муж болгоныхоо хуулийн дагуу 2012 онд хэрэгжүүлж эхэлсэн. Алсын зайн цахим нотариатын систем ашиглаж эхэлсэн. Skype болон түүнтэй адилхан бодит аудио-видео програмуудыг ашиглан иргэн нотариат дээр ирэхгүй байхаар бичиг баримтыг цахимаар баталгаажуулах боломж бурдсан. Нотариатын бүх үйлчилгээг иргэн өөрийн биеэр эсвэл алсын зайнаас авах боломжтой байдаг.

Япон Улс 2002 онд анх Цахим нотариатыг хэрэгжүүлж эхэлсэн. Улс орнуудын хувьд өөр өөрийн гэсэн онцлогтой байгаа. Япон Улсын онцлог гэвэл Хуульзүйн яамны портал сайтаар дамжуулан нотариатын танхимтай холбогдож үйлчилгээ авах боломжтой. Иргэн Нотариатын 5-н үйлчилгээг зайнаас хандан авах боломжтой. Гэхдээ иргэн нэг удаа заавал нотариат дээр очиж үйлчилгээ авах ёстой байдаг.

БНСУ 2008 онд анх Цахим нотариатын үйлчилгээг портал сайт ашиглан үзүүлдэг. Иргэн заавал өөрийн биеэр нэг удаа нотариатдээр ирж үйлчилгээг авдаг.

Франц 2000 онд Цахим нотариатыг хэрэгжүүлсэн. Франц улсын нотариатч бүх төлбөр тооцоог хүлээн авч бусад байгууллагаруу шилжүүлдэг. Иргэн заавал өөрийн биеэр Нотариатын бүх үйлчилгээн дээр ирнэ.

Манай улсад иргэн нотариатын үйлчилгээ авсаны дараа тухайн үйлчилгээг эрх бүхий байгууллагад бүртгүүлэхэд шаардлагатай төлбөр хураамжийг өөрсдөө банкин дээр очиж тушаадаг бол Франц улсын нотариатч тэр бүх байгууллагуудад төлөх төлбөр хураамжийг авч өөрөө шилжүүлдэг.

Манай улсын нотариатын байгууллагын хувьд цахимд шилжих бурэн боломжтой төдийгүй эхнээсээ хэрэгжиж эхэлсэн. Өвлөх эрхийн гэрчилгээ, өв хүлээн авах татгалзах хүсэлт, гэрээслэлийн мэдээллүүд серверт хадгалагдаж байгаа болно. Тус серверийн зохион байгуулалтаас үзүүлбэл:

БҮЛЭГ 4

ТӨСЛИЙН ХЭСЭГ

4.1 Системийн танилцуулга

Энэхүү систем нь ethereum блокчэйн технологийг ашиглан нотариатын бичиг баримтыг ил тод баталгаажуулах систем юм. Систем нь бичиг баримтыг баталгаажуулах хэсэг болон гэрчилгээ, гэрээний хэсэг 2 үндсэн хэсэгтэй.

Бичиг баримт баталгаажуулах хэсэг:

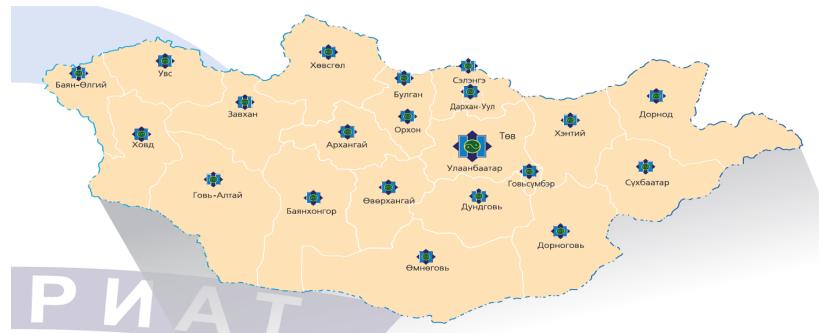
Энэ хэсэг нь нотариатчын баталгаажуулах бичиг баримтуудыг(docx,pdf,png) ухаалаг гэрээний заалтын дагуу тухайн бичиг баримтын хэш утга болон дэлрэнгүй мэдээлэл уншин авч тухайн мэдээллээ ухаалаг гэрээ болгон блокчэйнд хадгалах, блокчэйн руудамжуулах явдал юм.

Гэрчилгээний хэсэг:

Энэ хэсэг нь баталгаажсан бичиг баримтыг ухаалаг гэрээний дагуу блокчэйнээс уншин авч бичиг баримтад гэрчилгээ болгон өгөх зорилготой. Мөн энэ хэсэгт хэрэглэгчид эсвэл нотариатчид байгаа файлыг блокчэйн дээр хадгалагдсан файл мөн эсэхийг шалгах боломжийг олгодог.

4.2 Системийн хамрах хүрээ

Энэхүү систем нь бүх нотариатч нар болон тэдгээрийн туслахууд, нотариатын үүрэг гүйцэтгэгч Засаг даргын тамгын газрын дарга нар болон хилийн чанадад буй дипломат төлөөлөгчийн газрын эрх бүхий албан тушаалтнууд ашиглах боломжтой.



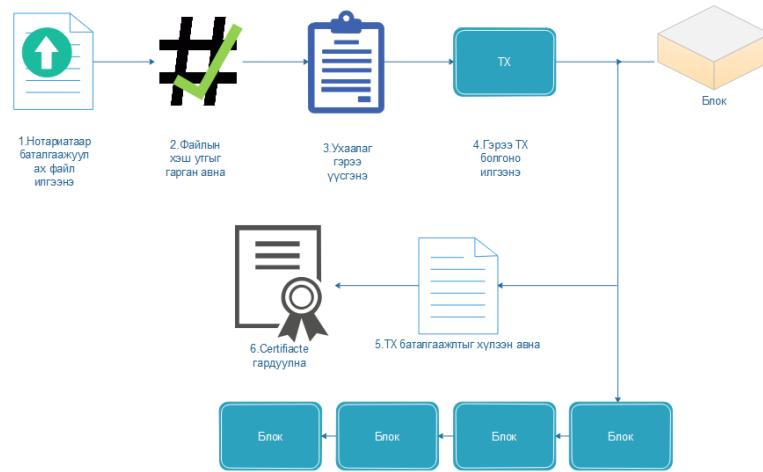
Зураг 4.1: Нотариат

4.3 Багаж хэрэгсэл

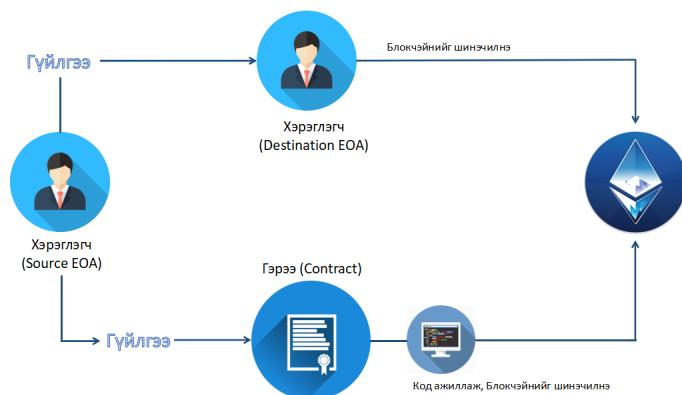
- **Solidity** - Ухаалаг гэрээг бичихэд зориулалсан програмчлалын хэл
- **Javascript** - JavaScript бол энгийн, хялбар програмчлалын хэл юм. Ethereum нь javascript хэл дээр тулгуурлан голчлон ажилладаг.
- **Metamask.io**-Энэ нь бүрэн Ethereum зангилааг татаж ажиллуулахгүйгээр таны хөтөч дээр ethereum dApps(decentralized apps)-ыг ажиллуулах боломжийг олгодог. Мөн хэрэглэгчийг өөр өөр сайтууд дээр таниулж, блокчэйн дэхь гүйлгээг баталгаажуулах боломжтой.
- **Mist browser** - Dapp-уудыг ашиглах болон хайлт хийхэд ашиглах хэрэгсэл
- **Parity** - хурдан, хөнгөн, хүчирхэг ethereum-ийн клиент програм

4.4 Ажиллагаа

Системийн ерөнхий ажиллагах зарчим :



Зураг 4.2: Системийн ерөнхий ажиллагаа



Зураг 4.3: Ethereum блокчэйны ажиллагах зарчим

Систем баталгаажуулах файлыг дараах ухаалаг гэрээний уншин авч блокчэйн рүү хийх мөн буцаагаад дараах байдлаар блокчэйнээс уншин авч харуулах буюу ухаалаг гэрээний ерөнхий схем:

```
[  
  { constant: true, inputs: [], name: "name", outputs: [{ name: "", type: "bytes32" }], payable: false, type: "function" },  
  { constant: true, inputs: [], name: "hash", outputs: [{ name: "", type: "bytes32" }], payable: false, type: "function" },  
  { constant: true, inputs: [], name: "owner", outputs: [{ name: "", type: "address" }], payable: false, type: "function" },  
  { constant: true, inputs: [], name: "size", outputs: [{ name: "", type: "uint256" }], payable: false, type: "function" },  
  { constant: true, inputs: [], name: "timestamp", outputs: [{ name: "", type: "uint256" }], payable: false, type: "function" },  
  { constant: true, inputs: [], name: "file_timestamp", outputs: [{ name: "", type: "uint256" }], payable: false, type: "function" },  
  { constant: true, inputs: [], name: "mime_type", outputs: [{ name: "", type: "bytes32" }], payable: false, type: "function" },  
  {  
    inputs: [  
      { name: "_hash", type: "bytes32" },  
      { name: "_name", type: "bytes32" },  
      { name: "_mime_type", type: "bytes32" },  
      { name: "_size", type: "uint256" },  
      { name: "file_timestamp", type: "uint256" }],  
    payable: true, type: "constructor"  
  }]
```

Зураг 4.4: Гэрээний бүтцийн схем

Блокчэйнээс уншин авах мэдээллүүд:

- **Name** - Файлын нэр
- **Hash** - Файлын хэш утга
- **Owner** - Гэрээг блокчэйнд хадгалж буй нотариатчын хаяг
- **Size** - Файлын хэмжээ
- **Timestamp** - Блокчэйнд хадаглагдсан хугацаа
- **File_timestamp** - Файлын хадаглагдсан хугацаа
- **Mime_type** - Файлын төрөл

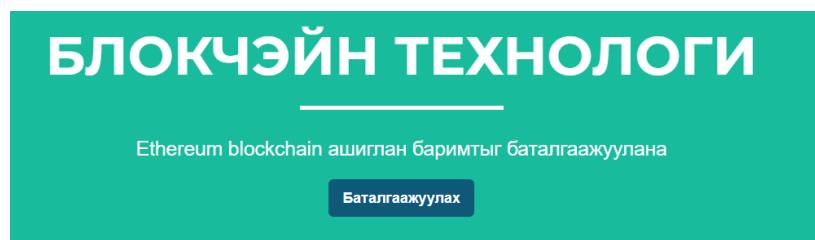
Файлаас унших авах мэдээллүүд:

- **Hash** - Файлын нэр
- **Name** - Файлын хэш утга
- **Mime_type** - Файлын төрөл
- **File_timestamp** - Файлын хадаглагдсан хугацаа
- **Size** - Файлын хэмжээ

4.4. АЖИЛЛАГАА

БҮЛЭГ 4. ТӨСЛИЙН ХЭСЭГ

Систем рүү нэвтрэн ороход дараах дэлгэн харгдах бөгөөд баталгаажуулах товчин дээр дарснаар файлыг баталгаажуулах үйл явц эхлэнэ. Зураг 4.5.



Зураг 4.5: Системийн үндсэн нүүр

Баталгаажуулах файлыг зөөх талбарт руу зөөснөөр файлыг байршуулахгүйгээр/upload/ зөвхөн өмнө дурдсан ухаалаг гэрээний дагуу файлын хэш, өргөтгөл, хэмжээ гэх мэт зүйлсийг уншиж авна. Мөн тухайн файл нь pdf,docx,png өргөтгөлтэй байх шаардлага-тай. Зураг 4.6.



6

Зураг 4.6: Файлаа хуулах талбар

Тухайн файлын мэдээлэл дараах байдлаар харагдана. Хэрэв мэдээллүүдээ шалгаад батлах буюу блокчэйн сүлжээнд оруулахыг хүсвэл батлах товч дээр дарж батална/о-руулна. Зураг 4.7

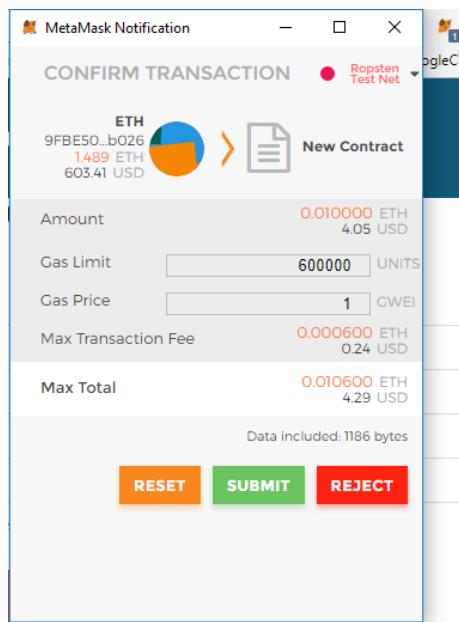
Нэр	notaryStep2.PNG
Файл төрөл	image/png
Хэмжээ	6694 bytes
Файлын сүүлийн сөрчлөлт	1512061502290
Хэш утга	0x519a4db643c24023eeeea49efb329753df16f891b9bb7cc4def59b5159e6b396
	Батлах Цуцлах

Зураг 4.7: Батлах файлын мэдээлэл

4.4. АЖИЛЛАГАА

БҮЛЭГ 4. ТӨСЛИЙН ХЭСЭГ

Файл бүрд тус тусад нь зориулсан шинэ гэрээ үүсгэж өгнө. Нотариатчын өөрийн ethereum хаягаас баталгаажуулалтын, гэрээ үүсгэлтийн гүйлгээг зөвшөөрөх талаар мэдэгдэл ирнэ. Гэрээг үүсгэхэд 0.01 ether, miner-уудада өгөх fee/gas 0.0006 ether буюу нийт 0.0106 ether шаардлагатай. Мөн гүйлгээнд хамт оруулах файлын мэдээлэл нь тогтмол 1186 bytes байна. Зураг 4.8



Зураг 4.8: Шинэ гэрээ үүсгэх

Тухайн бичиг баримтаяа баталсан баталгаа болгож url гэрчилгээг хэрэглэгчид өгнө. Ухаалаг гэрээнд заасны дагуу 7н үзүүлэлтээр гэрчилгээ өгөх болно. Зураг 4.9.

Нотариатын гэрчилгээ

Блокчейн дахь хаяг	0xa99dc7444c9df4d51a90772a512b1cd3354160b0
Нэр	notaryStep2.PNG
Файл төрөл	image/png
Хэмжээ	6694 bytes
Файлын сүүлийн сөрчлөлт	Fri Dec 01 2017 01:05:02 GMT+0800 (Ulaanbaatar Standard Time)
Хэш	0x519a4db643c24023eeeea49efb329753d1f6f891b9b7cc4def59b5159e6b396
Блокчейн дээр баталгажсан хугацаа	Fri Dec 01 2017 01:12:42 GMT+0800 (Ulaanbaatar Standard Time)

Зураг 4.9: Батлагдсан файлын гэрчилгээ

Бичиг баримтын гэрчилгээний дугаар буюу гүйлгээний хаягаар блокчэйн сүлжээнээс ялган харах боломжтой. Мөн хэрэглэгч энэ холбоос руу холбогдоход хаанаас харах, үзүүлэх боломжтой. Зураг 4.10

① localhost:9090/contract.html#0xa99dc7444c9df4d51a90772a512b1cd3354160b0

Зураг 4.10: Гэрчилгээний хаяг

БҮЛЭГ 5

ДҮГНЭЛТ

Нийгэм, техник технологи хурдацтай хөгжихийн хэрээр бүх зүйл бичиг цаасаар дамжих нь багассаар, хүмүүс ч энгийн хялбар ажлыг хөнгөвчилж байгаа зүйлийг хүсэх болсон билээ. Тиймээс ч ихэнх үйлчилгээнүүд электрон хэлбэр рүү шилжсээр байна. Үүнээс үндэслэн нотариатын тогтолцоог илүү хялбар түмэнд илүү хүртээмжтэй, олон дахин нааш цааш явах, хүнд суртлыг багасгах шаардлагатай байна.

Одоогийн веб програмуудын клиентүүд нь бүгд нэг төвлөрсөн сервертэй байдаг. Клиент сервер рүү хүсэлт гаргасны дараа сервер өгөгдлийн сан болон кэш рүү үнших/бичих/шинэчлэх үйлдлүүдээр үйлчилнэ. Тухайн өгөгдлийн сан хандалт нь хязгаарлагдмал, олон нийтэд ил тод биш. Тиймээс клиентийн өгөгдөл найдвартай хадгалаццаа байгаад эргэлзээг үүсгэдэг. Энэхүү хязгаарлагдмал байдлыг блокчэйн технологи дээр шийдсэн нь анхаарлыг татаж байна. Ethereum блокчэйн платформ дээр бүх клиент нь ижил эрхтэй, өгөгдөл сан буюу блокууд нь ил тод, клиентүүдэд төвлөрсөн серверүүд байдаггүй, блокчэйн дэхь бүх блокийг клиентүүд өөр дээрээ хадгалдаг.

Энэхүү системийг хийхэд блокчэйн технологийн давуу тал болох нэгдсэн төв удирдлагагүй, ил тод байдлаар нотариатын тогтолцоонд дутагдаж байгаа чанаруудыг нөхөж, илүү хүртээмжтэй байлгах, мөн блокчэйн технологийг судлан, мэдээлэл дамжуулах, бусдад танин мэдүүлэх зорилготой систем хийлгээ.

БҮЛЭГ 6

Хавсралт

code/js/notar.js

```
1 var app = new Vue({
2   el: '#app',
3   data: {
4     etherscanLink: '',
5     hash: '',
6     name: '',
7     lastModified: '',
8     size: '',
9     type: '',
10    error: '',
11    tx: '',
12    web3Missing: false,
13    animate: false,
14    upload_visible: false,
15    dragging: false
16  },
17  mounted:function(){
18    setTimeout(function() {
19      //console.log('here', web3.eth.accounts,
20      //web3.eth.accounts.length);
21      if (typeof web3 === 'undefined') {
22        app.web3Missing = true;
23      }
24    })
25  }
26})
```

```
23 }, 1000);
24 },
25 methods: {
26     display_upload: function() {
27         window.scrollTo(0,0);
28         app.upload_visible = true;
29     },
30     cancel_upload: function() {
31         app.upload_visible = false;
32         app.hash = "";
33         app.name = "";
34         app.lastModified = "";
35         app.size = "";
36         app.type = "";
37         app.error = "";
38         app.tx="";
39         app.animate = false
40     },
41     create_contract: function () {
42         // 'this' inside methods points to the Vue instance
43
44         if (web3.eth.accounts.length === 0) {
45             alert("Аккаунт олдсонгүй!");
46             return;
47         }
48         app.error="";
49
50         console.log("Гэрээг үүсгэжбайна ,", web3.eth.accounts[0]);
51         var nottarioContract = web3.eth.contract(abi);
52         var nottario =nottarioContract.new( this.hash, this.name,
53             this.type, this.size, this.lastModified,
54             {from:web3.eth.accounts[0], data: bin, gas: 600000, value:
55             100000000000000000}, function(err,data) {
56             console.log(err, data);
57             if (err) {
58                 setInterval(function(){
```

```
56         web3.eth.getTransactionReceipt(app.tx ,
57             function(err,d){
58                 if(!err && d.contractAddress) {
59                     window.location = 'geree.html#' +
60                         d.contractAddress;
61                 }
62             }, 2000);
63         } else {
64             if (data.address) {
65                 window.location = 'geree.html#' + data.address;
66             } else {
67                 app.tx = data.transactionHash;
68                 app.animate = true;
69                 app.etherscanLink = "https://ropsten.etherscan.io/tx/"
70                     + app.tx;
71             }
72         }
73     })
74 }
75
76 function allowDrop(ev) {
77     ev.preventDefault();
78     app.dragging = true;
79 }
80
81 function dragout(ev) {
82     console.logчирэж(' байна. ');
83     app.dragging=false;
84 }
85
86 function drop_handler(ev) {
87     //console.log("Доошоо");
88     ev.preventDefault();
```

```

89  app.dragging=false;
90  console.log('ev ', ev);
91  var f = ev.dataTransfer.files[0];
92  if (!f) {
93      return alertФайлын(' метадатаалдаатай !!!');
94  }
95  console.log ("Файл бол " , f);
96  app.lastModified = f.lastModified;
97  app.name = f.name.substr(0,32);
98  app.size = f.size;
99  app.type = f.type.substr(0,32);
100 if(app.type == "application/pdf" | app.type ==
101     "application/vnd.openxmlformats-o" | app.type == "image/png"){
102     //app.type = f.type.substr(0,32);
103     var reader = new FileReader();
104     reader.onload = function(event) {
105         //console.log(' onload!',event);
106         app.hash = web3.sha3(event.target.result);
107         console.log("хэш нь" + app.hash);
108     };
109     } else {
110         alert("Манай энхүүсistemзөвхөн pdf,docx,png өргөтгөлтэйфайлдэмжинэ
111         !!!");
112     }

```

code/js/notar.js

code/js/solidit.txt

```

1
2 var abi = [
3
4 { constant: true, inputs: [], name: "name",           outputs: [{ name:
5 "", type: "bytes32" }], payable: false, type: "function" },
6 { constant: true, inputs: [], name: "hash",           outputs: [{ name:

```

```
  "", type: "bytes32" }], payable: false, type: "function" },
6 { constant: true, inputs: [], name: "owner", outputs: [{ name:
  "", type: "address" }], payable: false, type: "function" },
7 { constant: true, inputs: [], name: "size", outputs: [{ name:
  "", type: "uint256" }], payable: false, type: "function" },
8 { constant: true, inputs: [], name: "timestamp", outputs: [{ name:
  "", type: "uint256" }], payable: false, type: "function" },
9 { constant: true, inputs: [], name: "file_timestamp", outputs: [{ name:
  "", type: "uint256" }], payable: false, type: "function" },
10 { constant: true, inputs: [], name: "mime_type", outputs: [{ name:
  "", type: "bytes32" }], payable: false, type: "function" },
11
12 { inputs: [
13   { name: "_hash", type: "bytes32" },
14   { name: "_name", type: "bytes32" },
15   { name: "_mime_type", type: "bytes32" },
16   { name: "_size", type: "uint256" },
17   { name: "_file_timestamp", type: "uint256" }],
18 payable: true, type: "constructor" }];
19 var bin =
  "0x606060405260405160a08061040283398101604052808051906020019091908051906020
```

code/js/solidit.txt

code/js/geree.js

```
1 function hextoascii(str1) {
2     var hex  = str1.toString().replace(/0x/, '');
3     var str = '';
4     for (var n = 0; n < hex.length; n += 2) {
5         var ascii = parseInt(hex.substr(n, 2), 16);
6         if (ascii > 0 ) {
7             str += String.fromCharCode(ascii);
8         } else {
9             break;
10        }
11    }
12 }
```

```
12     return str;
13 };
14
15 var app = new Vue({
16     el: '#app',
17     data: {
18         abi: '',
19         etherscanLink: '',
20         hash: '',
21         name: '',
22         type: '',
23         size: '',
24         lastModified: '',
25         address: '',
26         timestamp: '',
27         error: '',
28         web3Missing: false,
29         verified: false,
30         droppedHash: '',
31         dragging: false
32     },
33     mounted: function() {
34         setTimeout(function() {
35             //console.log(`аккаунт ${web3.eth.accounts.length}`);
36             if (typeof web3 === 'undefined') {
37                 app.web3Missing = true;
38             } else {
39                 app.abi = JSON.stringify(abi);
40                 app.read_contract();
41             }
42
43         }, 1000);
44     },
45
46     methods: {
```

```
47     read_contract: function () {
48
49         console.log("Гэрээний уншилт");
50
51         if (window.location.hash && window.location.hash !== '#') {
52
53             var address = window.location.hash.replace(/^#/,'');
54
55             app.address = address;
56
57             app.etherscanLink = "https://ropsten.etherscan.io/address/" +
58                 address;
59
60             var contract = web3.eth.contract(abi).at(address);
61
62             contract.hash(function(err,data){
63
64                 console.log(err,data);
65
66                 app.hash = data;
67
68             });
69
70             contract.name(function(err,data){
71
72                 console.log(err,data);
73
74                 app.name = hextoascii(data);
75
76             });
77
78             contract.timestamp(function(err,data){
79
80                 var timestamp = parseInt(data.toString());
81
82                 var ts = new Date(timestamp * 1000);
83
84                 app.timestamp = ts.toString();
85
86
87                 console.log('timestamp', data, typeof data);
88             });
89
90
91             contract.mime_type(function(err,data){
92
93                 console.log(err,data);
94
95                 app.type = hextoascii(data);
96
97             });
98
99             contract.size(function(err,data){
100
101                 console.log('size',err,data);
102
103                 app.size = parseInt(data.toString());
104
105             });
106
107             contract.file_timestamp(function(err,data){
108
109                 console.log('lastmodified',err,data);
110
111                 var ts = parseInt(data.toString());
112
113             });
114
115         });
116
117     }
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
```

```
82         app.lastModified = new Date(ts).toString();
83     });
84
85     } else {
86         app.error = "Гэрээний хаягбайхгүй !";
87     }
88 }
89 }
90 })
91
92 function allowDrop(ev) {
93     ev.preventDefault();
94     app.dragging=true;
95 }
96
97 function dragout(ev) {
98     console.logчирэхэд(' ');
99     app.dragging=false;
100 }
101
102 function verify_file(ev) {
103     console.log("Verifying");
104     ev.preventDefault();
105     app.dragging=false;
106     var f = ev.dataTransfer.files[0];
107     console.log ("the file is" , f);
108     var reader = new FileReader();
109     reader.onload = function(event) {
110         //console.log('onload!',event);
111         app.droppedHash = web3.sha3(event.target.result);
112         console.log("Файлын хэш " , app.droppedHash);
113         console.log("Блокчэйн дэххэш " , app.hash);
114         if (app.droppedHash == app.hash){
115             app.verified = true;
116         } else {
117             app.verified= false;
```

```
118      }
119
120
121
122  };
123  reader.readAsText(f);
124 }
```

code/js/geree.js

Номзүй

- [1] Blockchain For Dummies, *Dummies*, Tiana Laurence, 1st edition, 2017.
- [2] Blockchain Revolution, *How the technology behind bitcoin is changing money, business, and the world*, Don Tapscott, Alex Tapscott, 1st edition, 2016.
- [3] Mastering Bitcoin, *Programming the Open Blockchain*, Andreas M. Antonopoulos, 2nd edition, 2017.
- [4] Blockchain For Dummies, *IBM*, Manav Gupta, IBM Limited Edition, 2017.
- [5] What is Blockchain Technology? A Step-by-Step Guide For Beginners <https://blockgeeks.com/guides/what-is-blockchain-technology/>
- [6] A Guide to Bitcoin (Part I): A look under the hood <http://tech.eu/features/808/bitcoin-part-one/>
- [7] A Guide to Bitcoin (Part II): A deep dive into the Bitcoin ecosystem <http://tech.eu/features/926/bitcoin-ecosystem/>
- [8] Bitcoin by analogy <https://www.ybrikman.com/writing/2014/04/24/bitcoin-by-analogy/>
- [9] A gentle introduction to blockchain technology <https://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/>
- [10] Ethereum Blockchain App Platform <https://www.ethereum.org/>
- [11] Official Go implementation of the Ethereum protocol <https://github.com/ethereum/go-ethereum>
- [12] Testnet Ethereum Block Explorer <http://ropsten.etherscan.io/>